

cahiers scientifiques

FASCICULE XX

PUBLIÉS

ON DE GASTON JULIA

UNIVERSITY OF ARIZONA



39001006896784

algèbre

par PAUL DUBREIL,

professeur à la Faculté des Sciences de Paris

Maître de conférences à l'École Polytechnique

préface de Gaston JULIA, membre de l'Institut

GAUTHIER-VILLARS PARIS



Digitized by the Internet Archive
in 2022 with funding from
Kahle/Austin Foundation

ALGÈBRE

TOME I

ÉQUIVALENCES, OPÉRATIONS
GROUPES, ANNEAUX, CORPS

CAHIERS SCIENTIFIQUES

PUBLIÉS SOUS LA DIRECTION DE M. GASTON JULIA

FASCICULE XX

ALGÈBRE

PAR

Paul DUBREIL

ANCIEN ÉLÈVE DE L'ÉCOLE NORMALE SUPÉRIEURE
PROFESSEUR A LA FACULTÉ DES SCIENCES DE PARIS
MAÎTRE DE CONFÉRENCES A L'ÉCOLE POLYTECHNIQUE

Préface de M. Gaston JULIA

MEMBRE DE L'INSTITUT

TOME I

ÉQUIVALENCES, OPÉRATIONS
GROUPE, ANNEAUX, CORPS

TROISIÈME ÉDITION REVUE ET AUGMENTÉE

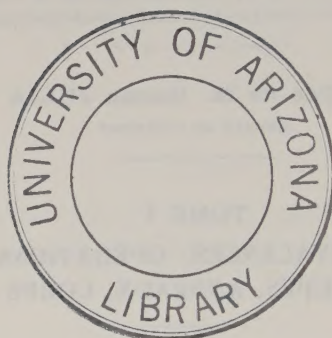
gv

PARIS

GAUTHIER-VILLARS & C^{ie}, ÉDITEUR-IMPRIMEUR-LIBRAIRE

55, Quai des Grands-Augustins

—
1963



© 1963 Copyright by Gauthier-Villars,
Tous droits de traduction, de reproduction et d'adaptation réservés
pour tous pays.

512
D819
1963
v.1

PRÉFACE

Chargé en 1941 d'une série de conférences d'Algèbre à l'Institut Henri Poincaré, M. Paul Dubreil eut l'occasion d'exposer les premiers principes des méthodes algébriques modernes. Ce fut l'origine du présent volume, qui développe cet enseignement en suivant les mêmes idées directrices.

L'objet de l'Algèbre est l'étude des ensembles où sont définies des opérations. La nature des éléments d'un tel ensemble, et celle des opérations importent beaucoup moins que les règles de calcul, qui constituent l'essentiel. Ces règles sont moins fixes qu'on ne le dit si souvent en parlant des *règles du Calcul algébrique*. Les Mathématiques font une place de plus en plus grande aux opérations non commutatives ou même non associatives; la distributivité de la multiplication par rapport à l'addition entraîne qu'un produit est nul dès qu'un facteur au moins l'est, mais la réciproque n'est nullement nécessaire : il peut exister des diviseurs de zéro. Il y a donc en réalité *des* calculs algébriques, ou plutôt différents types de domaines : *groupes* abéliens ou non, *anneaux* commutatifs ou non, *domaines d'intégrité*, *corps* de caractéristique nulle ou différente de zéro, etc . . . , dans lesquels le calcul obéit à des lois très diverses. Rechercher les possibilités intéressantes, les classer dans une axiomatique précise et les étudier systématiquement, telle est la tâche de l'Algébriste.

Dans son exposé, M. Paul Dubreil s'est laissé guider par quelques principes simples. Tout mathématicien fait, parfois sans le savoir, de l'Algèbre moderne, et l'on peut déjà aller loin en

partant des choses les plus connues. Construire, par exemple, les nombres rationnels à partir des entiers naturels (positifs ou négatifs), c'est plonger un domaine d'intégrité dans un corps. Ce *problème d'immersion*, qui est sans doute le plus important, dérive en réalité d'un autre, plus simple et plus typique : plonger un semi-groupe *abélien* dans un groupe ; si l'on passe au cas *non abélien*, la solution du même problème devient une question difficile, pleine d'intérêt pour l'Algébriste.

L'analyse méthodique des principes offre un second point de départ. Le tout premier principe de l'Algèbre, c'est la notion même d'*opération abstraite* ou *loi de composition*. En analysant systématiquement les propriétés possibles d'une opération, qui peuvent être classées en propriétés de fermeture, règles de calcul et propriétés d'inversion, on voit apparaître des liens logiques intéressants : quelques propriétés simples, convenablement combinées, entraînent des conséquences remarquables, d'où sortent, d'une façon à la fois logique et naturelle, les axiomes des groupes.

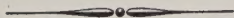
On ne saurait enfin trop mettre en évidence l'importance des emprunts que l'Algèbre fait à la *Théorie des Ensembles* : calcul des parties (intersection, réunion), applications, équivalences et décompositions en classes, ensemble-produit, etc. Sous l'influence des travaux de l'École américaine, particulièrement de O. Ore et G. Birkhoff, et de ceux qu'il a entrepris dès 1938 en collaboration avec M^{me} Dubreil, M. Dubreil insiste, plus qu'on ne le fait d'ordinaire, sur les équivalences, et montre qu'elles se prêtent maintenant à un calcul tout à fait souple. Avec la notion d'équivalence régulière par rapport à une ou plusieurs opérations ⁽¹⁾, on dispose d'un moyen qui conduit d'un coup à la décomposition d'un groupe par rapport à un sous-groupe, à la notion de sous-groupe invariant et à celle d'idéal dans un anneau.

(¹) Une équivalence, c'est-à-dire une relation réflexive, symétrique et transitive, est régulière à droite par rapport à la multiplication par exemple, si, a et x étant équivalents, ax et bx le sont quel que soit x .

On rencontre la même idée à la base des généralisations successives de la notion de nombre. A ces avantages didactiques s'ajoutent des énoncés nouveaux et simples : la condition nécessaire et suffisante pour que deux sous-groupes soient permutable est que les équivalences correspondantes soient associables ; l'équivalence de transitivité d'un groupe de substitutions est le produit des équivalences de transitivité des substitutions du groupe. Enfin, les équivalences régulières jouent un rôle essentiel dans les problèmes d'immersion et dans la recherche des groupes homomorphes à un demi-groupe donné.

Ces particularités font que le livre de M. Paul Dubreil diffère sensiblement des traités d'Algèbre déjà parus. Nous espérons que sa lecture pourra non seulement faciliter au public français l'étude de l'Algèbre moderne, mais aussi présenter quelque intérêt pour les spécialistes eux-mêmes.

GASTON JULIA.



INTRODUCTION

Ce premier volume contient, avec un chapitre préliminaire consacré aux éléments de la Théorie des Ensembles, une partie importante des notions fondamentales de l'Algèbre moderne : opérations, équivalences, homomorphismes ; groupes, anneaux, corps, idéaux ; polynômes et premières notions sur les équations algébriques. Un second volume qui se rattachera étroitement au premier, sera consacré aux groupes avec opérateurs (théorèmes d'isomorphisme et de Jordan-Hölder), aux éléments de l'Algèbre linéaire et à la Théorie de Galois. J'espère, en outre, développer dans des volumes ultérieurs, si les circonstances me le permettent, des théories algébriques relativement autonomes, telles que la Théorie des Idéaux et celle des Systèmes hypercomplexes.

La lecture de ce tome premier ne suppose à peu près aucune connaissance préalable, mais elle sera surtout profitable aux lecteurs possédant déjà une certaine culture mathématique, celle des mathématiques spéciales ou des premiers certificats de licence. Je me suis efforcé de commander l'exposé par un petit nombre d'idées générales faciles à assimiler, de donner les démonstrations avec tous les détails nécessaires, d'expliquer les principales définitions ou les points un peu délicats par des exemples aussi concrets et aussi simples que possible. Ces exemples, à vrai dire, n'ont rien à voir avec le développement logique et constituent parfois des anticipations. Pour cette raison, et bien qu'un peu de réflexion de la part du lecteur suffise à éviter tout malentendu, ils sont imprimés en caractères plus fins, employés également pour certaines remarques et pour les énoncés d'exercices. Ceux-ci, en général très faciles, permettront au lecteur de contrôler l'assimilation du texte et de travailler d'une façon plus vivante. On utilisera l'index alphabétique pour retrouver rapidement une définition oubliée ou pour étudier une question isolée. Quelques Notes, à la fin du volume, apportent différents

compléments utiles pour la compréhension de certains passages de ce tome ou des suivants.

Je voudrais m'être interposé aussi peu que possible entre le lecteur et la vaste littérature algébrique parue depuis une vingtaine d'années. J'ai tenu à donner toutes les indications bibliographiques me paraissant intéressantes, je souhaite ne pas avoir commis d'omissions trop nombreuses. Je me suis efforcé d'aider le lecteur débutant à lire sans trop de peine les Mémoires originaux; lorsque la terminologie n'était pas encore fixée, j'ai indiqué les différents termes dont il a été fait usage.

Ma tâche a été beaucoup facilitée par les remarquables Traités ou Monographies d'Algèbre parus depuis une quinzaine d'années, notamment :

H. HASSE, *Höhere Algebra*.

B. L. VAN DER WAERDEN, *Moderne Algebra*.

O. ORE, *L'Algèbre abstraite*.

A. A. ALBERT, *Higher Algebra*.

G. BIRKHOFF, *Lattice Theory*.

N. BOURBAKI, *Éléments de mathématique*.

Je leur ai emprunté bien des modes d'exposition devenus classiques, sans cependant me soustraire à l'influence de l'actualité scientifique, ni à mes tendances personnelles. Je tiens aussi à mentionner ici tout le profit que j'ai retiré jadis, grâce à la Fondation Rockefeller, de la fréquentation de plusieurs Maîtres éminents : E. Artin, Emmy Noether, B. L. van der Waerden.

J'espère que les nombreuses additions (environ cent cinquante pages) qui constituent la principale différence entre cette deuxième édition et la première élèveront sensiblement le niveau scientifique du livre, sans en changer l'esprit. Elles vont des tout premiers principes de la Théorie des Ensembles et de l'Algèbre aux théorèmes fondamentaux et aux applications.

Une large place a été faite aux ensembles partiellement ordonnés et à la Théorie des Treillis. Celle-ci a été récemment exposée pour elle-même dans les *Leçons sur la Théorie des Treillis, des Structures algébriques ordonnées et des Treillis géométriques* de M.-L. Dubreil-Jacotin, L. Lesieur et R. Croisot, fascicule XXI de cette collection. J'ai indiqué ici ses liens les plus simples avec la théorie des groupes et la théorie

des anneaux. J'ai utilisé par exemple le théorème de Moore et la notion de fermeture, au sens de cet auteur, dans l'étude des relations transitives, des sous-groupes d'un groupe, des idéaux d'un anneau.

Quelques pages ont été consacrées aux applications multiformes (chap. I, § 8); les deux théorèmes fondamentaux (p. 33 et 35) sont appliqués aux correspondances de Galois (p. 120), à la correspondance de Grell entre les idéaux d'un anneau et ceux d'un sur-anneau (p. 193), aux complexes forts d'un demi-groupe (p. 235).

La discussion des propriétés d'inversion d'une opération a été complétée par quelques emprunts à la Théorie de la résiduation. Les quotients d'un complexe par un élément, les résidus d'un complexe, les complexes unitaires (p. 92) jouent un rôle fondamental dans la partie de la Théorie des Demi-groupes qui est la plus proche de la Théorie des Groupes (chap. V, § 4 et 5) : étude des équivalences principales, des équivalences régulières (éventuellement simplifiables), des complexes forts (ou forts et symétriques), détermination des groupes et pseudo-groupes homomorphes. J'ai donné une assez large place à ces questions qui ont fait l'objet soit de travaux très récents, soit de publications un peu plus anciennes, mais assez difficilement accessibles.

Le paragraphe 14 du chapitre IV, entièrement ajouté, concerne les propriétés de décomposition dans un demi-groupe abélien avec élément-unité. On obtient d'abord la représentation d'un idéal d'un anneau noëthérien comme intersection d'idéaux primaires (p. 212), appliquée plus loin au théorème de Noëther sur l'intersection de deux courbes algébriques planes (p. 378). On aboutit d'autre part aux propriétés de factorisation dans les semi-groupes et les domaines d'intégrité (p. 217 et chap. VI, A); l'étude de ces propriétés est poussée plus avant au moyen de la condition de Krull caractérisant les anneaux à factorisation unique (p. 314).

L'ancienne Note sur les nombres naturels et les ensembles finis et dénombrables a été dédoublée et sérieusement modernisée. La Note I est consacrée maintenant à la théorie directe des ensembles finis. Au lieu de choisir une des définitions possibles, j'ai exposé les plus importantes et montré leur équivalence, car cette coexistence de propriétés caractéristiques très diverses est, à mon avis, le fait le plus intéressant. Par la notion d'ensemble discret sans dernier élément, on passe avec une grande facilité à l'ensemble des nombres naturels, objet de la Note II.

La Note III, consacrée à l'axiome du choix, a été complétée par quelques pages sur le théorème de Zorn, les conditions de Hausdorff et de Tukey ; l'équivalence de ces divers énoncés est établie.

Pour faciliter le travail du lecteur, la notion de corps a été rapprochée de celle d'anneau (p. 140) et les problèmes d'immersion abéliens ont été traités directement au début du chapitre V, où l'on trouvera, en particulier, l'immersion d'un domaine d'intégrité dans un corps (p. 228).

Enfin, quelques exercices ont été ajoutés.

J'exprime mes sincères remerciements aux Collègues qui m'ont suggéré telle ou telle amélioration. Mon amicale reconnaissance va tout particulièrement à M. Robert Croisot dont l'aide m'a été très précieuse dans la mise au point du texte et dans la correction des épreuves.

Qu'il me soit permis d'exprimer mon affectueuse gratitude à M. Gaston Julia qui a bien voulu provoquer la rédaction de ce livre et l'accueillir dans sa belle collection, et à M. Albert Châtelet à qui je dois de nombreux encouragements et de précieuses suggestions.

J'adresse aussi mes très sincères remerciements à la Maison Gauthier-Villars qui, après avoir mené à bien, malgré les plus grandes difficultés matérielles, l'impression de la première édition, a accepté, pour la deuxième, les nombreux remaniements et les larges additions que je lui proposais.



ALGÈBRE

CHAPITRE 1.

ENSEMBLES, RELATIONS, CORRESPONDANCES.

A. — ÉLÉMENTS, SOUS-ENSEMBLES.

1. **Principes de la Théorie des Ensembles.** — En Mathématiques comme dans la vie courante, on est souvent amené à rassembler des êtres $a, b, c, \dots$, possédant quelque caractère commun ou destinés à un même usage : on parle alors de l'*ensemble* E de ces êtres, on dit de ceux-ci qu'ils sont les *éléments* de E . On écrit

$$E = \{ a, b, c, \dots \}.$$

L'ensemble E est regardé comme *donné* ou *défini* quand on a énoncé une condition nécessaire et suffisante pour qu'un être soit élément de E , en d'autres termes quand on a fixé clairement le sens de la *propriété d'appartenance*

$a \in E$, « a est élément de E , ou appartient à E ».

On écrit aussi $E \ni a$, pour exprimer que E comprend a parmi ses éléments, et $m \notin E$ pour exprimer que l'être m n'est pas élément de E .

Deux ensembles *coïncident*, ou sont *égaux*, si chaque élément de l'un appartient à l'autre :

$$E = E' \quad \text{si} \quad a \in E \Leftrightarrow a \in E'$$

(le signe $\Leftrightarrow$ exprime l'équivalence logique de deux propositions : on le lit « équivaut à » ou « si et seulement si »).

Exemples et remarques. — La manière la plus simple de donner un ensemble consiste à désigner individuellement et successivement ses éléments; c'est ainsi que l'on définit un alphabet en indiquant l'une après l'autre les lettres qui le composent, ou qu'on parle en Géométrie de l'ensemble des sommets $\{ A, B, C, D \}$ d'un carré.

Mais le mode de définition précédent n'est pas toujours possible; il ne saurait s'appliquer, par exemple, à la définition d'une circonférence : la circonférence C de centre O et de rayon ρ , dans un plan, est l'ensemble des points m de ce plan tels que la distance Om soit égale à ρ :

$$C = \{ m \}_{Om=\rho}.$$

Cette définition suppose, d'une part, que l'on dispose préalablement du plan regardé comme ensemble de ses points, dans lequel l'ensemble C à définir va être plongé, d'autre part, que la notion de distance est acquise. Il est clair que les propriétés de cette distance vont commander la Géométrie du Cercle, et il faut noter que cette notion de distance repose à son tour sur celle de nombre réel.

Cet enchaînement dans la définition des ensembles qui interviennent en Mathématiques est sans aucun doute une source de difficultés, car il semble illusoire d'espérer partir de quelque ensemble primitif dont tous les autres dériveraient : l'ensemble $N = \{ 1, 2, 3, \dots, n, \dots \}$ des nombres naturels est déjà trop complexe pour pouvoir jouer convenablement ce rôle, l'étude des ensembles finis ne fera que le confirmer (*voir* Note I). Une autre difficulté dans l'exposé de la Théorie des Ensembles provient du fait qu'une théorie mathématique ne peut s'exprimer, d'une façon réellement accessible, qu'au moyen du langage, et que le langage contient déjà des termes fortement apparentés aux mathématiques, et particulièrement à la Théorie des Ensembles, comme *un, aucun, au moins un, plusieurs*, etc. Nous laisserons de côté la recherche du minimum de termes ou de signes indispensables pour constituer le langage mathématique, et l'étude de leurs combinaisons; cette recherche et cette étude sont plutôt du domaine de la logique mathématique. Sans nous attarder sur les fondements de la Théorie des Ensembles et sa formalisation ⁽¹⁾, ni sur les tentatives faites pour écarter les antinomies (plus ou moins sérieuses) qu'on a pu soulever à son sujet, nous essaierons d'indiquer sous une forme intuitive, mais précise, en partant à peu de choses près des axiomes de Zermelo-Fraenkel, les notions et les formules de Théorie des Ensembles qui sont indispensables en Algèbre comme dans la plupart des autres sciences mathématiques.

On dit qu'un ensemble A est *sous-ensemble* ou *partie* d'un ensemble E ou encore que A est *contenu dans* E , que E *contient* A , et l'on écrit

$$A \subseteq E \quad (\text{ou } A \subseteq E, E \supseteq A, E \supseteq A).$$

si tout élément de A appartient à E . L'égalité $E = E'$ signifie $E \subseteq E'$ et $E' \subseteq E$. La relation d'inclusion $\subseteq$ est transitive :

$$A \subseteq B \quad \text{et} \quad B \subseteq C \quad \text{entraînent} \quad A \subseteq C.$$

⁽¹⁾ On pourra consulter : A. FRAENKEL, *Einleitung in die Mengenlehre* (Berlin, Springer, 1923); J. CAVAILLES, *Remarques sur la formation de la Théorie abstraite des Ensembles* (Paris, Hermann, 1937); H. CARTAN, *Sur le fondement logique des Mathématiques* (*Revue scientifique*, n° 3216, 1943, p. 3); HAO WANG et R. NAUGHTON, *Les systèmes axiomatiques de la Théorie des Ensembles* (*Coll. Logique Math.*, fasc. IV, Paris, Gauthier-Villars, 1953).

Si A est contenu dans E sans coïncider avec lui, on dira que A est *partie propre*, ou *véritable sous-ensemble* de E , et l'on écrira $A \subset E$.

A étant une partie propre de E , l'ensemble des éléments de E qui n'appartiennent pas à A est une autre partie A' de E appelée *complément* (ou *sous-ensemble complémentaire*) de A dans E ; on écrit

$$A' = E - A \quad \text{ou} \quad A' = C_E A.$$

Si A est défini par une propriété caractéristique $\mathcal{P}$, portant sur les éléments de E , A' est défini par la *négarion* $\bar{\mathcal{P}}$ de $\mathcal{P}$ ⁽¹⁾.

Parmi les parties d'un ensemble E , nous nous donnerons le droit de considérer celle qui ne contient *aucun élément*, et nous l'appellerons la *partie vide*. On la rencontre toutes les fois que l'on cherche les éléments de E vérifiant un système de conditions incompatibles. (*Exemple* : ensemble des nombres premiers qui sont carrés parfaits, dans l'ensemble des nombres naturels, 1 n'étant pas regardé comme nombre premier.) La partie vide est le complément de E dans E . D'après la définition de l'égalité des ensembles, si E et E' sont des ensembles quelconques, leurs parties vides doivent être regardées comme égales : on parlera donc uniquement de l'*ensemble vide*, qui sera désigné par $\emptyset$.

Un ensemble E étant donné, nous nous donnerons le droit de regarder comme défini l'*ensemble de ses parties* (partie vide comprise), qui sera désigné par $\mathcal{P}(E)$:

$$A \in \mathcal{P}(E) \iff A \subseteq E.$$

Un sous-ensemble $\mathcal{F}$ de $\mathcal{P}(E)$,

$$\mathcal{F} = \{A, B, \dots\} \quad (A, B, \dots \subseteq E)$$

sera commodément désigné par *famille de parties* de E . Il est commode de représenter les éléments de E par des petites lettres, les parties par des capitales ordinaires, les familles de parties par des capitales italiques.

Remarque. — Le concept « l'ensemble de tous les ensembles » qui a donné lieu à l'une des antinomies de la Théorie des Ensembles, doit être rejeté comme contradictoire ⁽²⁾. Si E était l'ensemble de tous les ensembles, nous aurions

⁽¹⁾ La formation de la négation d'une propriété est parfois un peu délicate et il y a lieu de s'y entraîner. Soit, par exemple, E l'ensemble des fonctions réelles de la variable x , définies pour $x > 0$, et $\mathcal{P}$ la propriété : « A tout $\varepsilon > 0$, on peut associer $r > 0$ tel que $(0 <) x < r$ entraîne $|f(x)| < \varepsilon$ » [$f(x) \rightarrow 0$ quand $x \rightarrow +0$]. La négation s'énonce : « il existe au moins un $\varepsilon > 0$ tel que, quel que soit $r > 0$, on puisse trouver au moins un x vérifiant $(0 <) x < r$ et $|f(x)| \geq \varepsilon$ ».

⁽²⁾ Et aussi, bien entendu, comme dépourvu de sens : s'agit-il, en effet, de *tous* les ensembles dont les éléments sont actuellement des *êtres matériels* (?), ou admettra-t-on

$A \in E$ pour toute partie A de E , en particulier $E \in E$. Considérons alors les éléments de E (c'est-à-dire les ensembles) ayant la propriété $x \notin x$, et soit X la partie de E , ensemble de ces éléments $x : X \in E$. Si $X \in X$, on a, d'après la définition de X , $X \notin X$, et il y a contradiction; si $X \notin X$, on a $X \in X$, et il y a encore contradiction.

Soient A un ensemble et B un ensemble pouvant être distinct de A ou coïncider avec lui. Nous considérerons comme défini l'ensemble P des *couples ordonnés* (a, b) dont le premier élément a est un élément quelconque de A (nous dirons d'une façon plus imagée, *décrit* l'ensemble A), tandis que le second, b , décrit l'ensemble B , d'une façon indépendante. P est appelé *ensemble-produit* ou *produit* de A par B et désigné par $A \times B$. Si $B = A$, on écrit $A \times A = A^2$. On définit de même le produit $A \times B \times C$ comme l'ensemble des systèmes (a, b, c) , où $a \in A$, $b \in B$, $c \in C$, et ainsi de suite.

Exemple. — A étant l'alphabet français, $A^2 = \{aa, ab, \dots, zz\}$ est l'ensemble des *mots formels* de deux lettres, c'est-à-dire des assemblages considérés indépendamment de toute signification. On notera que l'ensemble des mots de deux lettres appartenant effectivement à la langue française ne peut pas être regardé comme une partie de A^2 , car deux mots distincts tels que *or* (substantif) et *or* (conjonction) coïncident en tant que mots formels.

On est souvent amené à considérer des ensembles dont les éléments sont eux-mêmes des ensembles : ensemble de sacs dont chacun est un ensemble de pommes, ensemble de droites dont chacune est un ensemble de points. Nous dirons alors, pour plus de commodité, que nous sommes en présence d'une *famille d'ensembles*, $\mathcal{F}$. Fréquemment, il existe une *correspondance biunivoque* entre les éléments de $\mathcal{F}$ et les éléments d'un certain ensemble Λ , c'est-à-dire une loi associant à chaque élément λ de Λ un élément L de $\mathcal{F}$ de façon que chaque élément de $\mathcal{F}$ soit obtenu ainsi une fois et une seule. On dit alors que la famille $\mathcal{F}$ est *indexée* par l'ensemble Λ , on note L sous la forme L_λ et l'on écrit

$$\mathcal{F} = \{L_\lambda\}_{\lambda \in \Lambda}$$

(« ensemble des L_λ quand λ décrit Λ »).

Si λ décrit seulement une partie Λ' de Λ , L_λ décrit une partie $\mathcal{F}'$ de $\mathcal{F}$:

$$\mathcal{F}' = \{L_\lambda\}_{\lambda \in \Lambda'}.$$

aussi comme éléments des êtres qui ne sont plus ou qui n'existent pas encore, des personnages légendaires, des concepts abstraits? De tels concepts, admis par les uns, peuvent être inconcevables pour les autres!

Exemple. — Considérons dans l'espace la famille $\mathcal{F}$ des droites D parallèles à une direction Δ . Il existe une correspondance biunivoque entre les droites D et leurs traces m sur un plan P non parallèle à Δ . On peut donc indexer la famille $\mathcal{F}$ par l'ensemble P des points m et écrire

$$\mathcal{F} = \{ D_m \}_{m \in P}.$$

L'ensemble des génératrices du cylindre ayant pour directrice une courbe C du plan P est la partie

$$\mathcal{F}' = \{ D_m \}_{m \in C}$$

de la famille $\mathcal{F}$.

Il peut y avoir intérêt à répéter, dans une famille $\mathcal{F}$, un même ensemble en l'affectant chaque fois d'un nouvel indice : les éléments de $\mathcal{F}$ ainsi obtenus seront alors regardés comme *distincts*.

Soit $\mathcal{F} = \{ L_\lambda \}_{\lambda \in \Lambda}$ une famille d'ensembles. Nous considérerons comme défini et appellerons *réunion générale* des ensembles constituant $\mathcal{F}$, l'ensemble E des éléments x des L_λ :

$$x \in E \Leftrightarrow x \in L_\lambda \quad \text{pour un } \lambda \in \Lambda.$$

Ainsi, l'espace est la réunion générale des droites D_m de la famille $\mathcal{F}$ considérée plus haut, le cylindre est celle de la sous-famille $\mathcal{F}'$.

Remarque. — On peut rattacher la notion d'ensemble-produit $A \times B$ à celle de réunion générale. Considérons la famille $\mathcal{F} = \{ A_b \}_{b \in B}$ obtenue en répétant l'ensemble A de façon à indexer $\mathcal{F}$ par B . La réunion générale E des ensembles de cette famille $\mathcal{F}$ correspond biunivoquement au produit $A \times B$; il suffit d'associer au couple $(a, b) \in A \times B$ l'élément a de A considéré comme appartenant à A_b . On peut convenir d'*identifier* E et $A \times B$, c'est-à-dire de ne faire aucune distinction entre ces deux ensembles.

2. Intersection, réunion. — Soient A et B deux parties d'un même ensemble E . L'*intersection*

$$I = A \cap B$$

notée parfois aussi $A.B$ ou $[A, B]$, de A et B , est, par définition, l'ensemble des éléments de E qui appartiennent *à la fois* à A et à B . Si l'on a $I = \emptyset$, donc si A et B n'ont aucun élément commun, on dit que A et B sont *disjoints*.

La *réunion*

$$R = A \cup B$$

de deux parties A et B de E est, par définition, l'ensemble des éléments de E qui appartiennent à *l'un au moins* des ensembles A et B ⁽¹⁾.

(1) Le signe $\cap$ se lit « inter »; le signe $\cup$ se lit « réunion ».

On a

$$I \subseteq A \subseteq R, \quad I \subseteq B \subseteq R$$

et la relation $A \subseteq B$ entraîne $I = A, R = B$.

Quand les deux ensembles A et B sont *disjoints*, leur réunion prend le nom de *somme* et se désigne par $A + B$.

L'intersection et la réunion des parties possèdent les propriétés suivantes. Elles sont *commutatives*, c'est-à-dire

$$A \cap B = B \cap A, \quad A \cup B = B \cup A,$$

puisque A et B jouent des rôles symétriques dans les définitions. Elles sont également *associatives*, c'est-à-dire

$$A \cap (B \cap C) = (A \cap B) \cap C, \quad (A \cup B) \cup C = A \cup (B \cup C),$$

car les deux membres de la première égalité sont l'un et l'autre l'ensemble des éléments de E qui appartiennent à la fois aux trois ensembles A, B, C ; de même les deux membres de la deuxième égalité sont l'un et l'autre l'ensemble des éléments de E qui appartiennent à l'un au moins des trois ensembles A, B, C .

Enfin, l'intersection est *distributive* par rapport à la réunion

$$(1) \quad A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$

et de même la réunion est distributive par rapport à l'intersection

$$(2) \quad A \cup (B \cap C) = (A \cup B) \cap (A \cup C).$$

Établissons la relation (1), en montrant que l'ensemble figurant au premier membre est contenu dans l'ensemble figurant au second membre, et inversement.

Soit $x \in A \cap (B \cup C)$: on a

$$x \in A \quad \text{et} \quad x \in B \cup C,$$

donc x appartient à l'un au moins des ensembles B et C , par exemple à B . Il en résulte

$$x \in A \cap B \subseteq (A \cap B) \cup (A \cap C)$$

et nous avons, par suite,

$$A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C).$$

Inversement, un élément x de $(A \cap B) \cup (A \cap C)$ appartient à l'un au moins des ensembles $A \cap B$ et $A \cap C$, par exemple à $A \cap B$; d'où $x \in A, x \in B \subseteq B \cup C$, donc

$$x \in A \cap (B \cup C)$$

et nous avons

$$A \cap (B \cup C) \supseteq (A \cap B) \cup (A \cap C),$$

d'où l'égalité.

Pour établir la relation (2), considérons un élément $x \in A \cup (B \cap C)$. Si $x \in A$, on a évidemment $x \in (A \cup B) \cap (A \cup C)$; sinon, $x \in B \cap C$, donc

$$x \in B \subseteq A \cup B, \quad x \in C \subseteq A \cup C,$$

et x appartient encore au second membre de (2).

Inversement, soit $x \in A \cup B$ et $x \in A \cup C$. Si $x \in A$, $x \in A \cup (B \cap C)$; sinon, $x \in B$ et $x \in C$, donc $x \in B \cap C$ et, par conséquent, $x \in A \cup (B \cap C)$.

Considérons d'une façon générale une famille non vide

$$\mathcal{F} = \{M, \dots\} \subseteq \mathcal{P}(E)$$

de parties de E . L'intersection

$$I = \bigcap_{M \in \mathcal{F}} M$$

des parties M appartenant à $\mathcal{F}$ est, par définition, l'ensemble des éléments de E qui appartiennent à *tous* les ensembles $M \in \mathcal{F}$; on a donc

$$(3) \quad I \subseteq M \quad \text{pour tout } M \in \mathcal{F}.$$

De plus, X étant une partie de E ,

$$(4) \quad X \subseteq M \quad \text{pour tout } M \in \mathcal{F} \quad \text{entraîne } X \subseteq I.$$

Les deux propriétés précédentes sont caractéristiques, car si une partie I' de E les possède aussi, on a visiblement

$$I' \subseteq I \quad \text{et} \quad I \subseteq I';$$

elles définissent donc l'intersection à partir de l'inclusion.

De même, la réunion

$$R = \bigcup_{M \in \mathcal{F}} M,$$

ensemble des éléments de E qui appartiennent à l'une au moins des parties $M \in \mathcal{F}$ peut aussi être caractérisée par les deux propriétés :

$$(3') \quad M \subseteq R \quad \text{pour tout } M \in \mathcal{F}$$

et

$$(4') \quad M \subseteq Y \quad \text{pour tout } M \in \mathcal{F} \quad \text{entraîne } R \subseteq Y.$$

Désignons enfin par $\mathfrak{X}$ l'ensemble des X contenus dans tout $M \in \mathfrak{F}$, par $\mathfrak{Y}$ l'ensemble des Y contenant tout $M \in \mathfrak{F}$; nous avons

$$(5) \quad I = \bigcup_{X \in \mathfrak{X}} X,$$

$$(5') \quad R = \bigcap_{Y \in \mathfrak{Y}} Y,$$

Pour démontrer, par exemple, cette dernière formule, remarquons que $R \subseteq Y$ pour tout $Y \in \mathfrak{Y}$ entraîne, d'après (4),

$$R \subseteq \bigcap_{Y \in \mathfrak{Y}} Y;$$

d'autre part, on a, d'après (3'), $R \in \mathfrak{Y}$, donc

$$\bigcap_{Y \in \mathfrak{Y}} Y \subseteq R,$$

d'où l'égalité à établir. La formule duale (5) s'établit d'une façon analogue.

Si les ensembles $M \in \mathfrak{F}$ sont deux à deux *disjoints*, la réunion prend le nom de *somme*, et l'on écrit ⁽¹⁾

$$(6) \quad R = \sum_{M \in \mathfrak{F}} M.$$

Les parties M sont alors appelées *classes*, on dit que la relation (6) définit une *décomposition de R en classes*, ou une *partition* de R : tout élément de R appartient à une classe et à une seule.

Exercices. — 1. Démontrer les relations de distributivité généralisées

$$A \cap \left(\bigcup_{M \in \mathfrak{F}} M \right) = \bigcup_{M \in \mathfrak{F}} (A \cap M),$$

$$A \cup \left(\bigcap_{M \in \mathfrak{F}} M \right) = \bigcap_{M \in \mathfrak{F}} (A \cup M).$$

2. Le complément d'une réunion d'ensembles $M, M', \dots$ est l'intersection des

⁽¹⁾ Le terme de *somme* et la notation correspondante ont aussi été employés par certains auteurs dans le cas de la réunion ordinaire; nous les réserverons strictement au cas considéré dans le texte.

compléments de ces ensembles

$$E - \left(\bigcup_{M \in \mathcal{F}} M \right) = \bigcap_{M \in \mathcal{F}} (E - M).$$

Quel est le complément d'une intersection ?

3. Soient E un ensemble, k un nombre entier. Posons

$$n = 2k - 1, \quad s = C_n^k = \binom{n}{k}$$

où $C_n^k = \frac{n!}{k!(n-k)!}$ désigne le nombre des combinaisons de n objets k à k et considérons n parties $A_1, A_2, \dots, A_n$ de E . Formons

$$\begin{aligned} P_1 &= A_1 \cap A_2 \cap \dots \cap A_k, & \dots, & & P_s &= A_{n-k+1} \cap \dots \cap A_{n-1} \cap A_n; \\ Q_1 &= A_1 \cup A_2 \cup \dots \cup A_k, & \dots, & & Q_s &= A_{n-k+1} \cup \dots \cup A_{n-1} \cup A_n. \end{aligned}$$

Établir l'égalité ⁽¹⁾

$$\bigcup_{i=1, \dots, s} P_i = \bigcap_{j=1, \dots, s} Q_j,$$

Généralisation. — $A_1, \dots, A_n$ étant n parties quelconques de E , on a la même égalité, les P_i désignant toutes les intersections de k parties A , les Q_j toutes les réunions de l parties A , et k, l vérifiant

$$k + l = n + 1.$$

(On montrera que

$$k + l \geq n + 1 \quad \text{entraîne} \quad \bigcup P_i \subseteq \bigcap Q_j$$

tandis que

$$k + l \leq n + 1 \quad \text{entraîne} \quad \bigcap Q_j \subseteq \bigcup P_i.)$$

4. On appelle *différence symétrique* $D = A \circ B$ de deux parties A, B d'un ensemble E l'ensemble des éléments de E qui appartiennent à l'un des ensembles A, B sans appartenir à l'autre. Établir les formules

$$D = (A \cup B) - (A \cap B),$$

$$D = [A - (A \cap B)] \cup [B - (A \cap B)].$$

$$D \cap A = A - (A \cap B),$$

$$E - D = (A \cap B) + [E - (A \cup B)].$$

5. Si E a n éléments, $\mathcal{X}(E)$ en a 2^n . En déduire la formule

$$1 + C_n^1 + \dots + C_n^{n-1} + 1 = 2^n,$$

⁽¹⁾ Pour $n = 3$, cf. G. BIRKHOFF, *Lattice Theory*, p. 133 et 135. Pour n quelconque impair, cet exercice m'a été communiqué par M. D. S. Mitrovitch; la généralisation m'a été signalée par R. Croiset.

6. Soient P l'ensemble des points d'un plan, $\mathcal{F}$ la famille des carrés $C (\subset P)$ ayant un point donné O pour centre et un côté de longueur donnée a ; tous les points situés sur les côtés sont regardés comme des points du carré. Quels sont les deux ensembles

$$I = \bigcap_{C \in \mathcal{F}} C \quad \text{et} \quad R = \bigcup_{C \in \mathcal{F}} C ?$$

Même question en supposant que l'on retranche de chaque carré : a . ses sommets; b . les milieux des côtés; c . les côtés tout entiers.

B. — RELATIONS.

3. **Relations binaires; calcul des relations** ⁽¹⁾. — Certaines propositions mathématiques, particulièrement simples, expriment qu'un être x , élément d'un ensemble donné E , possède une propriété P (*exemple* : le nombre naturel 5 est impair). Une telle proposition signifie que x appartient à la partie A de E caractérisée par la propriété P :

$$x \in A.$$

En considérant maintenant deux propriétés P_1, P_2 portant sur un même être $x \in E$, on rencontre des propositions du type suivant, exprimant que la propriété P_1 *implique* ou *entraîne* la propriété P_2 ($P_1 \rightarrow P_2$) : tout $x \in E$ possédant la propriété P_1 possède aussi la propriété P_2 (*exemple* : tout nombre naturel multiple de 6 est pair). Une telle proposition signifie que la partie A_1 de E caractérisée par P_1 est contenue dans la partie A_2 caractérisée par P_2 :

$$A_1 \subseteq A_2.$$

Mais il arrive qu'une propriété P porte sur *deux* éléments x, y appartenant respectivement à deux ensembles E, F , qui peuvent d'ailleurs coïncider. On peut alors considérer que P porte sur le couple ordonné (x, y) , élément de l'ensemble-produit $E \times F$ et l'on est ainsi ramené au premier cas : les couples (x, y) ayant la propriété P forment une partie S_P de $E \times F$. En fait, il est souvent commode de dire que la propriété P définit, sur les ensembles E et F , une *relation binaire*, $\mathcal{R}$, qui est vérifiée par les couples (x, y) possédant la propriété P , et par ceux-là seulement, on écrit dans ce cas :

$$x \mathcal{R} y,$$

⁽¹⁾ On pourra consulter à ce sujet, J. RIGUET, *Relations binaires, fermetures, correspondances de Galois* (Bull. Soc. Math. de France, t. 76, 1948).

à moins que l'on ne remplace la lettre $\mathcal{R}$ par un symbole spécial, ce qui est fréquent. L'ensemble $S_{\mathcal{R}}$ est appelé *ensemble représentatif* de la relation $\mathcal{R}$ dans l'ensemble-produit, et désigné encore par $S_{\mathcal{R}}$; on a donc, par définition,

$$(1) \quad x \mathcal{R} y \Leftrightarrow (x, y) \in S_{\mathcal{R}};$$

Si F coïncide avec E , on dit que $\mathcal{R}$ est une *relation binaire définie dans l'ensemble E* .

Exemples. — 1a. Le nombre naturel x divise le nombre naturel y : $x|y$ (on a ici $E = F = \mathbb{N}$, ensemble des nombres naturels).

1b. Les nombres naturels x, y sont premiers entre-eux.

2a. Le nombre réel x est plus petit que le nombre réel y : $x < y$ ($E = F = \mathbb{P}$, ensemble des nombres réels).

2b. Le nombre réel y est le carré du nombre réel x : $y = x^2$.

3. La droite x est parallèle au plan y : $x // y$ (E est l'ensemble des droites de l'espace, F celui des plans).

4a. La droite x est perpendiculaire à la droite y , sans nécessairement la rencontrer : $x \perp y$ ($E = F$ est l'ensemble des droites de l'espace).

4b. La droite x rencontre orthogonalement la droite y : $x \perp y$.

5a. La droite x coupe la sphère y : $x \cap y$ (on se place dans le domaine réel, E est l'ensemble des droites de l'espace, F celui des sphères). Plus généralement, on peut considérer la même relation $x \cap y$ entre les éléments de deux familles E, F de parties d'un même ensemble.

5. La droite x est orthogonale à la sphère y (passe par son centre) : $x \odot y$.

Les exemples précédents suffisent à montrer l'intérêt que présente la notion de relation, bien que, logiquement, elle dérive des notions fondamentales de *partie* et d'*ensemble-produit*. L'exemple 2b suggère que la représentation d'une relation comprend comme cas particulier la représentation graphique des fonctions. D'une façon générale, le *calcul des relations* que nous allons étudier, se rattache étroitement à la définition ensembliste (1).

La *relation vide* est celle qui n'est vérifiée par aucun couple : son ensemble représentatif est vide. La *relation universelle* ou *absolue* est celle qui est vérifiée par tous les couples (x, y) : son ensemble représentatif est $E \times F$.

La *négation* $\mathcal{R}'$ de $\mathcal{R}$ est la relation vérifiée par les couples (x, y) qui ne vérifient pas $\mathcal{R}$, et ceux-là seulement. L'ensemble représentatif de $\mathcal{R}'$ est le complément de celui de $\mathcal{R}$.

La relation *inverse* $\mathcal{R}^{-1}$ de $\mathcal{R}$ est la relation binaire définie sur F et E par

$$y \mathcal{R}^{-1} x \Leftrightarrow x \mathcal{R} y.$$

On a

$$(\mathcal{R}^{-1})^{-1} = \mathcal{R}.$$

Les ensembles E, F étant donnés, à l'égalité, à l'inclusion, à l'intersection et à la réunion des parties de $E \times F$ (regardées comme ensembles représentatifs) correspondent l'égalité, l'inclusion, l'intersection et la réunion des relations binaires définies sur E et F . On aura $\mathcal{R} = \mathcal{R}_1$ si $\mathcal{S}_{\mathcal{R}} = \mathcal{S}_{\mathcal{R}_1}$, c'est-à-dire si $\mathcal{R}$ et $\mathcal{R}_1$ sont vérifiées par les mêmes couples, $\mathcal{R} \subseteq \mathcal{R}_1$ (ou $\mathcal{R} \Rightarrow \mathcal{R}_1$) si $\mathcal{S}_{\mathcal{R}} \subseteq \mathcal{S}_{\mathcal{R}_1}$, donc si $x\mathcal{R}y$ entraîne $x\mathcal{R}_1y$: on dira alors que $\mathcal{R}$ est contenue dans $\mathcal{R}_1$ ou plus fine que $\mathcal{R}_1$; si $\mathcal{R}$ et $\mathcal{R}_1$ sont distinctes, on écrira $\subset$ au lieu de $\subseteq$ et l'inclusion sera dite stricte.

L'intersection $\mathcal{I} = \mathcal{R}_1 \cap \mathcal{R}_2$ de deux relations $\mathcal{R}_1, \mathcal{R}_2$ est celle qui a pour ensemble représentatif l'intersection $\mathcal{S}_{\mathcal{R}_1} \cap \mathcal{S}_{\mathcal{R}_2}$:

$$x\mathcal{I}y \Leftrightarrow x\mathcal{R}_1y \ \& \ x\mathcal{R}_2y.$$

D'une façon générale, l'intersection $\mathcal{I} = \bigcap_{\mathcal{R} \in \Phi} \mathcal{R}$ d'une famille Φ de relation $\mathcal{R}$ définies sur E et F est la relation vérifiée par les couples qui vérifient chacune des relations $\mathcal{R} \in \Phi$.

On définit, de même, la réunion $\mathcal{R}_1 \cup \mathcal{R}_2$ de deux relations, ou la réunion $\bigcup_{\mathcal{R} \in \Phi} \mathcal{R}$ d'une famille de relations, en remplaçant $\&$ par ou, « chacune » par « une au moins ».

Exemples. — 1 (cf. 3a et 3b). E étant l'ensemble des droites de l'espace, F celui des sphères, la relation $\perp\!\!\!\perp$ (« est orthogonale à ») est plus fine que $\perp$ (« coupe ») : $\perp\!\!\!\perp \subset \perp$.

2 (cf. 4a et 4b). $E = F$ étant l'ensemble des droites de l'espace, la relation $\perp$ (« rencontre orthogonalement ») est plus fine que $\perp\!\!\!\perp$ (« est perpendiculaire à ») : $\perp \subset \perp\!\!\!\perp$. On a : $\perp = \perp\!\!\!\perp \cap \perp\!\!\!\perp$.

3. Soit $E = F = C$, où $C = \{ \dots, -m, \dots, -1, 0, 1, 2, \dots, n, \dots \}$ est l'ensemble des entiers positifs, négatifs ou nuls, ou entiers relatifs. Soit $\mathcal{R}_m$ la congruence arithmétique modulo m , définie par

$$x\mathcal{R}_m y \Leftrightarrow x - y = km \quad (k \in C).$$

Soit Φ la famille des congruences obtenues en faisant décrire à m l'ensemble P des nombres premiers p . L'intersection $\mathcal{I} = \bigcap_{p \in P} \mathcal{R}_p$ est l'égalité, puisque tout élément de C non nul n'a qu'un nombre fini de diviseurs premiers.

Soit x un élément de E : on appelle coupe de $\mathcal{R}$ suivant x et l'on

désigne par $\mathcal{R}(x)$ l'ensemble des $y \in F$ vérifiant $x\mathcal{R}y$. $\mathcal{R}^{-1}(y)$ est, de même, l'ensemble des $x \in E$ vérifiant $x\mathcal{R}y$, où y est un élément donné de F . A une partie non vide quelconque X de E sont associées la *coupe de première espèce* $\mathcal{R}(X)$ de $\mathcal{R}$ suivant X , définie par

$$\mathcal{R}(X) = \bigcup_{x \in X} \mathcal{R}(x)$$

et la *coupe de seconde espèce* $\mathcal{R}[X]$ définie par

$$\mathcal{R}[X] = \bigcap_{x \in X} \mathcal{R}(x).$$

$\mathcal{R}(E)$, ensemble des $y \in F$ pour lesquelles existe au moins un $x \in X$ tel que l'on ait $x\mathcal{R}y$, est appelé *projection* de $\mathcal{R}$ sur F ou (notamment si $E = F$) *deuxième projection* de $\mathcal{R}$; on écrit

$$\mathcal{R}(E) = \text{pr}_F \mathcal{R} \quad \text{ou} \quad \text{pr}_2 \mathcal{R}.$$

L'ensemble analogue des $x \in E$ pour lesquels existe au moins un $y \in F$ tel que $x\mathcal{R}y$, n'est autre que $\mathcal{R}^{-1}(F)$; on l'appelle *projection* de $\mathcal{R}$ sur E , ou (si $E = F$) *première projection* de $\mathcal{R}$:

$$\mathcal{R}^{-1}(F) = \text{pr}_E \mathcal{R} \quad \text{ou} \quad \text{pr}_1 \mathcal{R}.$$

On a, d'après les définitions,

$$\mathcal{R}(X_1 \cup X_2) = \mathcal{R}(X_1) \cup \mathcal{R}(X_2), \quad \mathcal{R}[X_1 \cup X_2] = \mathcal{R}[X_1] \cap \mathcal{R}[X_2].$$

D'autre part, l'inclusion $A \subseteq B$ entraîne

$$\mathcal{R}(A) \subseteq \mathcal{R}(B), \quad \mathcal{R}[A] \supseteq \mathcal{R}[B],$$

d'où

$$\mathcal{R}(X_1 \cap X_2) \subseteq \mathcal{R}(X_1) \cap \mathcal{R}(X_2), \quad \mathcal{R}[X_1 \cap X_2] \supseteq \mathcal{R}[X_1] \cup \mathcal{R}[X_2].$$

L'égalité n'a pas lieu en général.

Exemples. — 1. Soit $E = F = \mathbf{P}$, ensemble des nombres réels; prenons comme relation $\mathcal{R}$ la relation $<$ (cf. ex. 2a, p. 11).

$\mathcal{R}(x)$ est l'ensemble des $y > x$ (demi-droite); si X est, par exemple, l'intervalle (a, b) , c'est-à-dire l'ensemble des nombres réels compris strictement entre a et b ($a < b$), on a

$$\mathcal{R}(X) = \{y\}_{a < y}, \quad \mathcal{R}[X] = \{y\}_{y \geq b}.$$

2. Avec toujours $E = F = \mathbf{P}$, considérons la relation $\mathcal{R}$ définie par

$$x\mathcal{R}y \Leftrightarrow y = x^2 \quad (\text{cf. ex. 2b, p. 11}).$$

On a $\text{pr}_1 \mathcal{R} = E$, tandis que $\text{pr}_2 \mathcal{R}$ est l'ensemble des nombres réels positifs ou nuls.

Si nous prenons pour X_1 et X_2 les segments $[-1, 0]$ et $[0, 1]$, ensembles des x_1, x_2 vérifiant respectivement $-1 \leq x_1 \leq 0, 0 \leq x_2 \leq 1$, nous avons

$$\begin{aligned}\mathcal{R}(X_1) &= \mathcal{R}(X_2) = [0, 1], & \mathcal{R}[X_1] &= \mathcal{R}[X_2] = \emptyset, \\ X_1 \cap X_2 &= \{0\}, \\ \mathcal{R}(0) &= \mathcal{R}[0] = \{0\},\end{aligned}$$

donc

$$\mathcal{R}(X_1 \cap X_2) \subset \mathcal{R}(X_1) \cap \mathcal{R}(X_2), \quad \mathcal{R}[X_1 \cap X_2] \supset \mathcal{R}[X_1] \cup \mathcal{R}[X_2].$$

Soient E, F, G des ensembles (distincts ou non), $\mathcal{R}$ une relation binaire définie sur E et F , $\mathcal{S}$ une relation binaire définie sur F et G . La *relation-produit* ou *relation composée* $\mathcal{R}\mathcal{S}$ (ou $\mathcal{R} \circ \mathcal{S}$) est la relation binaire définie sur E et G de la façon suivante : $x \in E$ et $z \in G$ vérifient $\mathcal{R}\mathcal{S}$ si et seulement s'il existe au moins un élément $y \in F$ tel que (x, y) vérifie $\mathcal{R}$ et (y, z) vérifie $\mathcal{S}$:

$$x\mathcal{R}\mathcal{S}z \Leftrightarrow \exists y \in F, \quad x\mathcal{R}y \text{ \& \& } y\mathcal{S}z$$

$\mathcal{R} \subseteq \mathcal{R}_1$ entraîne $\mathcal{R}\mathcal{S} \subseteq \mathcal{R}_1\mathcal{S}$; $\mathcal{S} \subseteq \mathcal{S}_1$ entraîne $\mathcal{R}\mathcal{S} \subseteq \mathcal{R}\mathcal{S}_1$. Les deux hypothèses entraînent donc $\mathcal{R}\mathcal{S} \subseteq \mathcal{R}_1\mathcal{S}_1$.

Si H est un nouvel ensemble, et $\mathfrak{S}$ une relation binaire définie sur G et H , on a immédiatement, d'après les définitions,

$$\mathcal{R}(\mathcal{S}\mathfrak{S}) = (\mathcal{R}\mathcal{S})\mathfrak{S}.$$

Cette relation est valable, en particulier, quand les ensembles H, G, F sont confondus avec E et signifie alors que le produit des relations binaires dans E est *associatif* : par suite, la puissance n -ième $\mathcal{R}^n$ d'une relation $\mathcal{R}$ possède une signification claire.

Exemples. — 1. Prenons comme ensembles E, F, G respectivement l'ensemble des points, celui des droites et celui des plans de l'espace; la relation $\mathcal{R}$, « le point x est sur la droite y », et la relation $\mathcal{S}$, « la droite y est dans le plan z », ont pour produit $\mathcal{R}\mathcal{S}$, « le point x est dans le plan z ».

2. Soit maintenant $G = F = E$, ensemble des points de l'espace. Donnons-nous deux directions distinctes δ_1, δ_2 et considérons les relations binaires $\mathcal{R}_1, \mathcal{R}_2$ définies dans E par $x\mathcal{R}_i y$ si x, y sont confondus ou si, étant distincts, ils déterminent une droite parallèle à δ_i ($i = 1, 2$).

La relation-produit $\mathcal{R}_1\mathcal{R}_2$ n'est autre que la relation $\mathcal{X}$ définie par : $x\mathcal{X}z$ si x, z sont confondus ou si, étant distincts, ils déterminent une droite parallèle à la direction de plan contenant δ_1, δ_2 . On remarquera qu'ici la relation $\mathcal{R}_2\mathcal{R}_1$ coïncide également avec $\mathcal{X}$.

Soient $\mathcal{R}$ une relation binaire définie sur E et F , et A, B respective-

ment des parties de E et de F : $A \subseteq E$, $B \subseteq F$; la relation $\mathcal{R}$ envisagée seulement pour les couples (a, b) , où $a \in A$, $b \in B$, est une relation binaire définie sur A et B , appelée *trace* de $\mathcal{R}$ sur A et B et désignée par $\mathcal{R}_{A,B}$ (on dit aussi que $\mathcal{R}_{A,B}$ est la relation $\mathcal{R}$ limitée ou restreinte à A et B , ou la restriction de $\mathcal{R}$ à ces ensembles). L'ensemble représentatif de $\mathcal{R}_{A,B}$ est l'intersection $\mathcal{S}_{\mathcal{R}} \cap (A \times B)$.

Si $E = F$ et $A = B$, la trace $\mathcal{R}_{A,A}$ est désignée, pour simplifier, par $\mathcal{R}_A$ et appelée, brièvement, trace de $\mathcal{R}$ sur A .

Exemples. — 1. Supposons que E, F soient tous deux l'ensemble des points de l'espace et que, O désignant un point fixe, $x \mathcal{R} y$ signifie : x et y sont situés sur une droite passant par O . Si A et B sont deux plans ne contenant pas O , $\mathcal{R}_{A,B}$ est la *projection centrale* de A sur B faite à partir de O . On considère également en Géométrie, la projection centrale ou perspective $\mathcal{R}'_{E,B}$, E' désignant l'espace E privé du point O : $E' = E - \{O\}$.

2. Soit P l'ensemble des droites d'un plan. Les traces $\perp_P$ et $\lrcorner_P$ des relations binaires $\perp$, $\lrcorner$ définies précédemment dans l'ensemble $E(=F)$ des droites de l'espace, se confondent avec la perpendicularité dans le plan considéré.

Étudions maintenant les *relations binaires dans un ensemble* E , ($F = E$). L'égalité $\mathcal{E}$ dans E est la relation

$$x \mathcal{E} y \quad \text{ou} \quad x = y$$

exprimant que x et y sont un seul et même élément de E ; sa négation

$$x \mathcal{E}' y \quad \text{ou} \quad x \neq y$$

exprime que x et y sont *distincts*. L'ensemble représentatif de l'égalité est la *diagonale* $\{(x, x)\}_{x \in E}$, c'est-à-dire l'ensemble des couples (x, x) où x décrit E .

Si $\mathcal{R}$ est une relation binaire quelconque dans E , on a

$$\mathcal{R} \mathcal{E} = \mathcal{R}, \quad \mathcal{E} \mathcal{R} = \mathcal{R}.$$

Une relation $\mathcal{R}$ définie dans E est dite :

Réflexive si l'on a

$$x \mathcal{R} x \quad \text{pour tout } x \in E, \quad \text{c'est-à-dire} \quad \mathcal{E} \subseteq \mathcal{R};$$

Symétrique (ou *réciproque*) si

$$x \mathcal{R} y \quad \text{entraîne} \quad y \mathcal{R} x, \quad \text{c'est-à-dire} \quad \mathcal{R} \subseteq \mathcal{R}^{-1} \quad (\text{d'où l'égalité } \mathcal{R}^{-1} = \mathcal{R});$$

Propre (ou *antisymétrique*) si

$$x \mathcal{R} y \quad \text{et} \quad y \mathcal{R} x \quad \text{entraînent} \quad x = y, \quad \text{c'est-à-dire} \quad \mathcal{R} \cap \mathcal{R}^{-1} \subseteq \mathcal{E};$$

Transitive si

$x\mathcal{R}y$ et $y\mathcal{R}z$ entraînent $x\mathcal{R}z$, c'est-à-dire $\mathcal{R}^2 \subseteq \mathcal{R}$.

Si $\mathcal{R}$ a l'une des propriétés précédentes, $\mathcal{R}^{-1}$ la possède aussi. Si toutes les relations d'une famille Φ ont l'une quelconque des propriétés précédentes, leur intersection la possède aussi.

Exemples. — 1. L'égalité est réflexive, symétrique et transitive. De même, la relation $x // y$ dans l'ensemble des droites du plan ou de l'espace; de même encore la congruence arithmétique $\mathcal{R}_m$ dans l'ensemble $\mathbb{C}$ des entiers relatifs.

2. La relation $x \parallel y$, dans l'ensemble des droites de l'espace, est réflexive. Elle ne l'est pas dans l'ensemble des parties $\mathcal{P}(\mu)$ d'un ensemble μ , car la partie vide ne se coupe pas elle-même. Dans un cas comme dans l'autre, cette relation est symétrique. Elle n'est pas transitive, sauf s'il s'agit de l'ensemble des parties $\mathcal{P}(\mu)$ d'un ensemble μ réduit à *un seul* élément : $\mu = \{x\}$.

3. Les relations $x \perp y$, $x \bot y$, dans l'ensemble des droites de l'espace, sont symétriques. Elles ne sont ni réflexives, ni transitives.

4. La relation $x|y$ (x divise y), dans l'ensemble $\mathbb{N}$ des entiers naturels, est réflexive et transitive; elle n'est pas symétrique. La relation $x \leq y$ dans l'ensemble $\mathbb{P}$ des nombres réels a également ces propriétés.

Soient $\mathcal{R}$ et $\mathcal{S}$ deux relations binaires définies dans le même ensemble $E(=F)$. On dit que $\mathcal{R}$ *respecte* $\mathcal{S}$ à gauche ou que $\mathcal{S}$ *absorbe* $\mathcal{R}$ à droite si l'on a

$$(2) \quad \mathcal{R}\mathcal{S} \subseteq \mathcal{S}.$$

De même, $\mathcal{R}$ *respecte* $\mathcal{S}$ à droite, ou $\mathcal{S}$ *absorbe* $\mathcal{R}$ à gauche si l'on a

$$(2') \quad \mathcal{S}\mathcal{R} \subseteq \mathcal{S}.$$

On dira enfin que $\mathcal{R}$ *respecte* $\mathcal{S}$ ou que $\mathcal{S}$ *absorbe* $\mathcal{R}$ si l'on a simultanément les propriétés (2) et (2').

Si $\mathcal{R}$ est réflexive, on a, quelle que soit $\mathcal{S}$,

$$\mathcal{S} \subseteq \mathcal{R}\mathcal{S}, \quad \mathcal{S} \subseteq \mathcal{S}\mathcal{R},$$

car, par exemple, $x\mathcal{S}y$ entraîne $x\mathcal{R}x$ et $x\mathcal{S}y$. Les propriétés (2) et (2') entraînent alors les égalités

$$(3) \quad \mathcal{S} = \mathcal{R}\mathcal{S} = \mathcal{S}\mathcal{R} = \mathcal{R}\mathcal{S}\mathcal{R}.$$

Si $\mathcal{S}$ est transitive, toute relation $\mathcal{R}$ qu'elle contient la respecte : $\mathcal{R} \subseteq \mathcal{S}$ entraîne, en effet,

$$\mathcal{R}\mathcal{S} \subseteq \mathcal{S}^2 \subseteq \mathcal{S}, \quad \mathcal{S}\mathcal{R} \subseteq \mathcal{S}^2 \subseteq \mathcal{S}.$$

Parmi les relations transitives, on distingue notamment les relations d'ordre et les relations d'équivalence.

4. Relations d'ordre. — Une *relation d'ordre partiel* est une relation $\mathcal{R}$ réflexive, propre et transitive ⁽¹⁾. On utilise généralement l'une des notations $\subseteq$, $\leq$, $\preceq$, ou l'un des symboles symétriques $\supseteq$, $\geq$, $\succeq$ et $x\mathcal{R}y$ s'énonce : x contenu dans y , inférieur ou égal à y , antérieur ou égal à y , — ou symétriquement.

$\mathcal{R}^{-1}$ est une relation d'ordre partiel en même temps que $\mathcal{R}$; toute intersection de relations d'ordre partiel est une relation d'ordre partiel. Un ensemble E où a été définie une relation d'ordre partiel est dit *partiellement ordonné* par cette relation; deux éléments x, y de E sont *comparables* si l'on a $x\mathcal{R}y$ ou $y\mathcal{R}x$.

Exemples. — 1. L'ensemble des parties $\mathcal{P}(M)$ d'un ensemble M est partiellement ordonné par la relation d'inclusion. L'inclusion des relations binaires sur deux ensembles E, F est également une relation d'ordre partiel.

2. La relation $x|y$ (x divise y) dans l'ensemble N des nombres naturels est une relation d'ordre partiel; 3 et 6 sont comparables, 2 et 3 ne le sont pas.

L'intersection $\mathcal{R}^* = \mathcal{R} \cap \mathcal{E}'$ d'une relation d'ordre partiel avec la négation $\mathcal{E}'$ de l'égalité est ce que l'on appelle la relation d'ordre partiel *stricte* (ou *forte*) associée à $\mathcal{R}$; on la note généralement $\subset$ ou $<$. $\mathcal{R}^*$ est *contenue dans* $\mathcal{E}'$, *incompatible avec son inverse* (car $\mathcal{R}^* \subseteq \mathcal{R}$ entraîne $\mathcal{R}^{*-1} \subseteq \mathcal{R}^{-1}$, donc $\mathcal{R}^* \cap \mathcal{R}^{*-1} \subseteq \mathcal{R} \cap \mathcal{R}^{-1} \subseteq \mathcal{E}$, alors que $\mathcal{R}^* \cap \mathcal{R}^{*-1} \subseteq \mathcal{R}^* \subseteq \mathcal{E}'$) et *transitive* (car $x\mathcal{R}^*y$ et $y\mathcal{R}^*z$ entraînent $x\mathcal{R}z$, et $x = z$ est impossible puisqu'on aurait $x\mathcal{R}^*y$ et $y\mathcal{R}^*x$).

Inversement, si $\mathcal{R}^*$ est une relation *contenue dans* $\mathcal{E}'$, *incompatible avec son inverse* et *transitive*, la relation $\mathcal{R} = \mathcal{R}^* \cup \mathcal{E}$ est une relation d'ordre partiel : $\mathcal{R}$ est, en effet, réflexive, propre (car $x\mathcal{R}^*y$ et $y\mathcal{R}^*x$ étant incompatibles, $x\mathcal{R}y$ et $y\mathcal{R}x$ entraînent $x = y$) et transitive, comme on le voit immédiatement. On dit que $\mathcal{R}$ est la relation d'ordre partiel *faible* associée à la relation stricte $\mathcal{R}^*$.

Les exemples donnés plus haut montrent que, dans un ensemble partiellement ordonné, il existe en général des couples d'éléments non comparables. Si, au contraire, deux éléments sont toujours comparables, donc si l'on a, $\mathcal{U}$ désignant la relation universelle,

$$\mathcal{R} \cup \mathcal{R}^{-1} = \mathcal{U} \quad (\text{ou } \mathcal{R}^* \cup \mathcal{E} \cup \mathcal{R}^{*-1} = \mathcal{U}),$$

(1) Cette définition est celle de G. BIRKHOFF, *Lattice Theory* (Amer. Math. Soc. Coll. Publ., vol. 25, 1948, p. 1). Certains auteurs appellent *relation d'ordre partiel* ou même *relation d'ordre* toute relation transitive. Ces définitions paraissent trop faibles, car elles s'appliquent à la relation universelle à laquelle, manifestement, n'est associée aucune idée d'ordre. Toutefois, il est commode de donner le nom de *quasi-ordre*. (G. BIRKHOFF, *ibid.*, p. 4) ou de *préordre* à une relation *réflexive et transitive*.

on dit que $\mathcal{R}$, ou $\mathcal{R}^*$, est une relation d'ordre *total* (ou *simple*) et que l'ensemble E est *totale*ment (ou *simple*ment) *ordonné*. On emploie alors généralement, pour $\mathcal{R}$ et $\mathcal{R}^*$ les symboles respectifs $\leq$ et $<$, ou les symboles symétriques $\geq$, $>$.

D'après ce qui précède, une relation d'ordre total stricte $<$, possède les deux propriétés suivantes :

1° Elle est *transitive*;

2° Pour chaque couple d'éléments x, y de E , on a l'une des trois propriétés

$$x < y, \quad x = y, \quad y < x,$$

à l'exclusion des deux autres ⁽¹⁾.

Les propriétés 1° et 2° sont caractéristiques, car 2° équivaut à

$$\begin{aligned} \mathcal{R}^* \cup \mathcal{E}' \cup \mathcal{R}^{*-1} &= \mathcal{U}, \\ \mathcal{R}^* \cap \mathcal{R}^{*-1} &= \emptyset = \mathcal{R}^* \cap \mathcal{E}, \end{aligned}$$

d'où $\mathcal{R}^* \subseteq \mathcal{E}'$; $\mathcal{R}^*$, contenue dans $\mathcal{E}'$, incompatible avec son inverse, et transitive est bien une relation d'ordre total stricte.

Exemples. — 1. L'alphabet est un ensemble *totale*ment ordonné (ordre alphabétique)

$$a < b < c < \dots < z.$$

2. L'ensemble N des nombres naturels, l'ensemble P des nombres réels sont ordonnés *totale*ment par les relations $\leq$ ou $<$ au sens habituel « inférieur ou égal », « plus petit que »).

Nous développerons un peu plus loin (§ 9, 10), l'étude des ensembles ordonnés, *partiellement* ou *totale*ment.

5. Relations d'équivalence. — On donne le nom de *relation d'équivalence*, d'*équivalence* (ou d'*égalité généralisée*) à toute relation qui est à la fois *réflexive*, *symétrique* et *transitive*. L'égalité est une équivalence, la relation universelle $\mathcal{U}$ également (pour cette raison, $\mathcal{U}$ est appelée souvent *équivalence universelle* ou *absolue*).

Exemples. — 1. Dans l'ensemble E des droites (du plan ou de l'espace) la relation $x // y$, « x est parallèle à y », est une équivalence.

2. Dans l'ensemble C des entiers relatifs, la congruence modulo m , $\mathcal{R}_m$, est une équivalence.

(1) Dans la première édition, nous appelions *relation d'ordre*, sans plus, une relation d'ordre total stricte.

Par analogie avec les congruences arithmétiques et pour distinguer les équivalences des relations quelconques, nous adopterons, pour toute équivalence $\mathcal{R}$, la notation

$$x \equiv y \ (\mathcal{R})$$

« x équivalent à y modulo $\mathcal{R}$ ».

THÉOREME 1. — 1° *A toute décomposition d'un ensemble E en classes X*

$$E = \sum X$$

correspond une équivalence, $\mathcal{R}$, définie par

$$x \mathcal{R} x_1 \Leftrightarrow x \ \& \ x_1 \text{ appartiennent à la même classe.}$$

2° *Inversement, à toute équivalence $\mathcal{R}$ définie dans E correspond une décomposition de E en classes, la classe X contenant un élément x étant la coupe $\mathcal{R}(x)$, c'est-à-dire l'ensemble des éléments de E équivalents à x , modulo $\mathcal{R}$.*

1° Puisqu'un élément x appartient à une classe et à une seule, la relation $\mathcal{R}$ définie dans la première partie de l'énoncé, est réflexive, symétrique et transitive : c'est une équivalence.

2° Puisque l'équivalence donnée $\mathcal{R}$ est une relation réflexive, tout élément x de E appartient à $\mathcal{R}(x)$: on a donc

$$\bigcup_{x \in E} \mathcal{R}(x) = E.$$

Si $x_1 \in \mathcal{R}(x)$, on a, puisque $\mathcal{R}$ est symétrique, $x \in \mathcal{R}(x_1)$ et, puisque $\mathcal{R}$ est transitive, $\mathcal{R}(x_1) \subseteq \mathcal{R}(x)$, mais aussi, en raison de la symétrie, $\mathcal{R}(x) \subseteq \mathcal{R}(x_1)$, d'où l'égalité. Plus généralement, les ensembles $\mathcal{R}(x)$ et $\mathcal{R}(z)$ coïncident dès qu'ils se coupent, puisque

$$y \in \mathcal{R}(x) \cap \mathcal{R}(z) \quad \text{entraîne} \quad \mathcal{R}(x) = \mathcal{R}(y) = \mathcal{R}(z).$$

Les ensembles $\mathcal{R}(x)$ distincts, $A, B, \dots, X, \dots$ sont donc deux à deux disjoints, et leur somme, qui coïncide avec la réunion de tous les $\mathcal{R}(x)$, n'est autre que E : on a bien une décomposition de E en classes, et il est clair que l'équivalence correspondant à cette décomposition n'est autre que $\mathcal{R}$.

L'ensemble $\mathcal{Q}$ des classes modulo $\mathcal{R}$, qui peut être regardé comme

une partie de $\mathfrak{E}(E)$, est appelé *ensemble-quotient* de E par $\mathcal{R}$. On écrit

$$(1) \quad \mathbf{Q} = E/\mathcal{R},$$

$$(2) \quad E = \sum_{x \in \mathbf{Q}} X.$$

A la décomposition (2), on associe souvent un *système de représentants*, S , c'est-à-dire un sous-ensemble $S = \{a, b, \dots, x, \dots\}$ de E tel qu'il y ait un élément de S et un seul contenu dans chaque classe modulo $\mathcal{R}$.

Exemples. — 1. A l'égalité correspond une décomposition dans laquelle chaque classe contient un seul élément. L'autre cas extrême est celui de l'équivalence absolue : l'ensemble-quotient se compose d'une seule classe, E .

2. Dans le cas de la congruence arithmétique $\mathcal{R}_m$ modulo m , les classes sont les différentes progressions arithmétiques de raison m : on les appelle *classes résiduelles modulo m* ; l'ensemble-quotient, appelé *ensemble des classes résiduelles modulo m* et désigné par $C/(m)$, a des propriétés variables suivant la nature arithmétique du nombre m , sur lesquelles nous reviendrons plus loin (chap. IV, § 9, p. 180). On prend ordinairement dans chaque classe résiduelle le reste lui-même comme représentant, ce qui conduit à désigner ces m classes par les symboles $0, 1, \dots, m-1$.

3. Dans l'ensemble des droites de l'espace, le parallélisme est, comme nous l'avons vu, une équivalence : les classes correspondantes sont, par définition, les *directions*. On prend généralement comme représentant d'une direction la droite appartenant à cette direction et passant par un point O choisi une fois pour toutes.

On définit de même les *directions de plans* comme classes formées par tous les plans parallèles entre eux.

4. Par *segment* ou *vecteur lié*, on entend (toujours dans l'espace euclidien) la portion de droite comprise entre deux points A et B de cette droite, pris dans l'ordre A, B : A est l'*origine*, B l'*extrémité* du segment. Deux segments sont *égaux* (au sens strict que nous donnons à ce mot) s'ils ont même origine et même extrémité, et dans ce cas seulement. Dans l'ensemble E des segments, considérons les deux équivalences suivantes :

$$AB \mathcal{R}_1 A'B'$$

si les segments $AB, A'B'$ ont même support, même sens, même longueur. Les classes modulo $\mathcal{R}_1$ sont, par définition, les *vecteurs glissants* ;

$$AB \mathcal{R}_2 A'B'$$

si les segments $AB, A'B'$ ont même direction, même sens, même longueur : on dit alors qu'ils sont *équipollents*. Les classes modulo $\mathcal{R}_2$ sont, par définition, les *vecteurs libres*. On représente souvent un vecteur libre $\vec{V}$ par le segment OM qui a pour origine un point O choisi une fois pour toutes, et appartient à la

classe $\vec{V}$; on écrit alors

$$\vec{V} = \vec{OM}.$$

On voit que le passage d'un ensemble E à l'ensemble-quotient $E/\mathcal{R}$ modulo une équivalence $\mathcal{R}$, permet de définir, sous forme de classes, de nouveaux êtres mathématiques; ce procédé de contraction est d'un emploi fréquent et d'une grande importance.

Une partie A non vide d'un ensemble E est dite *indivisible* par rapport à une équivalence $\mathcal{R}$ définie dans E , ou *$\mathcal{R}$ -indivisible*, si A est contenue dans une seule classe modulo $\mathcal{R}$. Une partie B est dite *saturée* par rapport à $\mathcal{R}$, ou *$\mathcal{R}$ -saturée*, si elle est une réunion de classes modulo $\mathcal{R}$.

Soit X une partie quelconque : la réunion des classes modulo $\mathcal{R}$ qui contiennent au moins un élément x de X , est la plus petite partie saturée de E contenant X : on l'appelle l'*extension saturée* ⁽¹⁾ de X par $\mathcal{R}$ et on la désigne par $\mathcal{R}(X)$ ou $\bar{X}$. $X \subseteq Y$ entraîne $\bar{X} \subseteq \bar{Y}$.

Les classes sont les parties à la fois indivisibles et saturées.

Toute réunion de parties saturées est saturée; toute intersection non vide de parties indivisibles est indivisible.

L'extension saturée $\bar{R}$ de la réunion R d'une famille de parties $\mathcal{F} = \{X, \dots\}$ est la réunion des extensions saturées $\bar{X}$ de ces parties; en effet, $X \subseteq R$ entraîne $\bar{X} \subseteq \bar{R}$, d'où

$$\bigcup_{X \in \mathcal{F}} \bar{X} \subseteq \bar{R}.$$

Inversement, si $r \in \bar{R}$, on a $r \equiv x(\mathcal{R})$, où $x \in R$, donc $x \in X$ pour au moins un $X \in \mathcal{F}$; mais alors $r \in \bar{X}$, d'où

$$\bar{R} \subseteq \bigcup_{X \in \mathcal{F}} \bar{X},$$

et l'égalité.

Si nous considérons maintenant une intersection $I = \bigcap_{X \in \mathcal{F}} X$, $I \subseteq X$ entraîne $\bar{I} \subseteq \bar{X}$ pour tout $X \in \mathcal{F}$, d'où

$$\bar{I} \subseteq \bigcap_{X \in \mathcal{F}} \bar{X};$$

mais ici, on n'a pas nécessairement l'égalité.

(1) Cette extension saturée n'est autre que la coupe de première espèce (voir § 3, p. 13).

Exemple. — Dans l'espace euclidien considéré comme ensemble de ses points et où l'on donne une direction Δ , soit $\mathcal{R}$ l'équivalence définie par $x\mathcal{R}y$ si x et y sont confondus ou si la droite xy est parallèle à Δ .

Un segment parallèle à Δ est indivisible. Un cylindre de génératrices parallèles à Δ est saturé. L'extension saturée d'une droite D non parallèle à Δ est le plan $\bar{D}$ parallèle à Δ passant par D . Si D_1, D_2 sont deux droites non parallèles à Δ et non coplanaires, on a $I = D_1 \cap D_2 = \emptyset$, $\bar{I} = \emptyset$, tandis que $\bar{D}_1 \cap \bar{D}_2$ est la parallèle à Δ s'appuyant sur D_1 et D_2 :

$$\bar{I} \subset \bigcap_{k=1,2} \bar{D}_k.$$

Considérons, dans un ensemble E , une équivalence $\mathcal{R}$. A une relation $\mathcal{S}$, définie dans E , associons dans l'ensemble-quotient $Q = E/\mathcal{R}$ les deux relations $\bar{\mathcal{S}}_0, \bar{\mathcal{S}}_1$ définies respectivement par :

$X\bar{\mathcal{S}}_0Y$ si l'on a $x\mathcal{S}y$ pour tout $x \in X$ et tout $y \in Y$;

$X\bar{\mathcal{S}}_1Y$ s'il existe $x \in X$ et $y \in Y$ tels que $x\mathcal{S}y$.

Si $\mathcal{S}$ est transitive, $\bar{\mathcal{S}}_0$ l'est; si $\mathcal{S}$ est réflexive, $\bar{\mathcal{S}}_1$ l'est. On a toujours $\bar{\mathcal{S}}_0 \subseteq \bar{\mathcal{S}}_1$.

THÉORÈME 2. — L'égalité $\bar{\mathcal{S}}_0 = \bar{\mathcal{S}}_1$ a lieu si et seulement si l'équivalence $\mathcal{R}$ respecte la relation $\mathcal{S}$. La relation $\bar{\mathcal{S}} = \bar{\mathcal{S}}_0 = \bar{\mathcal{S}}_1$ est alors appelée image de $\mathcal{S}$ dans l'ensemble-quotient ⁽¹⁾.

1° Soit $\bar{\mathcal{S}}_0 = \bar{\mathcal{S}}_1$; si $x\mathcal{R}\mathcal{S}y$, c'est-à-dire $x\mathcal{R}x_1$ et $x_1\mathcal{S}y$, et si X désigne la classe modulo $\mathcal{R}$ contenant x et x_1 , Y la classe contenant y , on a $X\bar{\mathcal{S}}_1Y$, donc $X\bar{\mathcal{S}}_0Y$, donc $x\mathcal{S}y$. Nous avons bien $\mathcal{R}\mathcal{S} \subseteq \mathcal{S}$ et de même $\mathcal{S}\mathcal{R} \subseteq \mathcal{S}$: la condition de l'énoncé est nécessaire.

2° Supposons $\mathcal{R}\mathcal{S} \subseteq \mathcal{S}$ et $\mathcal{S}\mathcal{R} \subseteq \mathcal{S}$, donc aussi, puisque $\mathcal{R}$ est réflexive, $\mathcal{S} = \mathcal{R}\mathcal{S} = \mathcal{S}\mathcal{R} = \mathcal{R}\mathcal{S}\mathcal{R}$. Si l'on a $X\bar{\mathcal{S}}_1Y$, il existe $x \in X$ et $y \in Y$ tels que $x\mathcal{S}y$. Si x_1, y_1 sont des éléments quelconques de X, Y , on a $x_1\mathcal{R}\mathcal{S}\mathcal{R}y_1$, donc $x_1\mathcal{S}y_1$ et X, Y vérifient $X\bar{\mathcal{S}}_0Y$: nous avons bien $\bar{\mathcal{S}}_1 \subseteq \bar{\mathcal{S}}_0$, d'où l'égalité.

Les relations réflexives et transitives, comprenant comme cas particuliers aussi bien les relations d'ordre partiel que les relations d'équivalence, sont appelées relations de préordre ou de quasi-ordre.

⁽¹⁾ Ce théorème est un cas particulier de propositions plus générales (voir § 12, exerc. 3, 2°, p. 60).

THÉOREME 3 ⁽¹⁾. — Soit $\mathcal{S}$ une relation de préordre dans un ensemble E . La relation $\mathcal{R} = \mathcal{S} \cap \mathcal{S}^{-1}$ est une équivalence qui respecte $\mathcal{S}$; dans l'ensemble-quotient $E/\mathcal{R}$, l'image $\bar{\mathcal{S}}$ de $\mathcal{S}$ est une relation d'ordre partiel.

$\mathcal{S}^{-1}$ est réflexive et transitive comme $\mathcal{S}$; il en est de même de $\mathcal{R}$, qui est en outre symétrique : $\mathcal{R}$ est donc bien une équivalence qui, étant contenue dans la relation transitive $\mathcal{S}$, la respecte. L'image $\bar{\mathcal{S}}$ de $\mathcal{S}$ dans $E/\mathcal{R}$ est réflexive et transitive; d'autre part, elle est *propre*, puisque $X\bar{\mathcal{S}}Y$ et $Y\bar{\mathcal{S}}X$ signifient, pour tout $x \in X$ et tout $y \in Y$, $x\mathcal{S}y$ et $y\mathcal{S}x$, c'est-à-dire $x\mathcal{R}y$ et, par conséquent, $X = Y$.

Exemple. — Dans l'ensemble $G = \{ \dots, -2, -1, 0, 1, \dots, n, \dots \}$ des entiers relatifs, la relation : « x divise y », $x|y$ ($y = cx$, $c \in G$), établit un *préordre*. L'équivalence $\mathcal{R} = \mathcal{S} \cap \mathcal{S}^{-1}$ n'est autre que $y = \pm x$. L'ensemble-quotient $E/\mathcal{R}$ est représenté par l'ensemble N_0 des nombres naturels et de zéro, la relation d'ordre partiel $\bar{\mathcal{S}}$ est $X|Y$ dans N_0 .

Exercice. — Soit E l'ensemble des points d'un plan P . On considère dans E un point particulier O et, a et b étant deux points quelconques, on pose $a\mathcal{S}b$ si et seulement si la distance Oa est inférieure ou égale à la distance Ob . Montrer que $\mathcal{S}$ est une relation de préordre. Quelles sont les classes modulo $\mathcal{R} = \mathcal{S} \cap \mathcal{S}^{-1}$? Quelle est la relation d'ordre $\bar{\mathcal{S}}$, image de $\mathcal{S}$ dans l'ensemble-quotient $E/\mathcal{R}$?

C. — CORRESPONDANCES.

6. Notions générales. — Soient E et E' deux ensembles, distincts ou non. On donne, d'une manière générale, le nom de *correspondance* entre E et E' à toute loi associant à un ou plusieurs éléments de E un ou plusieurs éléments de E' .

Plus particulièrement, une *application uniforme* f de E dans E' est une loi associant à *chaque* élément x de E un élément x' de E' appelé *image* de x dans l'application f , et désigné par l'une des notations

$$x' = xf, \quad fx \quad \text{ou} \quad f(x).$$

On donne encore à une telle application le nom de *fonction uniforme définie sur E , prenant ses valeurs dans E'* ; en Théorie des fonctions, on utilise de préférence la notation $x' = f(x)$, tandis qu'en Algèbre la

⁽¹⁾ Cf. SCHRÖDER, *Algebra der Logik* (Leipzig, 1890), p. 184, ainsi que G. BIRKHOFF, *Lattice Theory*, p. 4.

notation inversée $x' = xf$, d'ailleurs un peu plus simple, est souvent avantageuse.

L'*image* Af ou $f(A)$ d'une partie A de E est, par définition, l'ensemble $\{f(x)\}_{x \in A}$ des images des éléments de A . Si l'on a $f(E) = E'$, on dit que f est une application uniforme de E sur E' , ou un *homomorphisme d'ensembles* entre E et E' (ou, mieux, appliquant E sur E'), ou encore que E' , *image* de E , est un *ensemble homomorphe* à E . Ce cas, pour bien préciser, est caractérisé par les deux propriétés suivantes :

- 1° Tout élément x de E a dans E' une image x' bien déterminée;
- 2° Tout élément x' de E' est l'image d'au moins un élément de E .

On écrit fréquemment

$$E \rightarrow E' \quad \text{ou} \quad E \sim E'$$

(avec cette seconde notation, la dissymétrie qui existe en général entre l'ensemble E et son image E' , et qu'il ne faut jamais perdre de vue, se traduit seulement par l'ordre dans lequel les lettres E , E' sont écrites).

Une *application multiforme* f de E dans E' , ou une *fonction multiforme* f définie dans E , prenant ses valeurs dans E' , est une loi associant à chaque élément x de E un sous-ensemble non vide

$$X' = xf \quad \text{ou} \quad fx \quad \text{ou} \quad f(x)$$

de E' , appelé *image* de x . L'*image* Af , fA ou $f(A)$ d'une partie A de E est la réunion $\bigcup_{x \in A} f(x)$ des images des éléments de A .

Si $f(E) = E'$, f est une application de E sur E' . A désignant toujours une partie de E , l'application f effectuée seulement pour les éléments de A , est appelée *application induite* par f dans A , ou *application f limitée à A* et désignée, pour éviter toute confusion, par f_A .

Remarque. — Il est clair qu'en remplaçant E' par $\mathfrak{X}(E') = \mathfrak{F}'$, on peut ramener le cas d'une application multiforme à celui d'une application uniforme. Il en est de même pour une correspondance quelconque : il suffit de remplacer, en outre, E par la partie $\mathfrak{F}$ de $\mathfrak{X}(E)$ sur laquelle la correspondance est définie.

Les notions précédentes sont étroitement liées à celle de relation et, par conséquent, dérivent, elles aussi, des concepts fondamentaux de *parties* et d'*ensemble-produit*. Soit d'abord f une application uniforme

de E dans E', l'égalité

$$x' = f(x)$$

définit une *relation* $\mathcal{R}$ entre l'élément x de E et l'élément x' de E'. Cette relation n'est pas quelconque, puisque, x' étant défini quel que soit $x \in E$, la projection $\mathcal{R}^{-1}(E')$ coïncide avec E, et que, f étant uniforme, la coupe $\mathcal{R}(x)$ se compose au plus de l'élément $x' = f(x)$; on exprime cette seconde propriété en disant que $\mathcal{R}$ est une relation *quasi-fonctionnelle*, l'ensemble des deux propriétés en disant que $\mathcal{R}$ est une relation *fonctionnelle* ⁽¹⁾. Inversement, toute relation fonctionnelle $\mathcal{R}$ sur E et E' définit une application uniforme de E dans E'.

Si f est une *application multiforme* de E dans E', l'appartenance

$$x' \in f(x) = X'$$

définit encore une relation $\mathcal{R}$ entre x et x' , possédant la propriété $\mathcal{R}^{-1}(E') = E$; l'image X' de x est la coupe $\mathcal{R}(x)$; l'image $f(X)$ d'une partie X de E, définie par

$$f(X) = \bigcup_{x \in X} f(x)$$

n'est autre que la coupe de première espèce $\mathcal{R}(X)$. A toute relation $\mathcal{R}$ vérifiant la condition $\mathcal{R}^{-1}(E') = E$ correspond inversement une application f de E dans E', définie par

$$f(x) = \mathcal{R}(x)$$

multiforme si $\mathcal{R}$ n'est pas quasi-fonctionnelle.

L'ensemble *représentatif* d'une application f (uniforme ou multiforme) est la partie $\mathcal{S}_{\mathcal{R}}$ de $E \times E'$ représentant la relation $\mathcal{R}$ associée à f , donc l'ensemble des couples (x, x') pour lesquels on a $x' \in f(x)$ (on peut remplacer $\in$ par $=$ quand f est uniforme); on le désignera aussi par la notation $\mathcal{S}_f$.

Dans la pratique, l'aspect « application » ou « fonction » est souvent commode et suggestif; on est d'ailleurs amené fréquemment à combiner les notions de relation et de correspondance, et si l'on se limitait à l'une d'elles, on verrait vite apparaître des complications de langage.

Exemples. — 1. Soient E l'ensemble des points de l'espace, P l'ensemble des points d'un plan. La projection orthogonale f des points de E sur le plan P est

⁽¹⁾ Cf. J. RIGUET, *Relations binaires...* (Bull. Soc. Math. de France, t. 76, 1948, p. 114).

une application uniforme de E sur P : P est un ensemble homomorphe à E , chaque point de P est ici l'image d'une infinité de points de E . Soit A une *figure* dans E , c'est-à-dire un ensemble de points non vide; son image $f(A)$ est la projection de la figure A sur le plan P . Si A est un plan non perpendiculaire à P , on a $f(A) = P$; si A est un plan perpendiculaire à P , on a $f(A) \subset P$ et l'application induite f_A est une application de A dans P .

2. En posant $n' = n + 1$, on obtient une application de l'ensemble N des nombres naturels en lui-même.

3. En posant $y = x^2$, on obtient une fonction f définie dans l'ensemble $\mathbf{P}$ des nombres réels, prenant ses valeurs dans $\mathbf{P}$, ou même seulement dans l'ensemble $\mathbf{P}_+$ des nombres réels positifs ou nuls (application de $\mathbf{P}$ dans $\mathbf{P}$, de $\mathbf{P}$ sur $\mathbf{P}_+$). En représentant l'ensemble-produit $\mathbf{P} \times \mathbf{P}$ au moyen du plan xOy , on a, comme ensemble représentatif une parabole, dite courbe représentative de cette fonction.

4. Prenons comme ensemble E la droite $x'Ox$, comme ensemble E' le plan yOz (les axes Ox , Oy , Oz étant rectangulaires). A tout point x sur Ox , associons comme ensemble $f(x)$:

- a. La circonférence γ de centre O , de rayon $r = |x|$ dans yOz ;
- b. Le cercle Γ limité par γ (et comprenant sa frontière γ).

Nous définissons ainsi deux applications multiformes de E sur E' . En représentant le produit $E \times E'$ au moyen de l'espace $Oxyz$, on obtient comme ensemble représentatif de l'application a la surface du cône de révolution définie par l'équation

$$y^2 + z^2 = x^2,$$

comme ensemble représentatif de l'application b , la *région*

$$y^2 + z^2 \leq x^2,$$

c'est-à-dire le cône « plein » limité par la surface précédente.

Soient E , E' , E'' des ensembles distincts ou non et f une application de E dans E' , g une application de E' dans E'' . A, un élément x de E , f associe comme image dans E' l'ensemble $X' = xf$ ou $f(x)$, auquel g associe comme image dans E'' l'ensemble $X'' = X'g$ ou $g(X')$. Nous avons ainsi une loi h associant à tout $x \in E$ une partie X'' de E'' , donc une application de E dans E'' , appelée *produit* de f par g et désignée par $f'g$ quand on emploie la notation $X' = xf$, appelée encore *fonction composée* de f et g ou *fonction de fonction* et désignée par gf quand on emploie les notations $X' = fx$ ou $f(x)$:

$$X'' = x(fg) = (xf)g, \quad X'' = gf(x) = g f(x).$$

Si f et g sont des applications uniformes, leur produit est, lui aussi, uniforme.

Exemple. — Dans l'espace euclidien E , soient E' un plan, E'' une droite contenue dans E' (E , E' , E'' sont considérés comme ensembles de leurs points). Le théorème des trois perpendiculaires exprime que la projection orthogonale des points de E sur la droite E'' est le produit de la projection orthogonale des points de E sur le plan E' , par celle des points de E' sur la droite E'' .

7. Applications uniformes; théorème d'homomorphisme. — Une application *uniforme* f de E dans E' est *univalente* si l'égalité

$$f(a) = f(b) \quad \text{exige} \quad a = b.$$

Une application *univalente* de E sur E' est dite *biunivoque*; ce cas est celui où :

- 1° Tout élément x de E a dans E' une image x' bien déterminée;
- 2° Tout élément x' de E' est inversement l'image d'un élément x de E et d'un seul.

Cet élément x est dit *image inverse* de x' ; la loi associant x à x' est l'*application inverse* (ou *réciproque*) ou la *fonction inverse* f^{-1} de f ; on écrit

$$x = x' f^{-1} \quad \text{ou} \quad f^{-1}(x'),$$

f^{-1} est elle-même une application univalente de E' sur E .

Une application biunivoque f de E sur E' est encore appelée un *isomorphisme d'ensembles* entre E et E' ; on dit que E et E' sont *isomorphes en tant qu'ensembles* ou qu'ils ont même *puissance* (ou sont *équipotents*). On écrit

$$E \leftrightarrow E', \quad E \simeq E' \quad \text{ou} \quad E \cong E'.$$

Cette propriété est *réflexive* (car l'application identique $x' = x$ de E sur lui-même est biunivoque), *symétrique* (puisque f^{-1} est biunivoque quand f l'est), et *transitive* (car le produit de deux applications biunivoques est visiblement biunivoque). Par suite, dans l'ensemble des parties $\mathfrak{A}(E)$ d'un ensemble donné E , l'égalité des puissances est une relation d'équivalence, et l'on peut définir la *puissance* d'une partie A de E comme la classe à laquelle appartient A dans cette équivalence. Il en est de même, plus généralement, dans toute famille donnée d'ensembles.

Deux ensembles ordonnés E , E' sont *semblables* (ou *isomorphes*) si l'un est l'image de l'autre dans une *application biunivoque*

$$(\varphi) \quad E \leftrightarrow E'$$

qui respecte leurs relations d'ordre, ou est *isotone*, c'est-à-dire telle que

$$a \leq b \quad \text{dans } E \quad \text{entraîne} \quad \varphi(a) \leq \varphi(b) \quad \text{dans } E'$$

et inversement ⁽¹⁾ (suivant l'usage, nous représentons par le même signe les relations d'ordre de E et de E' qui, bien entendu, ne doivent pas être confondues). On écrit alors

$$(\varphi) \quad E \approx E'.$$

Exemples. — 1. En associant à tout nombre naturel n son suivant $n+1$, son double $2n$, son carré n^2 , nous définissons des applications *univalentes* (mais non biunivoques) de l'ensemble N des nombres naturels en lui-même.

2. L'égalité $y = x^2$ définit une application biunivoque de l'ensemble P_+ des nombres réels positifs ou nuls sur lui-même; la même égalité définit une application de P (décrit par x) sur P_+ (décrit par y) qui n'est pas univalente. Cet exemple montre nettement qu'il est indispensable de distinguer une fonction d'une formule servant éventuellement à la définir, et que les propriétés d'une fonction dépendent essentiellement du choix des ensembles entre lesquels cette fonction établit une correspondance.

3. La projection orthogonale f_A des points d'un plan A sur un plan P , non perpendiculaire à A , est une application biunivoque (alors que la projection f des points de l'espace sur P ne l'est pas : on voit pourquoi il y a lieu de distinguer l'application induite de l'application elle-même).

4. Soient, dans un plan, E, E' deux droites parallèles, orientées dans le même sens et regardées comme ensembles ordonnés de leurs points. O étant un point fixe du plan, n'appartenant ni à E ni à E' , associons à chaque point x de E la trace x' de Ox sur E' . Nous définissons ainsi une application biunivoque de E sur E' , E et E' sont *semblables* dans cette application si et seulement si O n'est pas situé entre E et E' .

On donne le nom de *transformation* ou d'*automorphisme d'ensemble* à toute application biunivoque d'un ensemble E sur lui-même. Si E est *fini*, on emploie ordinairement pour désigner une telle transformation, le mot de *substitution*. Dans ce cas, en supposant par exemple que les éléments de E sont les nombres $1, 2, \dots, n$, on définit la substitution en écrivant sous chacun de ces nombres le nombre-image, par exemple ($n=3$),

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

Cette substitution transforme la *permutation*, c'est-à-dire l'ensemble ordonné $(1, 2, 3)$, en $(2, 1, 3)$; on peut aussi, pour abrégé, la représenter par cette dernière permutation; pour cette raison, on donne parfois aux substitutions le nom de *permutations*.

⁽¹⁾ Cette deuxième partie de la condition est superflue si E, E' sont totalement ordonnés.

Exercice. — On considère les substitutions

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \quad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

Calculer les produits $\sigma_1 \sigma_2$ et $\sigma_2 \sigma_1$.

Considérons dans un ensemble E une équivalence $\mathcal{R}$ et associons à tout élément x de E la classe X modulo $\mathcal{R}$ qui le contient : cette correspondance est une application uniforme de E sur l'ensemble-quotient $\mathbf{Q} = E/\mathcal{R}$

$$E \rightarrow E/\mathcal{R}.$$

Inversement, soit f une application uniforme d'un ensemble E sur un ensemble E' . Considérons la relation $\mathcal{R}$ définie dans E par

$$x \mathcal{R} y \quad \text{si} \quad f(x) = f(y).$$

Cette relation, exprimant que deux points de E ont la même image dans E' est visiblement une relation d'équivalence appelée *équivalence d'application* ou d'*homomorphisme*. Elle coïncide avec l'égalité si f est biunivoque, et seulement dans ce cas. A tout élément x' de E' correspond une classe modulo $\mathcal{R}$ et une seule, ensemble de tous les éléments $x, x_1, \dots$ de E dont l'image dans E' est x' . L'ensemble E' et l'ensemble-quotient $E/\mathcal{R}$ sont, par conséquent, isomorphes :

$$E' \leftrightarrow E/\mathcal{R};$$

cette remarque presque évidente constitue le *théorème d'homomorphisme pour les ensembles*.

Exemple. — Soient E l'ensemble des points de l'espace, P l'ensemble des points d'un plan, f la projection orthogonale sur P , $\mathcal{R}$ l'équivalence d'application correspondante. Deux points m, m_1 sont équivalents modulo $\mathcal{R}$ si et si seulement ils appartiennent à une même perpendiculaire à P . L'ensemble-quotient $E/\mathcal{R}$, ensemble des perpendiculaires à P , correspond bien biunivoquement à l'ensemble des points de P .

8. Cas général : application inverse, sous-ensembles stables. — Soit maintenant f une application, uniforme ou *multiforme*, d'un ensemble E dans un ensemble E' . D'après la définition même de l'image d'un ensemble, on voit que

$$(1) \quad A \subseteq B \quad (\subseteq E) \quad \text{entraîne} \quad f(A) \subseteq f(B).$$

Si Φ désigne une famille de parties M de E , on a

$$(2) \quad f\left(\bigcup_{M \in \Phi} M\right) = \bigcup_{M \in \Phi} f(M),$$

« l'image d'une réunion est la réunion des images ». Pour une intersection, $I = \bigcap_{M \in \Phi} M$, on a, d'après (1), $f(I) \subseteq f(M)$ pour tout $M \in \Phi$, donc

$$(3) \quad f\left(\bigcap_{M \in \Phi} M\right) \subseteq \bigcap_{M \in \Phi} f(M),$$

mais l'égalité n'a pas lieu en général; dès que deux éléments distincts x_1, x_2 de E ont des images $f(x_1), f(x_2)$ qui se coupent, on a, en prenant $M_1 = \{x_1\}$ et $M_2 = \{x_2\}$,

$$I = M_1 \cap M_2 = \emptyset, \quad f(I) = \emptyset \quad \text{et} \quad f(M_1) \cap f(M_2) \neq \emptyset,$$

donc

$$f(M_1 \cap M_2) \subset f(M_1) \cap f(M_2).$$

Même si f est uniforme, l'égalité, dans (3), n'a pas nécessairement lieu.

Exemple. — Considérons la fonction uniforme $y = x^2$ appliquant l'ensemble $\mathbf{P}$ des nombres réels sur l'ensemble $\mathbf{P}_+$ des nombres réels positifs ou nuls, et les segments ⁽¹⁾ $M_1 = [-a, 0]$, $M_2 = [0, a]$, $a > 0$: nous avons

$$I = \{0\}, \quad f(I) = \{0\}, \quad f(M_1) = f(M_2) = [0, a^2],$$

donc

$$f(M_1 \cap M_2) \subset f(M_1) \cap f(M_2).$$

Si f est non seulement *uniforme* mais *univalente*, on a l'égalité

$$(3') \quad f\left(\bigcap_{M \in \Phi} M\right) = \bigcap_{M \in \Phi} f(M),$$

Soit, en effet, $x' \in \bigcap_{M \in \Phi} f(M)$ et M_0 un ensemble particulier de la famille Φ ; il existe $x_0 \in M_0$ tel que $x' = f(x_0)$ et, de même, pour chaque M , il existe $x \in M$ tel que $x' = f(x)$. Puisque f est univalente, il en résulte

$$x_0 = x \in \bigcap_{M \in \Phi} M, \quad \text{donc} \quad x' \in f\left(\bigcap_{M \in \Phi} M\right).$$

Soit f une application (uniforme ou multiforme) de E sur E' . Associons à chaque élément x' de E' l'ensemble X des $x \in E$ tels que $f(x) \ni x'$; nous définissons ainsi une application f^{-1} de $E' = f(E)$ sur E :

$$(4) \quad f^{-1}(x') = \{x \mid x' \in f(x)\}$$

⁽¹⁾ Rappelons qu'un segment $[\alpha, \beta]$ dans l'ensemble des nombres réels est l'ensemble des nombres x vérifiant $\alpha \leq x \leq \beta$: un segment comprend ses extrémités.

appelée *application inverse* de f . L'application inverse f^{-1} d'une application uniforme n'est elle-même uniforme que si f est univalente (donc biunivoque) et, dans ce cas, la définition précédente coïncide avec celle qui a été donnée plus haut.

On a

$$(f^{-1})^{-1} = f.$$

Posons, en effet, $f^{-1}(x') = \varphi(x')$; d'après (4), où l'on intervertit E et E', on a

$$\varphi^{-1}(x) = \{x'\}_{x \in \varphi(x')};$$

or, $x \in \varphi(x') = f^{-1}(x')$ signifie, d'après (4), $x' \in f(x)$. Donc $\varphi^{-1}(x)$ est l'ensemble des x' appartenant à $f(x)$, c'est-à-dire

$$\varphi^{-1}(x) = f(x) \quad \text{pour tout } x \in E.$$

La relation $\mathfrak{C}$ définie dans E par

$$x \mathfrak{C} x_1 \Leftrightarrow f(x) \not\subseteq f(x_1)$$

signifie : il existe au moins un x' tel que $x' \in f(x)$ et $x' \notin f(x_1)$; c'est aussi ce que signifie $x_1 \in f^{-1}f(x)$ ou $x \in f^{-1}f(x_1)$: les relations $x \mathfrak{C} x_1$, $x_1 \in f^{-1}f(x)$, $x \in f^{-1}f(x_1)$ ont donc lieu en même temps et, par conséquent, $x_1 \in f^{-1}f(x)$ est une relation *symétrique* (d'ailleurs aussi *réflexive*).

Pour toute partie A de E on a

$$(5) \quad f^{-1}f(A) \supseteq A.$$

Posons, en effet, $f(A) = A'$. Soit $a \in A$; si $a' \in f(a) \subseteq A'$, on a

$$a \in f^{-1}(a') \subseteq f^{-1}(A') = f^{-1}f(A),$$

d'où (5). On n'a pas, en général, l'égalité, même si f est uniforme, cependant l'égalité a lieu quel que soit $A \subseteq E$ si f est non seulement uniforme, mais univalente. Dans ce cas, en effet, $f(x) \not\subseteq f(x_1)$ entraîne $f(x) = f(x_1)$, puis $x = x_1$.

Exemples. — Si f est l'application $x \rightarrow x^2$ de $\mathbf{P}$ sur $\mathbf{P}_+$, on a

$$f^{-1}f(x) = \{x, -x\} \neq \{x\} \quad \text{pour } x \neq 0.$$

Un sous-ensemble S non vide de E est dit *stable* pour l'application f si l'on a

$$f^{-1}f(S) = S.$$

D'après (5), E est toujours stable.

Toute réunion $R = \bigcup_{s \in \Phi} S$ et toute intersection $I = \bigcap_{s \in \Phi} S$ d'ensembles stables, sont des ensembles stables.

On a, en effet,

$$f^{-1}f(R) = f^{-1}f\left(\bigcup_{s \in \Phi} S\right) = f^{-1}\left[\bigcup_{s \in \Phi} f(S)\right] = \bigcup_{s \in \Phi} f^{-1}f(S) = \bigcup_{s \in \Phi} S = R$$

et

$$f^{-1}f(I) = f^{-1}f\left(\bigcap_{s \in \Phi} S\right) \subseteq f^{-1}\left[\bigcap_{s \in \Phi} f(S)\right] \subseteq \bigcap_{s \in \Phi} f^{-1}f(S) = \bigcap_{s \in \Phi} S = I,$$

ce qui, d'après (5), entraîne

$$f^{-1}f(I) = I.$$

Si un ensemble stable S_1 contient un ensemble stable S , le complément $C = S_1 - S$ est un ensemble stable.

On a $S_1 = S \cup C$, d'où

$$S_1 = f^{-1}f(S_1) = f^{-1}f(S) \cup f^{-1}f(C) = S \cup f^{-1}f(C).$$

Si nous montrons que $S \cap f^{-1}f(C) = \emptyset$, la proposition en résultera, puisqu'on aura

$$S_1 = S + f^{-1}f(C), \quad \text{donc} \quad f^{-1}f(C) = S_1 - S = C.$$

Or, le fait que S et $f^{-1}f(C)$ sont disjoints, résulte du lemme suivant :

LEMME. — Si un ensemble stable S et un ensemble C quelconque sont disjoints, S et $f^{-1}f(C)$ le sont aussi.

Supposons que $x \in S \cap f^{-1}f(C)$. Il existerait $x_1 \in C$ tel que $x \in f^{-1}f(x_1)$; on aurait donc

$$x_1 \in f^{-1}f(x) \subseteq f^{-1}f(S) = S,$$

ce qui est contraire à l'hypothèse $S \cap C = \emptyset$.

On exprime les propriétés précédentes des ensembles stables en disant qu'ils forment un *corps complet d'ensembles*.

Si $x \in E$, il existe des ensembles stables contenant x : E , par exemple. Leur intersection S_x est le *plus petit ensemble stable contenant x* . C'est d'ailleurs un ensemble stable *minimal*, c'est-à-dire qui ne peut contenir aucun autre ensemble stable ($\neq \emptyset$). Si, en effet, T était une partie de E stable pour f et vérifiant $\emptyset \subset T \subset S_x$, on aurait $x \notin T$, donc

$x \in S_x - T$, ce qui est impossible puisque $S_x - T$ est stable et contenu strictement dans S_x .

Puisque, par définition, $x \in S_x$, on a

$$f^{-1}f(x) \subseteq f^{-1}f(S_x) = S_x,$$

quel que soit x .

Deux ensembles stables *minimaux* ne peuvent se couper qu'en coïncidant. Comme tout élément x de E appartient à l'un d'eux, S_x , ces ensembles déterminent une décomposition de E en classes; l'équivalence $\mathcal{C}$ correspondante est définie par

$$x \equiv y (\mathcal{C}) \Leftrightarrow S_x = S_y.$$

Revenons alors à la relation $\mathfrak{S}$, réflexive et symétrique; $x \mathfrak{S} y$, c'est-à-dire $f(x) \not\subseteq f(y)$, entraîne, comme nous l'avons vu,

$$y \in f^{-1}f(x) \subseteq f^{-1}f(S_x) = S_x,$$

d'où $S_y = S_x$, c'est-à-dire $x \equiv y (\mathcal{C})$. On a donc $\mathfrak{S} \subseteq \mathcal{C}$. Nous verrons plus loin (p. 59) que $\mathcal{C}$ est la plus fine équivalence contenant $\mathfrak{S}$.

Considérons, de même, dans E' les ensembles stables pour l'application inverse f^{-1} , les ensembles stables minimaux et l'équivalence correspondante. S étant une partie stable de E , on a

$$f^{-1}f(S) = S, \quad \text{d'où} \quad ff^{-1}f(S) = f(S),$$

donc l'image d'une partie stable S de E est une partie stable $S' = f(S)$ de E' , et inversement. *Les parties stables de E et de E' se correspondent biunivoquement par f et f^{-1} .* Puisqu'en outre l'inclusion est conservée par toute application, les parties stables *minimales*, c'est-à-dire les classes modulo $\mathcal{C}$ et $\mathcal{C}'$, se correspondent, elles aussi, biunivoquement. Nous pouvons donc énoncer ⁽¹⁾ :

THÉORÈME 1. — *Soient f une application (uniforme ou multiforme) d'un ensemble E sur un ensemble E' , $\mathcal{C}$ et $\mathcal{C}'$ les relations d'équivalence décomposant respectivement E et E' en parties stables minimales. La correspondance qui associe à l'ensemble stable minimal S_x contenant un élément x de E l'ensemble stable minimal S'_x contenant un élément quelconque x' de $f(x)$, est biunivoque :*

$$(6) \quad E/\mathcal{C} \leftarrow \rightarrow E'/\mathcal{C}'.$$

⁽¹⁾ Cf. M. L. DUBREIL-JACOTIN, *Quelques propriétés des applications multiformes* (C. R. Acad. Sc., t. 230, 1950, p. 806).

Exemple. — Dans un plan rapporté aux axes rectangulaires Ox, Oy , prenons comme ensembles E, E' les droites $y = +a, y = -a$ ($a > 0$) (fig. 1). Soit $H'H$

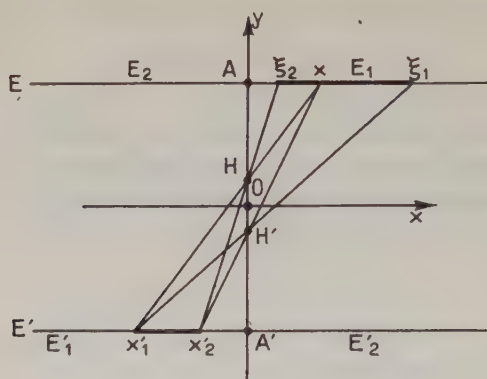


Fig. 1.

le segment $[-h, +h]$ porté par Oy , ($0 < h < a$). Au point d'abscisse x sur E , associons comme image le segment $[x'_1, x'_2]$ découpé sur E' par les droites xH, xH' . Posons

$$\frac{a+h}{a-h} = k > 1.$$

Les points x'_1 et x'_2 ont respectivement pour abscisse

$$x'_1 = -kx, \quad x'_2 = -x/k.$$

L'ensemble $f^{-1}f(x)$ est le segment $[\xi_2, \xi_1]$ découpé sur E par x'_1H' et x'_2H :

$$\xi_1 = k^2x, \quad \xi_2 = x/k^2.$$

Puisque $f^{-1}f(x) \subseteq S_x$, ces points appartiennent au plus petit ensemble stable S_x contenant x ; il en résulte que les ensembles stables minimaux de E sont : le point A situé sur Oy et les demi-droites E_1, E_2 limitées à ce point (et ne le comprenant pas). Ceux de E' sont, de même, A', E'_1, E'_2 : la correspondance biunivoque (6) apparaît nettement.

Cas particuliers. — 1. Le théorème 1 généralise le théorème d'homomorphisme pour les ensembles. Supposons, en effet, f uniforme. La relation $\mathfrak{G}$ définie par $f(x) \mathfrak{G} f(y)$, signifie ici $f(x) = f(y)$, donc coïncide avec l'équivalence d'application $\mathcal{R}$. Une partie stable $S = f^{-1}f(S)$ comprend au moins l'image inverse $X = f^{-1}(x')$ d'un élément de E' ; or, une telle image inverse est stable, ici, puisque $f^{-1}f(X) = f^{-1}(x') = X$. Les parties stables minimales sont donc, dans E , les images inverses $X = f^{-1}(x')$, c'est-à-dire les classes

modulo $\mathcal{R}$, et nous avons

$$\mathcal{C} = \mathfrak{C} = \mathcal{R}.$$

L'équivalence $\mathcal{C}'$, d'autre part, est l'égalité, puisque les ensembles stables minimaux de E' sont les images de ceux de E , donc les éléments x' de E' . La relation (6) s'écrit

$$E/\mathcal{R} \leftarrow \rightarrow E'$$

et nous avons bien le théorème d'homomorphisme obtenu plus haut.

2. L'égalité $\mathcal{C} = \mathfrak{C}$ n'a pas lieu seulement dans le cas uniforme. Nous dirons, d'une façon générale, qu'une application f de E sur E' est *semi-uniforme* (ou que la relation $\mathcal{R}$ correspondante, définie par

$$x \mathcal{R} x' \Leftrightarrow x' \in f(x),$$

est *difonctionnelle*) si $x \mathfrak{C} y$, c'est-à-dire $f(x) \not\parallel f(y)$, entraîne $f(x) = f(y)$. $\mathfrak{C}$ est alors une relation d'équivalence. Pour que f soit semi-uniforme, il suffit, puisque $\mathfrak{C}$ est toujours symétrique, que $f(x) \not\parallel f(y)$ entraîne $f(x) \subseteq f(y)$, c'est-à-dire que

$$\left. \begin{array}{l} y' \in f(x) \\ y' \in f(y) \\ x' \in f(x) \end{array} \right\} \text{ entraînent } x' \in f(y)$$

(et c'est évidemment aussi nécessaire). Or, cette condition peut s'écrire

$$\left. \begin{array}{l} x \in f^{-1}(x') \\ x \in f^{-1}(y') \\ y \in f^{-1}(y') \end{array} \right\} \text{ entraînent } y \in f^{-1}(x'),$$

ce qui signifie que f^{-1} est *semi-uniforme en même temps que f* . En particulier, *toute application inverse d'une application uniforme est semi-uniforme*.

THÉOREME 2. — Soit f une application de E sur E' , x un élément de E , $x' \in f(x)$, $X = f^{-1}(x')$. Si f est semi-uniforme, on a

$$X = f^{-1} f(X) = f^{-1} f(x) = S_x,$$

où S_x est le plus petit ensemble stable contenant x . Il en résulte que la relation $\mathfrak{C}$ coïncide avec l'équivalence $\mathcal{C}$.

Puisque $x' \in f(x)$, $x \in X$ et nous avons

$$X = f^{-1}(x') \subseteq f^{-1} f(x) \subseteq f^{-1} f(X).$$

Soit $x_1 \in f^{-1}f(X)$; il existe $x_2 \in X$ tel que $x_1 \in f^{-1}f(x_2)$, c'est-à-dire $x_1 \mathfrak{C} x_2$, d'où, f étant semi-uniforme, $f(x_1) = f(x_2)$, donc, puisque $x' \in f(x_2)$, $x' \in f(x_1)$, c'est-à-dire $x_1 \in X$ et $f^{-1}f(X) \subseteq X$, d'où les égalités

$$X = f^{-1}f(X) = f^{-1}f(X),$$

d'après lesquelles X est stable, et coïncide même avec le plus petit ensemble stable S_x contenant x , puisqu'on a toujours $f^{-1}f(x) \subseteq S_x$.

On voit que, si l'on se donne x , $X = f^{-1}(x')$ est indépendant du choix de x' dans $f(x)$.

Si enfin $S_x = S_y$, on a $y \in S_x = f^{-1}f(x)$, c'est-à-dire $x \mathfrak{C} y$, donc $\mathcal{C} \subseteq \mathfrak{C}$. Comme $\mathfrak{C}$ est toujours contenue dans $\mathcal{C}$ (cf. p. 33), on a bien l'égalité ⁽¹⁾ $\mathfrak{C} = \mathcal{C}$.

Exemple. — Dans l'exemple 4a, p. 26, où les $f(x)$ sont les circonférences γ de centre O et de rayon $|x|$ dans le plan $\gamma O z$, la relation $f(x) \mathfrak{C} f(y)$ entraîne bien $f(x) = f(y)$, et l'application f est semi-uniforme. L'équivalence $\mathfrak{C} = \mathcal{C}$ est caractérisée par

$$x \equiv y (\mathcal{C}) \Leftrightarrow |x| = |y|$$

et l'on a bien une correspondance biunivoque entre les circonférences γ , $\gamma^2 + z^2 = r^2$ du plan $\gamma O z$, et les couples de points $x = \pm r$ de l'axe Ox ⁽²⁾.

Exercice. — Soient E l'ensemble des points d'un plan, O un point fixe de E . On considère l'application f de E sur E associant à chaque point x l'intérieur $f(x)$ du cercle de centre O passant par x . Soit $\mathcal{F}$ la famille des droites M passant par O . Comparer

$$f\left(\bigcap_{M \in \mathcal{F}} M\right) \quad \text{et} \quad \bigcap_{M \in \mathcal{F}} f(M).$$

D. — ENSEMBLES ORDONNÉS.

9. Notions générales. — Soit E un ensemble partiellement ordonné par une relation réflexive, transitive et propre, O .

La trace de O sur une partie A de E possède encore, dans A , ces

⁽¹⁾ Le théorème qui vient d'être établi est aussi une conséquence d'une proposition générale que nous verrons plus loin (p. 59); *c* est l'équivalence la plus fine contenant $\mathfrak{C}$; on a donc $c = \mathfrak{C}$ dès que $\mathfrak{C}$ est une équivalence, ce qui a précisément lieu dans le cas semi-uniforme.

⁽²⁾ Diverses applications algébriques des théorèmes 1 et 2 seront vues plus loin (définition et propriétés des complexes forts dans la théorie des demi-groupes, p. 235; correspondances de Galois, p. 120, correspondance de Grell entre les idéaux d'un anneau et ceux d'un sous-anneau, p. 193).

propriétés, donc définit un ordre O_A . Si O est un ordre total, il en est de même de O_A . Si O est seulement un ordre partiel, il existe des parties A de E telles que O_A soit un ordre total; on dit alors que A est, par rapport à l'ordre O , une *chaîne* : un seul élément, un couple d'éléments comparables forment de telles chaînes. Une chaîne C est *maximale* si elle n'est partie véritable d'aucune autre chaîne ou, ce qui revient au même, si, pour chaque élément x de $E - C$, il existe au moins un élément de C non comparable à x .

D'autres parties remarquables d'un ensemble E ordonné par une relation d'ordre partiel, que nous noterons maintenant $\subseteq$, sont : les segments, les intervalles, les sections commençantes, les sections finissantes. Si $a \subseteq b$, le *segment* $[a, b]$ est l'ensemble des éléments x de E vérifiant $a \subseteq x \subseteq b$; si $a < b$, l'*intervalle* (a, b) est l'ensemble des éléments y vérifiant $a < y < b$. Une partie S de E est une *section commençante* si les relations $x < s$ et $s \in S$ entraînent $x \in S$, une *section finissante* ⁽¹⁾ si $s < x$ et $s \in S$ entraînent $x \in S$; par exemple, m étant un élément donné de E , l'ensemble (m) ou $C(m, E)$ des éléments x de E vérifiant $x \subseteq m$, est une section commençante (particulière), l'ensemble $)m($ des éléments y vérifiant $m \subseteq y$ est une section finissante. Les segments, les intervalles, les sections commençantes ou finissantes sont des *parties convexes* ou *sections*, c'est-à-dire des sous-ensembles S tels que $s' \in S, s'' \in S, s' \subseteq x \subseteq s''$ entraînent $x \in S$.

Deux éléments a, b distincts et comparables, $a < b$, sont dits *consécutifs* si l'intervalle (a, b) est vide; on dit aussi que b *couvre* a .

Soit A une partie non vide de E . On appelle *premier élément*, *plus petit élément* ou *élément minimum* de A un élément $a \in A$ tel que l'on ait $a \subseteq x$ pour tout $x \in A$; s'il existe, ce premier élément est nécessairement unique. De même, on appelle *dernier élément*, *plus grand élément* ou *élément maximum* de A un élément $z \in A$ tel que l'on ait $x \subseteq z$ pour tout $x \in A$. Le premier et le dernier élément de E lui-même, s'ils existent, sont souvent appelés, respectivement, *élément nul* et *élément universel*. Quand E a un premier élément a , un segment $[a, x]$ ayant a pour origine, est appelé *segment initial*.

On appelle *élément minimal* d'une partie A de E ($\emptyset \subset A \subseteq E$) un

⁽¹⁾ Cette terminologie, utilisée par M. L. Dubreil-Jacotin, L. Lesieur, R. Croisot [*Leçons sur la théorie des treillis, des structures algébriques ordonnées et des treillis géométriques* (Cahiers scientifiques, fasc. XXI, Gauthier-Villars, Paris, 1953)], est celle de M. A. Denjoy (*L'énumération transfinie*, Gauthier-Villars, Paris, 1947). J. Colmez (Thèse, *Portugaliæ Mathem.*, t. 6, 1947) appelle sections à gauche les sections commençantes.

élément m de A qui n'est supérieur à aucun autre élément de A :

$$x \in A \text{ et } x \subseteq m \text{ entraînent } x = m.$$

De même, un *élément maximal* de A est un élément m' de A qui n'est inférieur à aucun autre élément de A . Une chaîne C a au plus un *élément minimal*, qui est nécessairement *minimum*, et au plus un *élément maximal*, qui est *maximum*. Dans une partie A quelconque, tout élément *minimum* est *minimal*, tout élément *maximum* est *maximal*, mais la réciproque n'est pas vraie lorsque A est ordonné partiellement (par la trace de l'ordre considéré dans E); en particulier, on peut très bien avoir dans A plusieurs éléments maximaux (deux à deux incomparables), et plusieurs éléments minimaux (voir les exemples ci-dessous).

Soit x un élément de E . Si x n'est pas maximal dans E , la section finissante S , ensemble des éléments de E qui sont strictement supérieurs à x , n'est pas vide; si S a un premier élément, cet élément x^+ est appelé *suivant* (ou *successeur*) de x dans E ; si x n'est pas minimal et si la section commençante, non vide, S' des éléments strictement inférieurs à x a un dernier élément, cet élément x^- est appelé *précédent* (ou *prédécesseur*) de x . Les éléments x et x^+ sont consécutifs, de même x^- et x .

Si E est totalement ordonné (par une relation que nous notons, pour éviter toute confusion, $\leq$), on a :

Dès que x^- existe, $x = (x^-)^+$;

Dès que x^+ existe, $x = (x^+)^-$,

et la relation $x < y$ entraîne respectivement, si x, y ont des précédents x^-, y^- ou des suivants x^+, y^+ : $x^- < y^-$, $x^+ < y^+$.

On a, en effet, $x^- < x$ et $x \leq y^-$, donc $x^- < y^-$; on obtient, de même, $x^+ < y^+$.

Un élément m d'un ensemble E partiellement ordonné (par la relation $\subseteq$) est *majorant* d'une partie X , non vide, de E si l'on a

$$x \subseteq m \text{ pour tout } x \in X.$$

On dit aussi que X est *majoré par* m , que X est *majoré* s'il admet quelque majorant. Tout élément plus grand qu'un majorant de X est lui-même un majorant de X .

Si l'ensemble M , supposé non vide, des majorants de X a un plus petit élément m_0 , ce majorant minimum m_0 est appelé *borne supérieure* ⁽¹⁾ de X .

(1) Cette terminologie tend à prévaloir actuellement; elle diffère de celle de la première édition (nous disions : borne supérieure pour majorant, limite supérieure pour majorant minimum).

Lorsqu'un majorant de X appartient à X , il est à la fois borne supérieure et élément maximum de X .

On définit d'une façon évidente, par dualité, les notions de *minorant*, d'*ensemble minoré*, et de *borne inférieure*.

Une partie X de E est dite *bornée* si elle est à la fois majorée et minorée (on notera que cette propriété n'entraîne pas nécessairement l'existence de bornes inférieure ou supérieure, aux sens que nous avons attribués à ces mots, de minorant maximum et de majorant minimum).

Quand elle existe, la borne inférieure de l'ensemble $\{x, y\}$ formé par deux éléments de E est désignée par $\inf(x, y)$, $x \wedge y$ ou $x \cap y$: on emploie souvent cette dernière notation et l'on donne alors à la borne inférieure le nom d'*intersection*; mais il faut, bien entendu, éviter de le faire quand, E étant un ensemble de parties d'un certain ensemble fondamental, la borne inférieure dans E diffère de l'intersection au sens de la théorie des ensembles, ce qui peut arriver même quand la relation d'ordre de E est l'inclusion. Les signes $\cap$ et $\wedge$ se lisent *inter*.

De même, la borne supérieure de $\{x, y\}$, si elle existe, est notée $\sup(x, y)$, $x \vee y$ ou $x \cup y$ et souvent appelée *union*; les signes $\vee$ et $\cup$ se lisent *union*. Quand E est un ensemble de parties, l'union peut être différente de la réunion, même si la relation d'ordre est l'inclusion (voir l'exemple 4 ci-dessous).

L'utilisation systématique des notions précédentes va nous conduire à deux catégories de résultats fondamentaux : nous allons étudier maintenant, dans le cas d'un ordre total, les *ensembles bien ordonnés*, *discrets*, *finis*, *dénombrables* (§ 10), dans le cas d'un ordre partiel, les *demi-treillis*, *treillis*, *treillis complets* (§ 11).

Exemples. — 1. L'alphabet français, totalement ordonné par l'ordre alphabétique, admet un premier élément a , un dernier élément z ; pour chaque élément différent de a , il existe un précédent, chaque élément différent de z a un suivant.

2. Dans l'ensemble Γ des nombres rationnels et dans l'ensemble $\mathbf{P}$ des nombres réels, l'ordre usuel $\leq$ est un ordre total. Il n'existe ni élément maximum, ni élément minimum, ni couple d'éléments consécutifs.

L'ensemble A_Γ ou A_P des nombres positifs de Γ ou de $\mathbf{P}$ dont le carré est supérieur à 2 est une section finissante, admettant 1, par exemple, comme minorant. On voit facilement que A_Γ n'a pas de borne inférieure dans Γ , tandis que A_P a, dans $\mathbf{P}$, la borne inférieure $\sqrt{2}$.

3. L'ensemble $\mathcal{P}(M)$ des parties d'un ensemble M est ordonné par la relation d'inclusion $\subseteq$. Cet ordre est total si M se compose d'un élément unique, et dans ce cas seulement. La partie vide est élément minimum, M est élément maximum. L'intersection $A \cap B$, la réunion $A \cup B$ sont respectivement borne inférieure et borne supérieure de $\{A, B\}$.

4. Considérons l'ensemble $\mathcal{I}$ des intervalles et l'ensemble $\mathcal{S}$ des segments portés par une droite donnée ⁽¹⁾; ordonnons partiellement ces ensembles par l'inclusion. Dans aucun des deux cas, il n'existe d'élément maximal. $\mathcal{S}$ admet comme éléments minimaux les segments $[a, a]$ réduits à un point a , mais n'a pas d'élément minimum. $\mathcal{I}$ n'a pas d'éléments minimaux. Les intervalles, ou les segments, ayant pour milieu un point donné O forment une chaîne, qui est maximale.

Deux intervalles $I = (a, b)$, $I' = (a', b')$ ($a < b$, $a' < b'$) ont toujours une union $I \vee I' = \sup(I, I')$: c'est l'intervalle (α, β) défini par $\alpha = \text{Min}(a, a')$, $\beta = \text{Max}(b, b')$ ⁽²⁾ qui, si I et I' sont disjoints, contient strictement leur réunion au sens de la théorie des ensembles; $I \wedge I' = \inf(I, I')$ n'existe que si I et I' ne sont pas disjoints, et coïncide alors avec leur intersection $I \cap I'$ au sens de la théorie des ensembles. Mêmes propriétés pour les segments.

5. Les ensembles ordonnés les plus simples peuvent être représentés par un diagramme; chaque élément de l'ensemble est figuré par un point x du plan, et

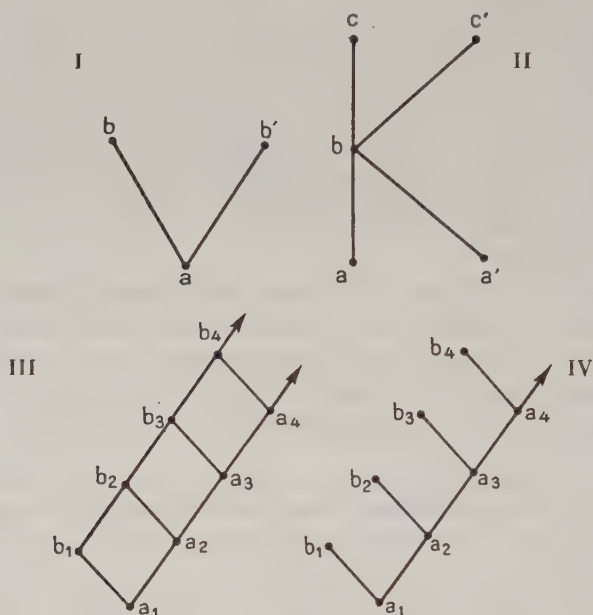


Fig. 2.

deux points x, y représentant des éléments consécutifs ($x < y$) sont réunis par un trait, ascendant de x vers y ; un élément supérieur à un autre est donc toujours placé plus haut que lui dans le diagramme.

⁽¹⁾ D'après la définition, un segment n'est jamais un ensemble vide; sur la droite, il en est de même pour un intervalle.

⁽²⁾ Les notations $\text{Min}(a, a')$, $\text{Max}(b, b')$ désignent respectivement le plus petit des deux nombres a, a' et le plus grand des deux nombres b, b' .

Inversement, un tel diagramme, donné *a priori* définit un ensemble ordonné; on a $r \subset s$ si l'on peut aller de r à s en suivant une ligne brisée constamment ascendante. Considérons, par exemple, les ensembles ordonnés définis par les diagrammes ci-dessus (fig. 2).

Nous avons :

Dans I, un élément minimum a ; deux éléments maximaux b, b' ;

Dans II, deux éléments minimaux a, a' ; deux éléments maximaux c, c' ; un élément b sans suivant ni précédent;

Dans III (où les flèches indiquent que la configuration se poursuit indéfiniment), un élément minimum, pas d'éléments maximaux; chaque élément a_i ($i \geq 2$) possède un précédent a_{i-1} , chaque élément b_j possède un suivant b_{j+1} ;

Dans IV, un élément minimum a_1 ; chaque élément b_j est maximal.

Exercices. — 1. On ordonne partiellement l'ensemble $N = \{1, 2, 3, \dots\}$ des entiers naturels par la relation $x \mid y$ (« x divise y »). Quels sont les éléments de N immédiatement supérieurs à 1 [c'est-à-dire admettant comme précédent le nombre 1, élément minimum ⁽¹⁾]. Montrer que deux éléments quelconques n, n' ont une union et une intersection, dont on précisera la définition arithmétique.

2. Dans le même ensemble ordonné N que dans l'exercice précédent, indiquer à quelle condition deux éléments sont consécutifs.

Tracer le diagramme du sous-ensemble S formé par 36 et ses diviseurs. Quel est le nombre de chaînes maximales distinctes contenues dans S ?

Tracer le diagramme du sous-ensemble $S' = \{1, 2, 3, \dots, 8, 9\}$.

3. On ordonne un jeu de 52 cartes suivant les valeurs respectives qu'elles ont au jeu de bridge avec l'atout « cœur ». Préciser quels sont : l'élément maximum, les éléments minimaux, les chaînes maximales. Existe-t-il un élément non minimal qui ne possède pas de précédent? (On pourra utiliser le diagramme de cet ensemble.)

10. Ensembles bien ordonnés, discrets, finis, naturels. — Soit E un ensemble *totalelement ordonné* ⁽²⁾ par un ordre O que nous désignerons également par $\leq$.

On dit que O est un *bon ordre*, que E est *bien ordonné* (par O) quand *toute partie non vide* A de E possède un *premier élément* (dans l'ordre O_A trace de O sur A). En particulier, E lui-même a un premier élément a , et tout élément x , sauf le dernier s'il existe, a un suivant x^+ (premier élément de la section finissante ensemble des éléments supérieurs à x). Les éléments x , autres que le premier, se répartissent en

(1) Lorsqu'il existe, comme ici, un élément minimum, les éléments qui (éventuellement) lui sont immédiatement supérieurs, sont appelés *points* ou *atomes*; on peut dire aussi qu'ils *couvrent* l'élément minimum.

(2) Pour l'étude des *procédés d'ordination* que nous utiliserons seulement dans la théorie des ensembles finis, voir le début de la Note I (p. 401), consacrée à cette théorie.

deux catégories selon qu'ils ont un précédent ou n'en ont pas : dans le second cas, x est dit *élément limite*. Cette seconde catégorie peut d'ailleurs être vide : c'est ce qui a lieu, par exemple, pour l'ensemble $E = \{a, b\}$ ($a < b$).

Toute partie non vide X d'un ensemble bien ordonné E est elle-même bien ordonnée (par la trace O_X de l'ordre O de E).

THÉOREME 1. — *Si une partie A d'un ensemble bien ordonné E est majorée, elle admet une borne supérieure.*

L'ensemble $\bar{M}$, non vide, des majorants de A possède, en effet, un élément minimum.

Remarque. — La partie vide peut être considérée comme majorée par tout élément de E , sa borne supérieure est le premier élément a de E .

On dit qu'un ensemble D est *discret* s'il est bien ordonné par un ordre O et si tout élément de D , autre que le premier, a un précédent.

THÉOREME 2. — *Si une partie non vide A d'un ensemble discret D est majorée, il existe dans A un élément maximum.*

D'après le théorème 1, A possède une borne supérieure m . Si m est le premier élément a de D , on a $A = \{a\}$, puisque A n'est pas vide : la proposition est vraie. S'il est supérieur à a , m a dans D un précédent m^- qui n'est pas majorant de A . Il existe donc un élément x de A vérifiant $m^- < x$ ($\leq m$), ce qui entraîne $m = x$; m est bien élément de A et, par conséquent, élément maximum.

THÉOREME 3. — *Toute partie non vide P d'un ensemble discret D , est un ensemble discret.*

P est bien ordonné par la trace O_P de l'ordre O de D ; P a donc un premier élément p . Montrons qu'un élément x de P , supérieur à p , a un précédent (dans P , par rapport à O_P). Soit Q l'ensemble des éléments q de P inférieurs à x ; $p \in Q$, donc Q n'est pas vide; comme, d'autre part, Q est majoré par x , il admet bien un dernier élément, d'après le théorème 2.

On dit qu'un ensemble E , totalement ordonné par O , est *doublement bien ordonné* (par O), ou encore que O est un *double bon ordre*, si toute partie non vide de E possède un premier et un dernier élément (en d'autres termes, si O et l'ordre inverse O^{-1} sont de bons ordres).

Toute partie non vide d'un ensemble doublement bien ordonné est elle-même doublement bien ordonnée.

Un ensemble doublement bien ordonné E a un premier et un dernier élément ; tout élément de F , sauf le premier, a un précédent ; tout élément autre que le dernier a un suivant : *un ensemble doublement bien ordonné est un ensemble discret avec dernier élément*. Nous établirons la réciproque après avoir étudié les procédés de raisonnement par induction.

Pour établir que tous les éléments d'un *ensemble bien ordonné* E ont une certaine propriété $\mathfrak{P}$, il suffit de montrer qu'un élément possède cette propriété dès qu'il en est ainsi pour tous ceux qui le précèdent (en particulier, on montrera que le premier élément de E a cette propriété). Si, en effet, l'ensemble des éléments de E qui n'ont pas la propriété en question n'était pas vide, il admettrait un premier élément, d'où contradiction.

Ce procédé de raisonnement, appelé *induction transfinie*, intervient également comme procédé de construction. Soit à associer à chaque élément x d'un ensemble bien ordonné E un être $f(x)$ appartenant à un certain ensemble E' , au moyen d'un système de *relations récurrentes*, c'est-à-dire de relations définissant d'une manière unique $f(x)$ à partir des images $f(r) \in E'$ des éléments r de E qui sont inférieurs à x (en particulier, la valeur de f pour le premier élément a de E est supposée déterminée ou imposée).

Il est clair d'abord que, si S désigne une section commençante de E (pouvant coïncider avec E), il existe *au plus* une fonction f_S définie sur S , prenant ses valeurs dans E' , et vérifiant pour tout $x \in S$ les relations récurrentes données. S'il y avait, en effet, deux telles fonctions distinctes $f_S(x)$, $\varphi_S(x)$, l'ensemble non vide des éléments x de S pour lesquels $f_S(x) \neq \varphi_S(x)$, aurait un premier élément p ($p \neq a$, $p \in S$) et les relations récurrentes ne détermineraient pas sans ambiguïté la valeur de la fonction pour $x = p$, contrairement à ce que nous avons supposé. L'*unicité* de la fonction f est donc assurée, sur toute section commençante, en particulier sur E .

Pour établir l'existence de la fonction f , associons à chaque élément x de E l'ensemble $S(x)$ des éléments de E inférieurs à x ; $x < y$ entraîne $S(x) \subset S(y)$: les sections commençantes $S(x)$ forment un ensemble ordonné par la relation d'inclusion et semblable à E ; adjoignons-lui E comme dernier élément : nous obtenons ainsi un ensemble bien ordonné $\mathcal{E} = \{ \dots, S(x), \dots, E \}$. Montrons par induction transfinie qu'il y a, quel que soit $S \in \mathcal{E}$, une fonction $f_S(s)$ vérifiant, pour tout $s \in S$, nos relations récurrentes. Distinguons deux cas.

1° *S a un dernier élément, z .* — Posons $S_1 = S - \{z\} \subset S$: il existe par hypothèse une fonction $f_{S_1}(x)$ vérifiant, pour tout élément de S_1 , les relations récurrentes. Posons donc

$$f_S(x) = f_{S_1}(x) \quad \text{pour tout } x \in S_1$$

et prenons $f_S(z)$ égal à la valeur déterminée à partir des $f_{S_1}(x)$ par les relations récurrentes : la fonction $f_S(x)$ ainsi définie pour tout $x \in S$, répond à la question dans *S*.

2° *S n'a pas de dernier élément.* — Tout $x \in S$ appartient alors à un $S' \in \mathcal{E}$, tel que $S' \subset S$: il suffit de poser

$$f_S(x) = f_{S'}(x).$$

Cette définition est légitime, puisque $f_{S'}(x)$ existe par hypothèse et est, d'après la propriété d'unicité établie plus haut, indépendante du choix de $S' (\ni x)$.

Nous avons ainsi une fonction $f_S(x)$ répondant à la question quel que soit $S \in \mathcal{E}$; la fonction $f(x) = f_E(x)$ est la fonction cherchée.

On dit qu'un ensemble *E* vérifie l'*axiome du choix* s'il existe dans *E* une *fonction de choix*, c'est-à-dire une *loi associant simultanément à chaque partie non vide X de E un élément x appartenant à X* (appelé souvent *élément distingué* de *X*).

Il est clair qu'un ensemble bien ordonné possède cette propriété, puisqu'on peut associer à chaque partie non vide *A* son premier élément. La réciproque de ce fait évident constitue le *théorème de Zermelo* ⁽¹⁾.

THÉORÈME DE ZERMELO. — *Moyennant l'axiome du choix, tout ensemble E peut être bien ordonné.*

Pour la démonstration, nous renvoyons à la Note III (p. 433).

Remarques. — 1. Il y a lieu, semble-t-il, de distinguer l'axiome du choix tel qu'il vient d'être énoncé, regardé comme propriété *éventuelle* d'un ensemble (donc ne prêtant aucunement à la critique) et le postulat : *tout ensemble vérifie l'axiome du choix*, qui pourrait être désigné sous le nom de *postulat de Zermelo*. Ce postulat, lui, a soulevé diverses objections : la plus sérieuse est sans doute que, jusqu'à présent, il a été impossible de construire un bon ordre pour l'ensemble des nombres réels. Actuellement, d'importants résultats mathématiques reposent sur l'axiome du choix. Nous nous efforcerons de ne jamais employer cet axiome, ou un axiome équivalent, sans mentionner explicitement

(1) *Math. Ann.*, t. 59, 1904, p. 514; t. 65, 1908, p. 107.

cet emploi. On confère aux résultats ainsi établis une sorte de validité absolue en adoptant une fois pour toutes le postulat de Zermelo; en même temps, on réalise des simplifications appréciables (voir Note III, p. 439).

2. Remarquons aussi qu'on utilise souvent, en réalité, l'*axiome du choix sous une forme restreinte*, qui est la suivante. Soit $\mathcal{M} = \{A, B, \dots\}$ un ensemble de parties de E : E vérifie l'axiome du choix sous forme restreinte pour la famille de parties $\mathcal{M}$, s'il existe pour chaque partie $A \in \mathcal{M}$ une fonction de choix $\mathcal{L}_A$ associant à tout sous-ensemble non vide X de A un élément $x_A \in X$ (« élément distingué relatif à A ») ⁽¹⁾.

Énonçons maintenant un axiome d'un emploi particulièrement commode en Algèbre, et qui est dû à Max Zorn ⁽²⁾.

PRINCIPE DE L'ÉLÉMENT MAXIMAL, OU THÉORÈME DE ZORN. — *Si, dans un ensemble partiellement ordonné E , toute chaîne possède une borne supérieure ⁽³⁾, E contient au moins un élément maximal.*

Ce principe, qui peut s'énoncer sous d'autres formes, elles aussi souvent utiles, est équivalent à l'axiome du choix (voir Note III, p. 439).

Dans le cas d'un *ensemble discret* D , les éléments limites n'existent pas et l'induction transfinie comprend comme cas particulier un type de raisonnement plus simple : l'*induction complète* ou *raisonnement par récurrence*. Pour établir que tous les éléments de D ont une certaine propriété $\mathcal{P}$, il suffit de montrer que le premier élément a de D possède cette propriété, et qu'elle est vraie pour un élément $x(>a)$ dès qu'elle l'est pour le précédent x^- . De même, pour construire par récurrence une fonction $f(x)$, définie dans D , prenant ses valeurs dans un ensemble E' , il suffit de se donner la valeur $f(a)$ de cette fonction pour $x=a$, et une relation déterminant d'une façon unique, pour $x>a$, la valeur $f(x)$ à partir de $f(x^-)$. Le raisonnement général fait plus haut montre que $f(x)$ est définie sur D d'une façon unique ⁽⁴⁾.

(1) Lorsqu'un même sous-ensemble X de E est contenu à la fois dans différentes parties $A, B, \dots \in \mathcal{M}$, les éléments $x_A, x_B, \dots$ peuvent être différents. Sous cette forme restreinte, l'axiome est vérifié d'une façon évidente toutes les fois que les parties $A, B, \dots$ sont finies, dénombrables ou bien ordonnées.

(2) *A remark on method in transfinite Algebra* (Bull. Amer. Math. Soc., t. 41, 1935, p. 667). Voir aussi N. BOURBAKI, *Théorie des ensembles* (Actualités scientifiques et industrielles, n° 846, Paris, Hermann, 1939, p. 37).

(3) On exprime cette propriété en disant que E est un *ensemble inductif*.

(4) Les sections commençantes S_x considérées dans ce raisonnement sont d'ailleurs, comme on le voit aisément, les segments $[a, x^-]$ (cf. Note II, th. 2).

Comme application de ce mode de raisonnement, établissons la proposition suivante :

THÉOREME 4. — *Il y a identité entre les notions d'ensemble doublement bien ordonné et d'ensemble discret avec dernier élément.*

Comme nous l'avons vu plus haut, un ensemble doublement bien ordonné est un ensemble discret avec dernier élément.

Inversement, soit D un ensemble discret possédant un dernier élément z . Soit a le premier élément de D ; désignons par X l'ensemble des éléments x de D tels que le segment initial $[a, x]$ soit doublement bien ordonné. Nous avons $a \in X$. Soient $a < x$ et $x^- \in X$; considérons une partie P non vide de $[a, x]$: si $x \in P$, x est dernier élément de P ; si $x \notin P$, nous avons $P \subseteq [a, x^-]$, et P a encore un dernier élément puisque $x^- \in X$ par hypothèse. P a donc toujours un dernier élément (et aussi un premier, puisque D est bien ordonné). Nous avons donc $x \in X$, d'où $X = D$ et par conséquent, l'ensemble $D = [a, z]$ est doublement bien ordonné ⁽¹⁾.

Il y a plus : les ensembles discrets avec dernier élément ne sont autres que les ensembles finis. Mais il est clair que pour établir ce résultat fondamental, et même pour lui donner un sens, nous devons d'abord donner une définition des ensembles finis. Historiquement, c'est Dedekind qui, le premier, a proposé une définition *directe*, c'est-à-dire indépendante de la notion de nombre naturel : un ensemble E est fini s'il est impossible qu'une partie de E ait même puissance que E . En réalité, cette définition, si intéressante qu'elle soit, n'est pas à retenir, parce que la démonstration de son équivalence avec d'autres propriétés caractéristiques, fait intervenir l'axiome du choix.

Parmi les définitions directes des ensembles finis dont l'équivalence, et même l'équivalence avec la définition indirecte, peut être établie sans faire appel à l'axiome du choix, les plus remarquables sont les suivantes.

1. DÉFINITION ORDINALE [A. DENJOY ⁽²⁾]. — *Un ensemble est fini s'il peut être ordonné totalement, et s'il est semblable à lui-même dans tous les ordres possibles.*

2. DÉFINITION ORDINALE (STÄCKEL, ENRIQUÈS). — *Un ensemble est fini s'il peut être doublement bien ordonné.*

⁽¹⁾ On trouvera une autre démonstration dans la Note I (th. 14, p. 412).

⁽²⁾ *L'énumération transfinie*, t. III (*Études complémentaires sur l'ordination*), chap. I, 615-665.

2 bis. — Un ensemble est fini s'il est discret et possède un dernier élément.

3. DÉFINITION CARDINALE (TARSKI). — Un ensemble E est fini s'il vérifie la condition minimale (en d'autres termes si tout ensemble $\mathfrak{M}$ non vide de parties de E contient une partie A minimale, c'est-à-dire ne contenant aucune autre partie X appartenant à la famille $\mathfrak{M}$).

La théorie directe des ensembles finis, exposée dans la Note I (p. 401), établit, sans aucun recours à la notion de nombre naturel et par des moyens qui restent élémentaires, l'équivalence des propriétés précédentes. Elle apporte, en outre, quelques résultats fondamentaux : toute partie d'un ensemble fini est finie ; la réunion, (éventuellement la somme), le produit d'une famille finie d'ensembles finis, sont finis ; l'ensemble des parties d'un ensemble fini est fini.

Un ensemble non fini est dit *infini* ; il est indiqué d'étudier d'abord les *ensembles discrets (non vides) sans dernier élément*, que nous appellerons *ensembles naturels*. Cette étude, développée dans la Note II (p. 420), conduit aux résultats fondamentaux suivants.

Deux ensembles naturels quelconques sont semblables ; tout segment initial (donc tout segment) d'un ensemble naturel est fini (au sens de la théorie directe), et inversement tout ensemble fini est semblable à un segment initial, et à un seul, d'un ensemble naturel N , que l'on pourra choisir une fois pour toutes ; pour plus de commodité, les éléments de N seront appelés *nombres naturels*, nommés successivement *un, deux, trois, ...*, désignés par les symboles $1, 2, 3, \dots$, et l'on dira que l'ensemble fini $F \leftarrow \rightarrow [1, n]$ a n éléments ; deux ensembles finis ont même puissance s'ils ont le même nombre d'éléments, et seulement dans ce cas. Tout ensemble ayant même puissance que N est dit *dénombrable*.

On voit facilement que tout ensemble naturel vérifie les axiomes de Peano (voir Note II), et inversement. Les propriétés classiques des nombres naturels et des opérations sur ces nombres en résultent, d'une façon connue, et il est facile d'obtenir en outre l'équivalence des définitions directes des ensembles finis avec la définition reposant sur la notion de nombre naturel, introduit au moyen des axiomes de Peano.

Remarque. — La théorie qui vient d'être esquissée est sensiblement plus longue que celle qui consiste à introduire d'abord, au moyen des axiomes de Peano, l'ensemble N des nombres naturels et à appeler fini tout ensemble vide ou ayant même puissance qu'un segment initial $[1, n]$ de N (voir première

édition, Note I). Mais elle apporte un ensemble de faits beaucoup plus riche, et est plus satisfaisante pour l'esprit en ce qu'elle ne fait pas dépendre la théorie des ensembles finis de la définition et des propriétés d'un ensemble infini N . On reconnaîtra d'ailleurs que les définitions 1, 2 et 2 *bis* présentent un caractère intuitif satisfaisant, tandis que 3 a l'avantage d'être un cas particulier d'une condition dont l'emploi, en Algèbre, est devenu extrêmement courant.

En dernière analyse, les progrès récents de cette partie élémentaire de la Théorie des Ensembles montrent qu'on ne peut plus accepter le jugement de J. Cavaillès (que nous faisons nôtre dans la première édition, p. 267) : « Le moyen employé uniformément pour démontrer ces équivalences (des définitions directes des ensembles finis) est l'induction complète; il semble donc que, sous-jacent à chacune de ces définitions, se trouve un renvoi à la *définition arithmétique ordinaire*, la construction progressive de l'ordre, intuition irremplaçable, comme le voulait Poincaré. Seule, la propriété prise par Dedekind comme première définition est pure de toute notion d'ordre : elle est démontrable à partir des autres définitions, mais ne permet pas de démontrer les propriétés énoncées dans celle-ci à moins que l'on n'ait recours à un instrument sur lequel concentraient leurs attaques, au début du siècle, la plupart des mathématiciens hostiles à la Théorie des Ensembles, l'axiome du choix... » (J. CAVAILLÈS, *Remarques sur la formation de la Théorie abstraite des Ensembles*, p. 113).

L'induction complète, nous l'avons vu, appartient comme instrument logique aux ensembles *discrets*, finis ou infinis, la distinction entre les deux types se faisant par l'existence ou la non-existence d'un dernier élément, caractère parfaitement intuitif. En elle-même, la définition de Tarski est aussi pure de toute notion d'ordre que celle de Dedekind, et elle se révèle équivalente à la définition de Denjoy et à celle de Stäckel-Enriquès sans qu'aucun recours à l'axiome du choix soit nécessaire. Il en est d'ailleurs de même pour l'équivalence avec la définition de Russell et Whitehead (*voir* Note I, th. 20, p. 416).

Considérons une application α de l'ensemble N des nombres naturels dans un ensemble donné E : cette application, définie par la donnée des images $a_n = \alpha(n)$, prises dans l'ordre de leurs indices, est ce qu'on appelle une *suite* S . On écrit

$$S = \{ a_1, a_2, \dots, a_n, \dots \}.$$

Il importe de remarquer que les éléments d'une suite ne sont *pas forcément distincts* : ainsi, on pourra considérer une suite de la forme $\{ a, a, \dots, a, \dots \}$. En ne conservant dans une suite S que les éléments distincts, ce qu'on peut faire en barrant tout élément égal à un élément placé avant lui, on obtient un ensemble M_S associé à cette suite, fini ou infini (dans ce dernier cas, dénombrable, puisque toute partie infinie de l'ensemble des nombres naturels est dénombrable, Note II, p. 425).

11. Treillis. — On appelle *treillis* ou *ensemble réticulé* ⁽¹⁾ un

⁽¹⁾ En anglais, *lattice*; en allemand, *Verband*. Nous donnons ici seulement quelques notions fondamentales et un petit nombre de résultats que nous aurons à utiliser. On

ensemble partiellement ordonné T dans lequel deux éléments quelconques x, y ont une *borne inférieure* (ou *minorant maximum*) et une *borne supérieure* (ou *majorant minimum*).

LEMME. — Si deux parties A, B d'un ensemble partiellement ordonné E ont des bornes supérieures a, b et si la borne supérieure $s = a \vee b$ existe, s est la borne supérieure de la réunion $R = A \cup B$.

L'élément s , au moins égal à a ou à b , est un majorant pour A et pour B , donc pour R . Si t est un majorant de R , donc de A , on a $t \geq a$, de même $t \geq b$, donc $t \geq s$: s est bien majorant minimum de R .

Du lemme précédent, de la proposition *duale* ⁽¹⁾ et d'un raisonnement immédiat, résulte que toute partie finie $F = \{x_1, x_2, \dots, x_n\}$ d'un treillis T a une borne inférieure, $\bigcap_{i=1, \dots, n} x_i$, $\bigcap_{x \in F} x$ ou $\bigwedge_{x \in F} x$ et une borne supérieure $\bigcup_{i=1, \dots, n} x_i$, $\bigcup_{x \in F} x$ ou $\bigvee_{x \in F} x$.

On appelle *sous-treillis* d'un treillis T un sous-ensemble non vide S contenant, en même temps que deux éléments x, y , leur borne inférieure $x \cap y$ et leur borne supérieure $x \cup y$. S est donc encore un treillis par rapport à la trace O_S de l'ordre O de T . Mais inversement, un sous-ensemble S de T peut être un treillis par rapport à O_S sans être un sous-treillis de T : il en est ainsi pour le sous-ensemble $S = \{a, c, c', e\}$ du treillis T défini par le diagramme ci-dessous (*fig. 3*).

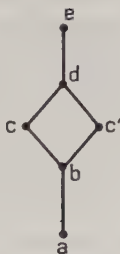


Fig. 3.

trouvera une étude développée de ces questions dans les *Leçons sur la Théorie des Treillis, des structures algébriques ordonnées et des Treillis géométriques*, par M. L. DUBREIL-JACOTIN, L. LESIEUR et R. CROISOT (*Cahiers scient.*, fasc. XXI, 1953, Gauthier-Villars), et un exposé systématique dans *Lattice Theory*, par G. BIRKHOFF (*Amer. Math. Soc.*, Colloquium Publications, XXV, New-York, 1948).

⁽¹⁾ Dans un treillis, la proposition *duale* d'une proposition est celle que l'on en déduit en remplaçant $\leq$ par $\geq$, borne supérieure par borne inférieure et inversement.

On appelle *demi-treillis* un ensemble U partiellement ordonné dans lequel deux éléments quelconques x, y ont toujours une *borne supérieure*; on voit comme plus haut que toute partie finie de U a une borne supérieure. Un $\cap$ -*demi-treillis* (inter-demi-treillis) est un ensemble partiellement ordonné dans lequel deux éléments quelconques x, y ont toujours une *borne inférieure*; toute partie finie de U a alors une borne inférieure.

Un treillis T est *complet* si toute partie non vide de T a une borne inférieure et une borne supérieure. Un treillis complet a un *élément maximum* (ou universel) et un *élément minimum* (ou élément nul). De même, un demi-treillis U est *complet* si toute partie non vide de U a une borne supérieure; de cette définition, on déduit par dualité celle d'un $\cap$ -demi-treillis complet.

Tout treillis, demi-treillis ou $\cap$ -demi-treillis *fini* est *complet*, mais on a d'autres conditions *suffisantes* beaucoup plus générales : ce sont les importantes *conditions de chaîne*, que nous énoncerons pour un ensemble partiellement ordonné quelconque.

Un ensemble partiellement ordonné E vérifie la *condition de chaîne ascendante* si toute chaîne strictement croissante indexée par les nombres naturels

$$(C) \quad a_1 \subset a_2 \subset \dots \subset a_n \subset \dots$$

est *nécessairement finie*, ou, ce qui revient au même, si dans toute chaîne faiblement croissante infinie indexée par les nombres naturels

$$(C') \quad x_1 \subseteq x_2 \subseteq \dots \subseteq x_n \subseteq \dots,$$

tous les éléments sont égaux à partir d'un certain rang.

On dit, d'autre part, que E vérifie la *condition maximale* si toute partie non vide de E possède un élément maximal. Il est clair que la condition maximale entraîne la condition de chaîne ascendante, puisqu'une chaîne C ou C' aura un élément maximal, qui sera nécessairement maximum.

La *réciproque* est vraie moyennant l'*axiome du choix*. Soit, en effet, a_1 l'élément distingué de $E_1 \subseteq E$: s'il est maximal, la réciproque est établie. Sinon, soit a_2 l'élément distingué de l'ensemble E_2 des éléments x de E_1 vérifiant $x \supset a_1$; si a_2 est maximal dans E_1 , la proposition est établie. Sinon, le raisonnement se poursuit ⁽¹⁾. La condition de chaîne ascendante étant supposée vérifiée, on

⁽¹⁾ On notera que c'est grâce à l'axiome du choix que l'on peut regarder comme définie la suite $\{a_1, a_2, \dots\}$ sur laquelle on raisonne.

rencontre au bout d'un nombre fini d'opérations un élément maximal.

Remarquons encore que, si la *condition maximale* est vérifiée dans E, on dispose du mode de *raisonnement par induction* suivant : *Pour établir que tous les éléments de E ont une certaine propriété P, il suffit de montrer que, si un élément a n'avait pas cette propriété, il existerait un élément $a' \supset a$ qui ne l'aurait pas non plus (ce qui exige, en particulier, que l'élément maximum de E, s'il existe, ait la propriété P).* Ce point étant établi, on voit en effet que l'ensemble des éléments qui n'ont pas la propriété P est vide car, dans le cas contraire, il contiendrait un élément *maximal*, ce qui est contradictoire.

On définit, par dualité, la *condition de chaîne descendante* et la *condition minimale*; la seconde entraîne la première; moyennant l'axiome du choix, elle lui est équivalente.

LEMME. — *Moyennant l'axiome du choix, un demi-treillis U vérifiant la condition de chaîne ascendante est complet; toute union $u = \bigcup_{s \in S} s$ ($S \subseteq U$) est union finie : $u = \bigcup_{i=1, \dots, m} s_i$.*

Soit $s_1 = x_1$ l'élément distingué de S; s'il est élément maximum, le lemme est établi; sinon, soit s_2 l'élément distingué de l'ensemble non vide des éléments de S qui ne sont pas inférieurs ou égaux à x_1 ; on a $x_2 = s_1 \cup s_2 \supset x_1$. Si x_2 est supérieur ou égal à tout élément de S, x_2 est borne supérieure de S. Sinon, le raisonnement se poursuit, mais la chaîne croissante $x_1 \subset x_2 \subset \dots$ ne pouvant avoir qu'un nombre fini de termes, on obtient un élément $x_m = s_1 \cup s_2 \cup \dots \cup s_m$ ($s_i \in S$) qui est union des éléments de S, et même union d'un nombre fini d'entre eux.

Du lemme précédent et de la proposition duale, nous déduisons :

THÉOREME 1. — *Moyennant l'axiome du choix, un treillis T qui vérifie les conditions de chaîne ascendante et descendante, est complet.*

On peut affaiblir les hypothèses et établir la proposition suivante, et sa duale.

THÉOREME 2. — *Un $\cap$ -demi-treillis complet I possédant un élément maximum ε , est un treillis complet.*

Il suffit de montrer que toute partie X non vide de I a une borne

supérieure s . Or, l'ensemble M des majorants m de X , non vide, puisqu'il contient z , possède une borne inférieure s . Soit $x \in X$: la relation $x \subseteq m$, pour tout $m \in M$, entraîne $x \subseteq s$; s appartient donc à M et en est élément minimum, c'est-à-dire borne supérieure de X .

COROLLAIRE. — *Si une partie S d'un treillis complet T vérifie les deux conditions suivantes, appelées conditions de Moore :*

- a. L'élément universel u de T appartient à S ,*
- b. Si X est une partie non vide de S , la borne inférieure de X dans T appartient à S ,*

S est un treillis complet; l'intersection dans S est la même que dans T ; l'union $\bigvee$ dans S est donnée par

$$(1) \quad \bigvee_{a \in A} a = \bigcap_{m \in M(A, S)} m,$$

où $M(A, S)$, ($A \subseteq S$) est l'ensemble des éléments de S qui majorent A .

D'après *b*, toute partie non vide X admet par rapport à la trace O_S de l'ordre O de T , une borne inférieure qui coïncide avec celle que l'on a dans T : S est donc un $\cap$ -demi-treillis complet. D'autre part, S a un élément maximum u ; S est donc, d'après le théorème 2, un treillis complet (pour l'ordre O_S), dans lequel l'union est définie par la relation (1). En général, l'ensemble $M(A, S)$ est une partie véritable de l'ensemble $M(A, T)$ des majorants de A dans T , et alors l'union dans S ne coïncide pas avec l'union dans T (voir l'exemple 4).

CAS PARTICULIER. — *Toute famille $\mathcal{S}$ de parties d'un ensemble E qui comprend E comme élément et, en même temps que les parties d'une sous-famille $\mathcal{F}$ de $\mathcal{S}$, leur intersection, est un treillis complet; la relation d'ordre est l'inclusion, la borne inférieure est l'intersection au sens de la théorie des ensembles, mais l'union $\bigvee$ est, en général, distincte de la réunion (voir l'exemple 3).*

Un cas intéressant dans lequel le corollaire du théorème 2 s'applique est celui des *fermetures*. Une application

$$(\varphi) \quad x \rightarrow \bar{x}$$

d'un ensemble partiellement ordonné E en lui-même est appelée *fermeture* si elle possède les trois propriétés suivantes :

1° $x \subseteq \bar{x}$ (φ est extensive);

2° $\bar{\bar{x}} = x$ (φ est idempotente);

3° $x \subseteq y$ entraîne $\bar{x} \subseteq \bar{y}$ (φ est isotone).

Un élément f est *fermé* (pour φ) s'il coïncide avec son image $\bar{f}$, $f = \bar{f}$. D'après 2°, tout $\bar{x}$ est fermé; d'après 1°, tout élément maximal (éventuel) est fermé.

En particulier, l'élément maximum d'un treillis complet T est fermé pour toute fermeture définie dans T .

LEMME. — Dans un treillis complet T , l'intersection ou borne inférieure i d'un ensemble non vide F d'éléments fermés (par rapport à une fermeture donnée φ) est un élément fermé.

La relation $i \subseteq f$ entraîne $\bar{i} \subseteq \bar{f} = f$ pour tout $f \in F$, d'où $\bar{i} \subseteq i$ et, d'après 1°, $\bar{i} = i$.

D'après ce qui précède, l'ensemble S des éléments fermés d'un treillis complet vérifie les deux conditions a , b de Moore. Le corollaire établi plus haut donne donc le

THÉORÈME 3 (THÉORÈME DE MOORE). — L'ensemble S des éléments d'un treillis complet T , qui sont fermés pour une fermeture φ donnée, est un treillis complet, dans lequel l'union est définie par

$$(1') \quad \bigvee_{f \in F} f = \bigcap_{s \in M(F, S)} s$$

[$M(F, S)$ désigne l'ensemble des majorants de F dans S].

Inversement, à une partie S vérifiant les conditions a et b de Moore, dans un treillis complet T , correspond une fermeture φ telle que S soit l'ensemble des éléments fermés correspondants.

Posons, en effet, pour tout $x \in T$,

$$(2) \quad \bar{x} = \bigcap_{x \subseteq s \in S} s.$$

Cet élément $\bar{x}$, qui existe d'après a , est, d'après b , un élément de S ; comme $s \in S$ entraîne $\bar{s} = s$, S est l'ensemble des $\bar{x}$. De plus, nous avons $x \subseteq \bar{x}$, puis

$$\bar{\bar{x}} = \bigcap_{\bar{x} \subseteq s \in S} s = \bar{x},$$

puisque $x \in S$; enfin $x \subseteq y$ entraîne d'après (2), $\bar{x} \subseteq \bar{y}$: l'application $x \rightarrow \bar{x}$ est bien une fermeture.

Plus généralement, à une *partie* non vide X de T , nous pouvons associer l'élément de S

$$(3) \quad \bigcap_{s \in \mathcal{M}(X, S)} s = \sigma(X)$$

qui est le plus petit élément $\bar{X}$ de S contenant chaque élément x de X .

Exemples. — 1. Un ensemble E totalement ordonné est un treillis où

$$a \vee b = \text{Max}(a, b), \quad a \wedge b = \text{Min}(a, b).$$

Ce treillis n'est pas nécessairement complet (exemples : l'ensemble des nombres naturels, celui des nombres rationnels, etc.).

2. L'ensemble $\mathcal{X}(E)$ des parties d'un ensemble E , ordonné par l'inclusion, est un treillis complet, car, d'après les propriétés établies au paragraphe 2, toute famille $\mathcal{F}$ de parties a pour borne inférieure l'intersection

$$I = \bigcap_{M \in \mathcal{F}} M$$

et pour borne supérieure la réunion

$$R = \bigcup_{M \in \mathcal{F}} M.$$

3. L'ensemble $\mathcal{S}$ des segments $[a, b]$ portés par une droite, ordonné par inclusion, est un demi-treillis, mais n'est pas un treillis (voir § 9, ex. 4, p. 40). Ce demi-treillis $\mathcal{S}$ n'est pas complet, puisque, par exemple, l'ensemble des segments $[-n, +n]$ et celui des segments $[2n, 2n+1]$ ($n \in \mathbb{N}$), n'ont pas de borne supérieure.

4. Considérons le treillis T , fini, donc complet, défini par le diagramme ci-contre (cf. § 9, exerc. 2). Chacun des sous-ensembles $\{a, b_1, b_2, c_1, c_2, c_3, e\}$,

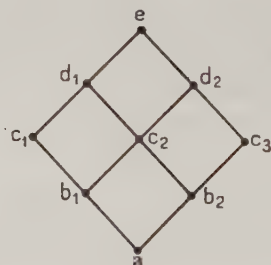


Fig. 4.

$\{a, b_1, b_2, e\}$, $\{a, b_1, c_3, e\}$ est un treillis complet dans lequel la borne inférieure est la même que dans T , mais aucun de ces sous-ensembles n'est un sous-

treillis de T ; dans le dernier, par exemple, $b_1 \vee c_3 = e$, tandis que, dans T , $b_1 \cup c_3 = d_2$.

Les sous-ensembles $\{a, b_1, c_1, c_2, d_1, e\}$, $\{a, c_1, c_3, e\}$, $\{a, b_1, c_3, d_2, e\}$ sont des sous-treillis.

5. Soit E un plan considéré comme ensemble de ses points (ou, plus généralement, un espace euclidien, voir Note IV, p. 441). L'ensemble $\mathcal{T}(E)$ des parties $X, Y, \dots$ de E , ordonné par inclusion, est un treillis complet $\mathcal{T}$. Un ensemble de points $X \in \mathcal{T}$ est dit *convexe* s'il contient, en même temps que deux points a, b tous les points du segment de droite ab . Les conditions de Moore sont vérifiées : le plan E tout entier est convexe, et toute intersection d'ensembles convexes est convexe, d'après la définition. L'ensemble $\mathcal{S}$ des ensembles convexes est un treillis complet dans lequel l'union, définie par (1), est, comme le montrent des exemples géométriques simples, distincte de la réunion des ensembles (l'union de deux segments équipollents est le parallélogramme qu'ils définissent). Associons à un ensemble X l'intersection $\bar{X}$ de tous les ensembles convexes contenant X : $\bar{X}$ est le plus petit ensemble convexe contenant X , et l'application $X \rightarrow \bar{X}$ est une fermeture. $\bar{X}$ est appelé *fermeture convexe* ou *enveloppe convexe* de X (cf. Alexandroff-Hopf *Topologie*, Berlin, Springer, 1935).

Exercices. — 1. On considère les ensembles ordonnés de l'exemple 5 (§ 9, p. 40). Examiner si chacun d'eux est un demi-treillis, un $\cap$ -demi-treillis, ou un treillis. Dans l'affirmative est-il complet ?

2. On ordonne partiellement l'ensemble N des entiers naturels en posant $a \leq b$ si $a = mb$, $m \in N$. Montrer que N est un treillis; indiquer la signification arithmétique de $x \cup y$ et de $x \cap y$ (comparer à l'exercice 1 du paragraphe 9, p. 41). Montrer que N est un demi-treillis complet; est-il un treillis complet ?

3. Soit $X \rightarrow \bar{X}$ une fermeture dans le treillis des parties X d'un ensemble E (1).

1° $\mathcal{F}$ étant une famille de parties de E , montrer que l'on a

$$(4) \quad \overline{\bigcap_{M \in \mathcal{F}} M} \subseteq \bigcap_{M \in \mathcal{F}} \bar{M}, \quad \bigcup_{M \in \mathcal{F}} \bar{M} \subseteq \overline{\bigcup_{M \in \mathcal{F}} M} = \bigcup_{M \in \mathcal{F}} \bar{M}.$$

2° $\mathcal{R}$ étant une équivalence définie dans E , l'application $X \rightarrow \bar{X}$, où $\bar{X} = \mathcal{R}(X)$ est l'extension saturée de X par rapport à une équivalence $\mathcal{R}$ définie dans E (voir § 5, p. 21), est une fermeture. Montrer que l'on peut, dans ce cas particulier, remplacer l'une des inclusions (4) par l'égalité.

(1) Dans cet exercice, le mot *fermeture* est pris au sens qui lui a été donné dans le texte. Toutefois, la plupart des fermetures considérées dans le treillis des parties d'un ensemble (en particulier la fermeture telle qu'on la considère en topologie, voir Note IV) vérifient la condition supplémentaire suivante : *la réunion de deux ensembles fermés est fermée* (axiome d'additivité). On pourra consulter, au sujet de cette importante notion : G. BIRKHOFF, *Lattice theory*, p. 49, et *On the Combination of topologies* (*Fundam. Math.*, t. 29, 1936, p. 156-166); O. ORE, *Combination of closure relations* (*Annals of Math.*, 44, 1943, p. 514-533), et *Some studies on closure relations* (*Duke Math. J.*, t. 10, 1943, p. 761-785).

E. — RELATIONS TRANSITIVES; RELATIONS D'ÉQUIVALENCE.

12. Produit transitif, fermeture transitive. — Comme nous l'avons vu (§ 3, p. 10), les relations binaires dans un ensemble E correspondent biunivoquement aux parties de l'ensemble-produit $E \times E$. Il en résulte que l'ensemble $\mathbf{P}$ de ces relations, ordonné par l'inclusion, est un *treillis complet* dans lequel la borne inférieure est l'intersection $\cap$, la borne supérieure la réunion $\cup$.

La relation universelle $\mathcal{U}$ est une équivalence (§ 5, p. 18); d'autre part, si toutes les relations $\mathcal{R}$ d'une famille Φ possèdent l'une des trois propriétés fondamentales : réflexivité, symétrie, transitivité, leur intersection la possède aussi. Par conséquent, l'ensemble des relations réflexives, Σ_1 , celui des relations symétriques Σ_2 et celui des relations transitives Σ_3 satisfont aux conditions de Moore (§ 11) : ce sont des treillis complets où l'intersection est la même que dans $\mathbf{P}$.

Toute relation contenant une relation réflexive, en particulier toute réunion de relations réflexives, est réflexive : l'union, dans le treillis Σ_1 des relations réflexives, coïncide donc avec la réunion, et Σ_1 est un *sous-treillis* de $\mathbf{P}$. De même, le treillis Σ_2 des relations symétriques est un *sous-treillis* de $\mathbf{P}$, puisque toute réunion de relations symétriques est symétrique.

Au contraire, la réunion de deux relations transitives n'est pas en général transitive.

Exemple 1. — Soit E l'ensemble des points $M = (x, y)$ du plan, où x et y désignent les coordonnées de M par rapport à des axes Ox, Oy ; posons

$$\begin{aligned} M \mathfrak{E} M' & \quad \text{si } x < x', \\ M \mathfrak{E}' M' & \quad \text{si } y < y'. \end{aligned}$$

Les relations $\mathfrak{E}, \mathfrak{E}'$ ainsi définies sont transitives. Considérons les points

$$A = (0, 2), \quad B = (1, 0), \quad C = (-1, +1);$$

nous avons $A \mathfrak{E} B$ et $B \mathfrak{E}' C$, donc $A(\mathfrak{E} \cup \mathfrak{E}')B$ et $B(\mathfrak{E} \cup \mathfrak{E}')C$, mais nullement $A(\mathfrak{E} \cup \mathfrak{E}')C$.

L'union $\vee$ dans le treillis complet Σ_3 des relations transitives est donc en général différente de la réunion; elle est définie, rappelons-le, par

$$(1) \quad \bigvee_{\mathcal{R} \in \mathcal{F}} \mathcal{R} = \bigcap_{\mathfrak{E} \in \mathcal{M}(\mathcal{F}, \Sigma_3)} \mathfrak{E},$$

où $\mathcal{M}(\mathcal{F}, \Sigma_3)$ désigne l'ensemble des relations *transitives* ($\in \Sigma_3$) qui majorent la famille $\mathcal{F}$ considérée.

La définition (1) garde un sens si l'on remplace la famille $\mathcal{F}$ de relations transitives par une *famille Φ de relations quelconques* : la relation

$$(2) \quad \mathcal{T} = \bigcap_{\mathcal{R} \in \mathcal{M}(\Phi, \Sigma_3)} \mathcal{R},$$

où $\mathcal{M}(\Phi, \Sigma_3)$ désigne l'ensemble des relations *transitives* qui majorent Φ , est la *plus fine relation transitive contenant toutes les relations $\mathcal{R} \in \Phi$* : on l'appelle *produit transitif* des relations $\mathcal{R}$ et l'on écrit aussi

$$\mathcal{T} = \prod'_{\mathcal{R} \in \Phi} \mathcal{R}$$

et, si $\Phi = \{\mathcal{R}_1, \mathcal{R}_2\}$,

$$\mathcal{T} = \mathcal{R}_1 \times \mathcal{R}_2 (= \mathcal{R}_2 \times \mathcal{R}_1).$$

On remarquera que la formule (2) est l'application au cas considéré ici, de la formule (3) du paragraphe 11, et que le produit transitif

$\prod'_{\mathcal{R} \in \Phi} \mathcal{R}$ contient la réunion ordinaire $\bigcup_{\mathcal{R} \in \Phi} \mathcal{R}$, et coïncide avec l'union

$\bigvee_{\mathcal{R} \in \Phi} \mathcal{R}$ du treillis Σ_3 lorsque toutes les relations $\mathcal{R}$ de Φ sont transitives.

Si la famille Φ se réduit à une seule relation, $\Phi = \{\mathcal{R}\}$ le produit transitif $\mathcal{T}$, qui est la plus petite relation transitive contenant $\mathcal{R}$, se note

$$(3) \quad \overline{\mathcal{R}} = \bigcap_{\mathcal{R} \subseteq \mathcal{R}' \in \Sigma_3} \mathcal{R}'$$

et est appelé *fermeture transitive* de $\mathcal{R}$. L'application $\mathcal{R} \rightarrow \overline{\mathcal{R}}$ est, en effet, une *fermeture* au sens défini au paragraphe 11 [voir, en particulier, la formule (2), p. 53].

On peut donner une deuxième définition, souvent utile, du produit transitif. Posons

$$x\mathcal{T}'y$$

si et seulement s'il existe un ensemble fini $\{m_2, \dots, m_k\}$ d'éléments de E , tel qu'en posant $m_1 = x$, $m_{k+1} = y$, on ait

$$(4) \quad m_i \mathcal{R}_i m_{i+1}, \quad \text{où } \mathcal{R}_i \in \Phi \quad (i = 1, \dots, k)$$

(les relations $\mathcal{R}_i$ ne sont pas forcément deux à deux distinctes).

THÉOREME. — La relation $\mathcal{R}'$ ainsi définie coïncide avec le produit transitif,

$$\mathcal{R}' = \mathcal{R} = \prod_{\mathcal{R} \in \Phi}^t \mathcal{R}.$$

D'après sa définition, la relation $\mathcal{R}'$ est transitive [deux suites (4), écrites bout à bout, forment une suite de même nature]. De plus, $\mathcal{R}'$ contient chaque relation $\mathcal{R} \in \Phi$ ($k=1$, $\mathcal{R}_1 = \mathcal{R}$).

Si maintenant $\mathcal{G}$ est une relation transitive contenant toute relation $\mathcal{R} \in \Phi$, (4) entraîne $m_i \mathcal{G} m_{i+1}$ ($i=1, \dots, k$), d'où $x \mathcal{G} y$ et, par conséquent, $\mathcal{R}' \subseteq \mathcal{G}$; $\mathcal{R}'$ est la plus petite relation transitive majorant Φ , et nous avons bien $\mathcal{R}' = \mathcal{R}$.

COROLLAIRE. — Le produit transitif $\mathcal{R} = \prod_{\mathcal{R} \in \Phi}^t \mathcal{R}$ contient tout produit (ordinaire) d'un ensemble fini de relations, distinctes ou non, extrait de la famille Φ ⁽¹⁾. En particulier, si $\Phi = \{\mathcal{R}_1, \mathcal{R}_2\}$, on a

$$\mathcal{R}_1 \mathcal{R}_2 \subseteq \mathcal{R}_1 \times \mathcal{R}_2, \quad \mathcal{R}_2 \mathcal{R}_1 \subseteq \mathcal{R}_1 \times \mathcal{R}_2$$

et, si $\Phi = \{\mathcal{R}\}$:

$$\mathcal{R}^n \subseteq \overline{\mathcal{R}},$$

quel que soit le nombre naturel n .

D'après sa définition, la relation $\mathcal{R}'$ s'écrit ici

$$\mathcal{R}' = \bigcup_{n \in \mathbb{N}} \mathcal{R}^n$$

et l'égalité $\mathcal{R} = \mathcal{R}'$ nous donne

$$(5) \quad \overline{\mathcal{R}} = \bigcup_{n \in \mathbb{N}} \mathcal{R}^n.$$

Si la famille Φ contient au moins une relation réflexive $\mathcal{R}$, le produit transitif $\mathcal{R}$ est réflexif ($x \mathcal{R} x$ entraîne $x \mathcal{R} x$); en particulier, la fermeture transitive d'une relation réflexive est une relation de préordre.

Si toutes les relations de la famille Φ sont symétriques, leur produit transitif $\mathcal{R}$ l'est aussi, puisque, d'après (4), $x \mathcal{R} y$ entraîne $y \mathcal{R} x$.

Il en résulte que la fermeture transitive d'une relation $\mathcal{R}$ réflexive et symétrique est une relation d'équivalence, et c'est évidemment la plus fine équivalence contenant $\mathcal{R}$.

(1) Cette propriété explique le nom de produit transitif donné à la relation $\mathcal{R}$.

Considérons, en particulier, une application f (uniforme ou multi-forme) d'un ensemble E sur un ensemble E' , et la relation $\mathfrak{E}$ définie dans E par

$$x \mathfrak{E} x_1 \Leftrightarrow f(x) \mathfrak{E}' f(x_1)$$

(voir § 8, p. 31), évidemment réflexive et symétrique, et contenue, comme nous l'avons vu, dans l'équivalence $\mathcal{C}$ réalisant la décomposition de E en ensembles stables minimaux (p. 32). Nous avons donc, en désignant par $\overline{\mathfrak{E}}$ la fermeture transitive de $\mathfrak{E}$,

$$\mathfrak{E} \subseteq \mathcal{C}.$$

Chaque classe X modulo $\overline{\mathfrak{E}}$ est donc contenue dans une classe modulo $\mathcal{C}$, c'est-à-dire dans un ensemble stable minimal S , celui, par exemple, qui contient un élément quelconque x de X : $S = S_x$. Or, l'ensemble X lui-même est *stable*; si l'on a, en effet, $y \in f^{-1} f(X)$, cela signifie que $y \in f^{-1} f(p)$, où $p \in X$, ce qui peut s'écrire

$$y \mathfrak{E} p, \quad \text{avec} \quad p \overline{\mathfrak{E}} x.$$

Or, d'après (5), $p \overline{\mathfrak{E}} x$ signifie que l'on a $p \mathfrak{E}^n x$ pour un certain entier n ce qui entraîne $y \mathfrak{E}^{n+1} x$ et, par conséquent, encore d'après (5),

$$y \overline{\mathfrak{E}} x,$$

c'est-à-dire

$$y \in X, \quad \text{d'où} \quad f^{-1} f(X) \subseteq X,$$

ce qui entraîne l'égalité, puisqu'on a toujours, évidemment

$$X \subseteq f^{-1} f(X).$$

X , étant stable, coïncide nécessairement avec l'ensemble stable minimal S_x qui le contient et, puisqu'il en est ainsi pour toute classe X modulo $\overline{\mathfrak{E}}$, nous avons l'égalité

$$\overline{\mathfrak{E}} = \mathcal{C};$$

$\mathcal{C}$ est la plus petite relation d'équivalence, ou, ce qui revient au même, la plus petite relation transitive contenant $\mathfrak{E}$.

Exemple 2. — Dans le plan euclidien E , un *ensemble ouvert* est un ensemble M de points $m, \dots$, ayant la propriété suivante : quel que soit $m \in M$, il existe un cercle Γ_m de centre M dont tous les points appartiennent à M . Considérons alors, pour deux points m et p de M , la relation $\mathcal{R}$ suivante :

$$m \mathcal{R} p \quad \text{si et seulement si} \quad \Gamma_m \mathfrak{E} \Gamma_p,$$

Γ_m et Γ_p étant deux cercles de centres m, p contenus dans M . $\mathcal{R}$ est une relation réflexive et symétrique; sa fermeture transitive est une relation d'équivalence $\mathcal{S}$. Les classes modulo $\mathcal{S}$ sont, par définition, les *composantes connexes* de l'ensemble M ; M est *connexe* ou *d'un seul tenant* si $\mathcal{S}$ est la relation universelle dans M ⁽¹⁾.

Exercices. — 1. Quel est le produit transitif des relations $\mathcal{S}, \mathcal{S}'$ définies dans l'exemple 1 ?

2. 1° Si l'on remplace dans un produit transitif

$$\mathcal{Q} = \coprod_{\mathcal{R} \in \Phi} \mathcal{R}$$

une relation $\mathcal{R}$ par une relation $\mathcal{S} \supseteq \mathcal{R}$, on obtient un produit transitif $\mathcal{Q} \supseteq \mathcal{Q}$.

2° On ne change pas un produit transitif en y remplaçant une ou plusieurs relations par leur fermeture transitive.

3° Soient Φ_1, Φ_2 deux familles de relations binaires définies dans l'ensemble E , Φ leur réunion. On désigne respectivement par $\mathcal{Q}, \mathcal{Q}_1, \mathcal{Q}_2$ les produits transitifs des relations de Φ , de Φ_1 , de Φ_2 ; établir l'égalité

$$\mathcal{Q} = \mathcal{Q}_1 \times \mathcal{Q}_2.$$

3. Soit f une application (uniforme ou multiforme) d'un ensemble E sur un ensemble E' . On considère une relation $\mathcal{R}$ définie dans E et on lui associe les relations $\mathcal{R}'_0, \mathcal{R}'_1$ définies dans E' par :

$$\begin{aligned} x' \mathcal{R}'_0 y' & \text{ si l'on a } x \mathcal{R} y \text{ pour tout } x \in f^{-1}(x') \text{ et tout } y \in f^{-1}(y'), \\ x' \mathcal{R}'_1 y' & \text{ s'il existe } x \in f^{-1}(x') \text{ et } y \in f^{-1}(y') \text{ tels que } x \mathcal{R} y. \end{aligned}$$

1° Si $\mathcal{R}$ est transitive, $\mathcal{R}'_0$ l'est aussi; si $\mathcal{R}$ est réflexive, $\mathcal{R}'_1$ l'est; si $\mathcal{R}$ est symétrique, $\mathcal{R}'_0$ et $\mathcal{R}'_1$ le sont.

2° On a $\mathcal{R}'_0 \subseteq \mathcal{R}'_1$. Pour que l'égalité ait lieu, il faut et il suffit que $\mathcal{R}$ soit *f-invariante*, c'est-à-dire que l'on ait $\mathcal{S}\mathcal{R} \subseteq \mathcal{R}$ et $\mathcal{R}\mathcal{S} \subseteq \mathcal{R}$, donc que $\mathcal{R}$ soit respectée par la relation $\mathcal{S}$ considérée dans le texte :

$$x \mathcal{S} y \Rightarrow f(x) \mathcal{S} f(y).$$

On pourra rattacher à ce résultat le théorème 2 du paragraphe 5, page 22.

3° Une relation $\mathcal{S}'$ définie dans E' est dite *f-compatible* avec $\mathcal{R}$ si

$$x \mathcal{R} y \Rightarrow x' \mathcal{S}' y' \text{ pour tout } x' \in f(x) \text{ et tout } y' \in f(y).$$

Si, en outre, $\mathcal{R}$ est *f*⁻¹-compatible avec $\mathcal{S}'$, $\mathcal{R}$ et $\mathcal{S}'$ sont dites *f-équivalentes*.

⁽¹⁾ Pour une définition générale d'un ensemble connexe (s'appliquant à une partie d'un espace topologique quelconque), voir N. BOURBAKI, *Topologie générale*, chap. I : *Structures topologiques* (Act. Scient. et ind., t. 858, p. 70, Paris, Hermann, 1940).

Pour que $\mathcal{S}'$ soit f -compatible avec $\mathcal{R}$, il faut et il suffit que l'on ait $\mathcal{R}'_1 \subseteq \mathcal{S}'$. $\mathcal{R}'_1$ est la seule relation de E' qui puisse être f -équivalente à $\mathcal{R}$; pour qu'elle le soit, il faut et il suffit que $\mathcal{R}$ soit f -invariante.

4° L'équivalence $\mathcal{C} = \mathcal{S}$ décomposant E en sous-ensembles stables minimaux est f -invariante; $\mathcal{C}$ et la relation analogue $\mathcal{C}'$ dans E' sont f -équivalentes.

5° Si $\mathcal{S}'$ est f -compatible avec $\mathcal{R}$, elle l'est aussi avec toute relation $\mathcal{R}_1 \subset \mathcal{R}$.

Si $\mathcal{S}'$ est f -compatible avec une relation $\mathcal{R}$ réflexive, $\mathcal{S}'$ contient la relation $\mathcal{S}'$ [définie par $x' \mathcal{S}' y' \Leftrightarrow f^{-1}(x') \{ f^{-1}(y') \}$].

6° On suppose que $\mathcal{R}$ et $\mathcal{S}'$ sont des relations de préordre.

Montrer que $\mathcal{S}'$ est, en même temps, f -compatible avec $\mathcal{R}$ et avec $\mathcal{R} \times \mathcal{C} = \mathcal{R} \times \mathcal{S}$ ($\mathcal{C} = \mathcal{S}$, pour l'égalité des produits transitifs précédents, voir l'exercice 2).

La propriété précédente ramène la recherche des relations de préordre $\mathcal{S}'$ f -compatibles avec une relation de préordre $\mathcal{R}$, au cas où $\mathcal{R} \supseteq \mathcal{C}$. Dans ce cas, $\mathcal{R}_0 = \mathcal{R}'_1$ est f -équivalente à $\mathcal{R}$ et c'est la plus fine relation de préordre f -compatible avec $\mathcal{R}$.

Ces dernières propriétés subsistent si l'on suppose que $\mathcal{R}$ et $\mathcal{S}'$ sont des relations d'équivalence.

On pourra consulter : M. L. DUBREIL-JACOTIN, *Applications multiformes et relations d'équivalence* (C. R. Acad. Sc., t. 230, 1950, p. 906); P. DUBREIL, *Relations binaires et applications* (ibid., p. 1028); *Comportement des relations binaires dans une application multiforme* (ibid., p. 1242).

13. Produits de relations d'équivalences. — Dans le treillis des relations binaires d'un ensemble E , l'ensemble Σ des relations d'équivalence vérifie les conditions de Moore : Σ est donc un treillis complet. Considérons Σ comme sous-ensemble du treillis Σ_3 des relations transitives, dans lequel l'union $\vee$ est, comme nous l'avons vu, le produit transitif. Puisqu'un produit transitif est réflexif dès qu'un facteur l'est, et symétrique dès que tous les facteurs le sont, tout produit transitif d'une famille Φ d'équivalences est une équivalence; c'est la plus fine équivalence contenant toutes celles de Φ ⁽¹⁾ (puisque c'est déjà la plus fine relation transitive ayant cette propriété). On voit donc que l'union dans Σ coïncide avec l'union dans Σ_3 : le treillis des relations d'équivalence est un sous-treillis de celui des relations transitives.

D'après le théorème établi au paragraphe 12, si $\mathcal{R} = \prod_{\alpha \in \Phi}^t \mathcal{R}_\alpha$ est le produit transitif d'une famille Φ d'équivalences, on a $x \mathcal{R} y$ si et seulement s'il existe, dans l'ensemble E considéré, un ensemble

⁽¹⁾ Cf. G. BIRKHOFF, *On the structure of abstract Algebra* (Proc. Cambridge Phil. Soc., t. 31, 1935, p. 433-454).

fini $\{m_2, \dots, m_k\}$ tel qu'en posant $m_1 = x$, $m_{k+1} = y$, on ait

$$(1) \quad m_i \equiv m_{i+1} \quad (\mathcal{R}_i) \quad (i = 1, \dots, k)$$

où les $\mathcal{R}_i$ sont des équivalences, distinctes ou non, appartenant à Φ .

Dans la suite (1), on peut supposer $\mathcal{R}_i \neq \mathcal{R}_{i+1}$, car si $\mathcal{R}_i$ et $\mathcal{R}_{i+1}$ sont égales, on peut se contenter d'écrire $m_i \equiv m_{i+2} \quad (\mathcal{R}_i)$. Si, en particulier, Φ comprend seulement deux équivalences $\mathcal{R}$, $\mathcal{R}'$, les congruences d'une suite (1) seront prises alternativement modulo $\mathcal{R}$ et modulo $\mathcal{R}'$. On peut d'ailleurs convenir de commencer toujours par l'équivalence $\mathcal{R}$, en écrivant au besoin en tête $x \equiv x \quad (\mathcal{R})$, et de terminer par l'équivalence $\mathcal{R}'$:

$$(1') \quad x \equiv m_1 \equiv m_2 \quad (\mathcal{R}), \quad m_2 \equiv m_3 \quad (\mathcal{R}'), \quad \dots, \quad m_{2r-2} \equiv m_{2r-1} \equiv y \quad (\mathcal{R}').$$

Exemple. — Dans l'ensemble E des points de l'espace euclidien, regardons deux points A, A' comme équivalents modulo $\mathcal{S}$ s'ils coïncident ou si AA' est parallèle à une direction donnée D. Soit $\mathcal{S}'$ l'équivalence analogue définie à partir d'une direction D' non parallèle à D. A et A' sont équivalents modulo $\mathcal{T} = \mathcal{S} \times \mathcal{S}'$ s'ils coïncident ou sont parallèles à la direction de plan définie par D et D'. Il faut et il suffit pour cela qu'il existe un point B tel que AB soit parallèle à D et BA' parallèle à D', c'est-à-dire

$$A \equiv B \quad (\mathcal{S}) \quad \text{et} \quad B \equiv A' \quad (\mathcal{S}')$$

On peut donc, *ici*, ramener la suite (1') à ne contenir que deux signes d'équivalence et le produit $\mathcal{S} \times \mathcal{S}'$ coïncide avec le produit ordinaire $\mathcal{S}\mathcal{S}'$, et de même avec $\mathcal{S}'\mathcal{S}$. Étudions d'une façon générale les questions ainsi soulevées.

Le produit $\mathcal{R}\mathcal{R}'$ de deux relations d'équivalence est *réflexif*, mais en général il n'est pas symétrique, car $x\mathcal{R}\mathcal{R}'y$ (c'est-à-dire $x\mathcal{R}m$ et $m\mathcal{R}'y$) entraîne $y\mathcal{R}'\mathcal{R}x$. $\mathcal{R}\mathcal{R}'$ n'est pas non plus en général, transitif : $x\mathcal{R}\mathcal{R}'y$ et $y\mathcal{R}\mathcal{R}'z$ entraînent $x\mathcal{R}\mathcal{R}'\mathcal{R}\mathcal{R}'z$.

Le produit $\mathcal{R}\mathcal{R}'$ est *symétrique* si l'on a

$$(2) \quad \mathcal{R}'\mathcal{R} \subseteq \mathcal{R}\mathcal{R}'.$$

Mais, $\mathcal{R}$ et $\mathcal{R}'$ étant transitives ($\mathcal{R}^2 \subseteq \mathcal{R}$, $\mathcal{R}'^2 \subseteq \mathcal{R}'$), (2) entraîne

$$\mathcal{R}\mathcal{R}'\mathcal{R}\mathcal{R}' \subseteq \mathcal{R}^2\mathcal{R}'^2 \subseteq \mathcal{R}\mathcal{R}',$$

c'est-à-dire la *transitivité* de $\mathcal{R}\mathcal{R}'$. En outre, (2) entraîne (1)

$$(\mathcal{R}'\mathcal{R})^{-1} \subseteq (\mathcal{R}\mathcal{R}')^{-1}, \quad \text{c'est-à-dire} \quad \mathcal{R}^{-1}\mathcal{R}'^{-1} \subseteq \mathcal{R}'^{-1}\mathcal{R}^{-1}$$

(1) Rappelons la définition de l'inverse $\mathcal{S}^{-1}$ d'une relation $\mathcal{S}$:

$$x\mathcal{S}^{-1}y \Leftrightarrow y\mathcal{S}x.$$

En particulier, $x(\mathcal{R}\mathcal{R}')^{-1}y$ signifie $y\mathcal{R}\mathcal{R}'x$, c'est-à-dire $y\mathcal{R}m$ et $m\mathcal{R}'x$, ou $x\mathcal{R}'^{-1}m$ $m\mathcal{R}^{-1}y$, ou enfin $x\mathcal{R}'^{-1}\mathcal{R}^{-1}y$; on a donc :

$$(\mathcal{R}\mathcal{R}')^{-1} = \mathcal{R}'^{-1}\mathcal{R}^{-1}.$$

ou puisque ici $\mathcal{R}$ et $\mathcal{R}'$ sont symétriques, $\mathcal{R}\mathcal{R}' \subseteq \mathcal{R}'\mathcal{R}$ et, par conséquent l'égalité

$$(2') \quad \mathcal{R}'\mathcal{R} = \mathcal{R}\mathcal{R}'.$$

En résumé, pour que le produit $\mathcal{R}\mathcal{R}'$ de deux relations d'équivalence soit symétrique, il faut et il suffit qu'on ait l'égalité (2') c'est-à-dire que $\mathcal{R}$ et $\mathcal{R}'$ soient *permutables*; alors, $\mathcal{R}\mathcal{R}'$ est aussi transitif; donc, la permutabilité (2') est aussi une condition nécessaire et suffisante pour que $\mathcal{R}\mathcal{R}'$ soit une équivalence (contenant $\mathcal{R}$ et $\mathcal{R}'$).

Or, le produit ordinaire $\mathcal{R}\mathcal{R}'$ est contenu dans le produit transitif $\mathcal{R} \times \mathcal{R}'$; si donc $\mathcal{R}\mathcal{R}'$ est une équivalence, il coïncide avec le produit transitif $\mathcal{R} \times \mathcal{R}'$, et inversement. Nous pouvons donc énoncer la proposition suivante :

THÉOREME 1. — *Pour que le produit ordinaire $\mathcal{R}\mathcal{R}'$ de deux équivalences définies dans un ensemble E soit une équivalence, ou pour qu'il coïncide avec le produit transitif $\mathcal{R} \times \mathcal{R}'$, il faut et il suffit que $\mathcal{R}$ et $\mathcal{R}'$ soient permutables (il suffit même qu'un des produits $\mathcal{R}\mathcal{R}'$, $\mathcal{R}'\mathcal{R}$ soit contenu dans l'autre).*

COROLLAIRE. — *Soient P une classe modulo $\mathcal{R} \times \mathcal{R}'$, A une classe modulo $\mathcal{R}$, A' une classe modulo $\mathcal{R}'$, toutes deux contenues dans P : si $\mathcal{R}$ et $\mathcal{R}'$ sont permutables, A et A' se coupent :*

$$A \cap A' \neq \emptyset.$$

Soient, en effet, a un élément de A, a' un élément de A'; nous avons

$$a \equiv a' \quad (\mathcal{R}), \quad \text{c'est-à-dire} \quad a \equiv a' \quad (\mathcal{R}\mathcal{R}').$$

Il existe donc un élément x de E tel que

$$a \equiv x \quad (\mathcal{R}) \quad \text{et} \quad x \equiv a' \quad (\mathcal{R}'),$$

d'où $x \in A \cap A'$ et, par suite, $A \cap A' \neq \emptyset$.

La propriété de permutabilité de deux relations d'équivalence $\mathcal{R}$, $\mathcal{R}'$ peut s'exprimer au moyen des classes des partitions correspondantes de l'ensemble E. Désignons par A, B, ... les classes modulo $\mathcal{R}$, par A', B', ... les classes modulo $\mathcal{R}'$. Nous dirons que $\mathcal{R}$ et $\mathcal{R}'$ sont *associables*, et nous écrirons

$$\mathcal{R} \square \mathcal{R}'$$

si les conditions

$$(3) \quad A \cap A' \neq \emptyset, \quad A' \cap B \neq \emptyset, \quad B \cap B' \neq \emptyset$$

entraînent

$$(4) \quad A \cap B' \neq \emptyset,$$

ce qu'on peut encore écrire

$$\text{si } A \cap A' \cap B \cap B' \text{ entraîne } A \cap B'.$$

THÉOREME 2. — Deux relations d'équivalence $\mathcal{R}$ et $\mathcal{R}'$, définies dans un ensemble E , sont associables si elles sont permutables, et dans ce cas seulement.

1° Soit $\mathcal{R} \square \mathcal{R}'$; supposons que l'on ait $a \mathcal{R}' \mathcal{R} b$, c'est-à-dire $a \mathcal{R}' m$ et $m \mathcal{R} b$, et désignons par A, A' les classes modulo $\mathcal{R}, \mathcal{R}'$ qui contiennent a , par B, B' les classes modulo $\mathcal{R}, \mathcal{R}'$ qui contiennent b . Nous avons

$$m \in A' \quad \text{et} \quad m \in B,$$

d'où (3), et, par conséquent. (4) : soit

$$p \in A \cap B';$$

nous avons $a \mathcal{R} p$ et $p \mathcal{R}' b$, donc $a \mathcal{R} \mathcal{R}' b$, d'où $\mathcal{R}' \mathcal{R} \subseteq \mathcal{R} \mathcal{R}'$, ce qui entraîne la permutabilité.

2° Soit $\mathcal{R} \mathcal{R}' = \mathcal{R}' \mathcal{R}$; considérons quatre classes A, B, A', B' vérifiant (3) et soient

$$a \in A \cap A', \quad m \in A' \cap B, \quad b \in B \cap B',$$

d'où $a \mathcal{R}' m$ et $m \mathcal{R} b$, c'est-à-dire $a \mathcal{R}' \mathcal{R} b$. Il en résulte $a \mathcal{R} \mathcal{R}' b$; il existe donc un élément p de E tel que $a \mathcal{R} p$ et $p \mathcal{R}' b$, d'où $p \in A \cap B'$; (4) est vérifiée et l'on a bien

$$\mathcal{R} \square \mathcal{R}'.$$

Si $\mathcal{R}$ est contenue dans $\mathcal{R}'$, $\mathcal{R} \subseteq \mathcal{R}'$, les équivalences $\mathcal{R}$ et $\mathcal{R}'$ sont permutables puisque le produit $\mathcal{R} \mathcal{R}'$ et le produit transitif $\mathcal{R} \times \mathcal{R}'$ coïncident tous deux avec $\mathcal{R}'$ ⁽¹⁾.

L'associabilité est une propriété réflexive et symétrique, mais non transitive, comme le montre l'exemple suivant.

(1) Il est immédiat aussi, directement, que $\mathcal{R}$ et $\mathcal{R}'$ sont associables, car les conditions (3) entraînent ici $B \subseteq A'$, $B \subseteq B'$, d'où $A' = B'$, et $A \subseteq A'$ donc $A \subseteq B'$ et, par conséquent (4).

Exemple. — Dans l'ensemble E de quatre points d'une droite, considérons les équivalences suivantes (les points équivalents sont situés à l'intérieur d'un même contour).

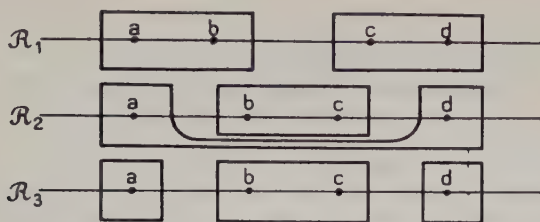


Fig. 5

On a $\mathcal{R}_1 \sqsubset \mathcal{R}_2$ et $\mathcal{R}_2 \supset \mathcal{R}_3$, donc $\mathcal{R}_2 \sqsupset \mathcal{R}_3$. Mais $\mathcal{R}_1$ et $\mathcal{R}_3$ ne sont pas permutable; on a, en effet, $a \mathcal{R}_1 \mathcal{R}_3 c$, mais non $a \mathcal{R}_3 \mathcal{R}_1 c$.

Exercices. — 1. Dans un ensemble E comprenant n éléments, il y a un nombre fini N_n d'équivalences distinctes; établir la relation ⁽¹⁾

$$N_n = \sum_{h=1}^n C_{n-1}^{h-1} N_{n-h} \quad (N_0 = 1).$$

(On remarquera qu'il y a C_{n-1}^{h-1} classes possibles de h éléments contenant un élément donné a .)

2. Si $\mathcal{R} \subseteq \mathcal{R}'$, on a

$$\mathcal{R} \cap \mathcal{R}' = \mathcal{R}, \quad \mathcal{R} \times \mathcal{R}' = \mathcal{R}'.$$

Il en résulte, quelles que soient les équivalences $\mathfrak{S}$ et $\mathfrak{S}'$:

$$\mathfrak{S} \cap (\mathfrak{S} \times \mathfrak{S}') = \mathfrak{S}, \quad \mathfrak{S} \times (\mathfrak{S} \cap \mathfrak{S}') = \mathfrak{S}.$$

3. Soient $\mathcal{R}$, $\mathcal{R}'$, $\mathfrak{S}$ trois relations d'équivalence définies dans le même ensemble E .

1° Si l'on a

$$\mathfrak{S} \sqsubset \mathcal{R}, \quad \mathfrak{S} \sqsubset \mathcal{R}'.$$

il en résulte

$$\mathfrak{S} \sqsubset \mathcal{R} \times \mathcal{R}'.$$

2° Si l'on a

$$\mathfrak{S} \subseteq \mathcal{R}, \quad \mathfrak{S} \sqsubset \mathcal{R}',$$

il en résulte

$$\mathfrak{S} \sqsubset \mathcal{R} \cap \mathcal{R}' \quad (2)$$

⁽¹⁾ Cf. A. C. AITKEN, *Edimburg Math. Notes* t. 28, 1933, XVIII et XXIII, ainsi que G. WILLIAMS, *Amer. Math. Monthly*, t. 52, 1945, p. 233.

⁽²⁾ Cf. P. DUBREIL et M. L. DUBREIL-JACOTIN, *Théorie algébrique des relations d'équivalence* (*J. Math.* 9^e série, t. 18, 1939, p. 75). Voir aussi O. ORE, *Theory of*

4. On considère un ensemble $M = \{\alpha, \beta, \dots\}$, deux relations d'équivalence $\mathcal{R}, \mathcal{R}'$ définies dans M , les ensembles-quotients $E = M/\mathcal{R}$, $E' = M/\mathcal{R}'$ et l'application multiforme f de E sur E' définie par

$$f(x) = \{x'\}_{x'} \setminus x \quad (\text{ensemble des classes } x' \in E' \text{ coupant } x).$$

Pour que l'application f soit semi-uniforme (voir § 8, p. 35), il faut et il suffit que $\mathcal{R}$ et $\mathcal{R}'$ soient associables (ou, ce qui revient au même, permutables).

Equivalence relations (Duke Math. J., t. 9, 1942, p. 573-627), et P. M. WHITMAN, *Lattices, Equivalence relations and subgroups* (Bull. Amer. Math. Soc., t. 52, 1946, p. 507-522), où est établi le résultat suivant : tout treillis est isomorphe à un sous-treillis du treillis des relations d'équivalence d'un certain ensemble (c'est-à-dire lui correspond biunivoquement avec conservation des opérations $\cap$ et $\cup$). Le comportement des relations d'équivalence par rapport à une relation d'ordre a été étudié récemment par M. L. DUBREIL-JACOTIN et R. CROISOT, *Équivalences régulières dans un ensemble ordonné* (Bull. Soc. Math. de France, t. 80, 1952, p. 11-35).



CHAPITRE II.

OPÉRATIONS.

A. — GROUPOIDES. ALGÈBRES.

1. Loi de composition. — Nous appellerons *loi de composition*, *opération abstraite*, ou simplement *opération*, définie dans un ensemble E non vide, toute loi associant à chaque couple ordonné (a, b) d'éléments de E , *termes* de l'opération, un élément bien déterminé de E , *résultat* de l'opération. Une opération dans un ensemble E non vide est donc une application du produit $E \times E = E^2$ dans E . Un ensemble où est définie une telle opération prend le nom de *système* ou de *groupoïde* ⁽¹⁾. Un ensemble où existent plusieurs opérations est appelé *domaine* ou *algèbre*.

Le résultat d'une opération O effectuée sur les éléments a et b se désigne par

$$c = aOb.$$

Mais, pour les opérations qui ont un sens concret, on remplace ordinairement la lettre O par des signes qui leur sont spécialement affectés, et dont les principaux sont les suivants :

- + pour l'addition (des nombres, des vecteurs, des polynomes, etc.);
- pour la soustraction (des nombres, des vecteurs, etc.);

⁽¹⁾ Le mot *groupoïde* est employé dans ce sens par O. Ore [cf. O. Ore et B. A. HAUSSMANN, *Theory of Quasigroups* (*American Journ. of Mathem.*, t. 49, 1937, p. 983)]. Mais il a aussi été utilisé antérieurement, dans un autre sens, par H. Brandt [*Verallgemeinerung des Gruppenbegriffs* (*Math. Ann.*, t. 96, 1926, p. 360)]. Il semble que, dans chacun des deux sens, le mot *groupoïde* convienne parfaitement : pour parer aux risques de confusion, à vrai dire minimes, nous utiliserons le terme de *groupoïde de Brandt* pour la seconde notion qui n'a pas, à beaucoup près, le caractère immédiat de la première et qui joue un rôle important dans plusieurs théories, notamment dans la composition des formes quadratiques (voir la définition p. 70).

- $\times, .$ ou absence de signe, pour $\left\{ \begin{array}{l} \text{la multiplication (des nombres, po-} \\ \text{lynomes, etc.)}; \\ \text{la composition des transforma-} \\ \text{tions}; \\ \text{le produit des équivalences}; \end{array} \right.$
 $:$ pour la division (pour laquelle on a également la notation fraction-
 naire);
 $\wedge$ pour la multiplication vectorielle;
 $\cap$ pour l'intersection (des ensembles, des équivalences, des éléments
 d'un treillis);
 $\cup$ pour la réunion des ensembles, l'union des éléments d'un treillis.

Très fréquemment, on utilise aussi l'un des signes précédents pour une opération abstraite, lorsque celle-ci a les mêmes propriétés que l'opération concrète à laquelle ce signe est ordinairement affecté. L'opération abstraite prend alors le nom d'addition, de multiplication, etc., et le groupoïde considéré est appelé groupoïde (ou système) additif, multiplicatif. Nous préciserons ultérieurement les conditions d'utilisation des notations additive et multiplicative (*cf.* p. 81).

Soit $E = \{a_1, a_2, \dots, a_n\}$ un groupoïde *fini* et d'*ordre* n , c'est-à-dire possédant n éléments. L'opération O de E peut être définie ou représentée par une *table d'opération*, c'est-à-dire par un tableau carré de n éléments, dans lequel le résultat $a_i O a_j$ est inscrit à l'intersection de la $i^{\text{ème}}$ ligne et de la $j^{\text{ème}}$ colonne. Ainsi, la table suivante définit un groupoïde $E_3 = \{a, b, c\}$ de trois éléments.

	a	b	c
a	a	c	b
b	c	b	a
c	b	a	c

2. Remarques sur la notion d'opération. — Il est essentiel de remarquer que le sens, d'ailleurs assez vague, donné au mot *opération* dans le langage mathématique courant, est sensiblement plus étendu que le sens précis qui vient de lui être attribué. C'est ce que nous allons montrer par les exemples suivants, qui soulèvent d'ailleurs plusieurs questions intéressantes.

Désignons par $V_2, V_3, \dots, V_r, \dots$ les ensembles formés par tous les vecteurs libres du plan, de l'espace, $\dots$, de l'espace euclidien à r dimen-

sions.... Si l'*addition géométrique* ou composition des vecteurs est bien, dans l'un quelconque de ces ensembles, une opération, il n'en est pas de même pour la *multiplication scalaire ou intérieure*, car celle-ci associe à un couple de vecteurs un *nombre* : le produit scalaire est donc une application de V_r^2 dans l'ensemble $\mathbf{P}$ des nombres réels. De même, la multiplication des vecteurs de V_r par les nombres réels ne doit pas être regardée comme une opération : c'est une application du produit $\mathbf{P} \times V_r$ dans V_r : on dit que les nombres réels sont des *opérateurs* pour le domaine V_r . Enfin la *multiplication extérieure* des vecteurs ne doit pas non plus, *du moins pour r quelconque*, être considérée comme une véritable opération. A un couple de vecteurs du plan V_2 , elle fait correspondre un vecteur *perpendiculaire* à ce plan. Le produit extérieur de deux vecteurs de V_r est, d'une manière générale, un *bivecteur* qui admet $\frac{r(r-1)}{2}$ composantes ⁽¹⁾, et peut être assimilé à un vecteur de $V_{\frac{r(r-1)}{2}}$. C'est donc *seulement pour $r = 3$* , c'est-à-dire dans l'espace euclidien à trois dimensions, que la multiplication extérieure des vecteurs est une véritable opération, à laquelle on donne le nom de *multiplication vectorielle* (et cela suppose encore, à vrai dire, que l'on a fixé l'*orientation de l'espace* et choisi l'*unité de longueur* : dans plus d'un cas, il est préférable de ne pas regarder le produit vectoriel de deux éléments de V_3 comme un élément de V_3 ; on dira qu'un tel produit vectoriel est un *vecteur axial*).

La définition d'une opération abstraite implique, d'autre part, que cette opération est *toujours possible*, c'est-à-dire qu'à *chaque* couple sans exception d'éléments a, b de l'ensemble E correspond un résultat c : or il n'en est ainsi ni pour la soustraction, ni pour la division exacte, dans l'ensemble N des nombres naturels : la soustraction et la division exacte ne sont donc pas, dans N , des opérations à proprement parler. Il est vrai que des généralisations convenables permettent de faire disparaître les conditions de possibilité de la soustraction et de la division exacte : on construit, comme nous le verrons, de nouveaux ensembles, comprenant N comme partie, et dans lesquels la soustraction et la division sont de véritables opérations ; les éléments de ces ensembles sont les nombres relatifs et les nombres rationnels. Les *problèmes d'extension*, ainsi posés par une simple analyse de la notion d'opération, présentent une importance fondamentale.

(1) Voir, par exemple, É. CARTAN, *Leçons sur la Géométrie des Espaces de Riemann*, chap. I, p. 5-12, Paris, Gauthier-Villars, 1928.

Une opération, une loi de composition soumises à une restriction de possibilité sont dites *partielles*. Comme le remarque A. Speiser ⁽¹⁾, un exemple simple et intéressant est celui de la *composition des segments* : deux segments ne sont *composables* que si l'origine de l'un coïncide avec l'extrémité de l'autre, et l'on a alors

$$AB + BC = AC.$$

Le passage des segments aux vecteurs libres, consistant à faire abstraction de la position de l'origine pour tenir compte uniquement des composantes, fait disparaître cette restriction : ce résultat est atteint ici, non par une *extension* de l'ensemble considéré, mais au contraire par *contraction* de cet ensemble au moyen de l'équivalence $\mathcal{R}_2$, ou *équipollence*, que nous avons définie au chapitre I (§ 5, p. 20).

On peut précisément rattacher au problème de la composition des segments la notion de *groupeïde de Brandt*, signalée plus haut [§ 1, note ⁽¹⁾, p. 67].

Un groupeïde de Brandt est un ensemble non vide Γ dans lequel *certain*s éléments sont composables : lorsqu'il en est ainsi pour deux éléments α et β , on écrit $\alpha\beta = \gamma$. On suppose, de plus, que cette composition partielle des éléments vérifie les quatre axiomes suivants :

I. Quand $\alpha\beta = \gamma$, chacun des trois éléments α , β , γ est défini univoquement par les deux autres.

II. Si $\alpha\beta$ et $\beta\gamma$ existent, il en est de même de $(\alpha\beta)\gamma$ et de $\alpha(\beta\gamma)$; si $\alpha\beta$ et $(\alpha\beta)\gamma$ existent, il en est de même de $\beta\gamma$ et de $\alpha(\beta\gamma)$; si $\beta\gamma$ et $\alpha(\beta\gamma)$ existent, il en est de même de $\alpha\beta$ et $(\alpha\beta)\gamma$; et l'on a, dans chacun de ces trois cas

$$(\alpha\beta)\gamma = \alpha(\beta\gamma).$$

III. Pour chaque élément α de Γ , il existe toujours, et d'une manière unique, un élément ε appelé *unité à droite* de α , tel que $\alpha\varepsilon = \alpha$; une *unité à gauche* ε' , telle que $\varepsilon'\alpha = \alpha$, et un inverse $\bar{\alpha}$, c'est-à-dire un élément tel que $\bar{\alpha}\alpha = \varepsilon$ ⁽²⁾.

⁽¹⁾ A. SPEISER, *Gruppentheorie (Grundlehren der Math. Wiss., t. 5, Berlin, 1927, p. 5)*.

⁽²⁾ On en déduit, en tenant compte de II,

$$\alpha\bar{\alpha} = \varepsilon', \quad \varepsilon\bar{\alpha} = \bar{\alpha}, \quad \bar{\alpha}\varepsilon' = \bar{\alpha}, \quad \varepsilon\varepsilon = \varepsilon, \quad \varepsilon'\varepsilon' = \varepsilon'.$$

De plus, une condition nécessaire et suffisante pour que α et β soient composables (dans cet ordre), est que l'unité à droite de α coïncide avec l'unité à gauche de β . Dans le cas des segments, les unités sont les *points* regardés comme segments nuls. Pour plus de détails sur les groupeïdes de Brandt, voir le Mémoire déjà cité de cet auteur (*Math. Ann.*, t. 96, 1926, p. 360).

IV. Pour deux unités quelconques $\varepsilon_1, \varepsilon_2$, il y a toujours un élément λ de Γ ayant ε_1 pour unité à gauche et ε_2 pour unité à droite.

Considérons le produit $E \times E = \Gamma$ d'un ensemble $E = \{x, y, z, \dots\}$ par lui-même, avec la loi de composition partielle

$$(1) \quad (x, y)(y, z) = (x, z),$$

tandis que, pour $s \neq t$, le produit $(r, s)(t, u)$ n'existe pas. On vérifie immédiatement que Γ est un groupoïde de Brandt, dans lequel l'élément $\alpha = (x, y)$ admet comme unité à gauche $\varepsilon' = (x, x)$ et comme unité à droite $\varepsilon = (y, y)$.

Soient alors $\mathcal{R}$ une relation d'équivalence définie dans E et $S_{\mathcal{R}}$ son ensemble représentatif dans $E \times E$. D'après (1), le produit de deux éléments composables de $S_{\mathcal{R}}$ est un élément de $S_{\mathcal{R}}$, puisque $\mathcal{R}$ est *transitive*. De plus, cette multiplication partielle vérifie visiblement les axiomes I, II, III : les unités, éléments de la forme $(x, x) = \varepsilon$, appartiennent toutes à $S_{\mathcal{R}}$, puisque $\mathcal{R}$ est *réflexive*; l'existence, dans $S_{\mathcal{R}}$, de l'inverse $\bar{\alpha}$ de $\alpha = (x, y) \in S_{\mathcal{R}}$ résulte de la *symétrie* de $\mathcal{R}$. Quant à l'axiome IV, il est vérifié si $\mathcal{R}$ est l'équivalence universelle (ou absolue), et seulement dans ce cas.

Appelons *groupe partiel* ⁽¹⁾ tout ensemble (non vide) où l'on a une multiplication partielle vérifiant les axiomes I, II, III : nous voyons que *l'ensemble représentatif d'une relation d'équivalence $\mathcal{R}$, définie dans E , est un groupe partiel $S_{\mathcal{R}}$ qui contient chaque unité (x, x) de Γ* . Nous allons établir la réciproque.

Soit Γ' un sous-ensemble non vide de Γ . Définissons dans Γ' une opération partielle de la façon suivante : si $\alpha = (x, y)$ et $\beta = (y, z)$ appartiennent à Γ' , et si, en outre, $\gamma = (x, z)$ appartient à Γ' , le produit $\alpha\beta$ existe et est égal à γ . Supposons que Γ' vérifie, par rapport à l'opération partielle que nous venons d'y définir, les axiomes I, II, III, en d'autres termes que Γ' est un *groupe partiel* contenu dans Γ ; supposons, en outre, que Γ' *contienne chaque unité (x, x) de Γ* , et montrons que Γ' *est alors l'ensemble représentatif d'une relation d'équivalence définie dans E : il existe donc une correspondance*

(1) L'introduction de cette notion et son utilisation dans la représentation des relations d'équivalence sont dues, ainsi que diverses autres applications, à R. CROISOT, *Une interprétation des relations d'équivalence dans un ensemble* (C. R. Acad. Sc., t. 226, 1948, p. 616); *Condition suffisante pour l'égalité des longueurs de deux chaînes...* (*ibid.*, p. 767).

biunivoque entre les relations d'équivalence de E et les groupes partiels $\Gamma' (\subseteq \Gamma)$ comprenant toutes les unités.

Posons $x\mathcal{R}y$ si $(x, y) \in \Gamma'$, et seulement dans ce cas. Cette relation $\mathcal{R}$ est *réflexive* puisque $(x, x) \in \Gamma'$, pour tout $x \in E$. Soient

$$\alpha = (x, y) \in \Gamma' \quad \text{et} \quad \beta = (y, z) \in \Gamma';$$

comme $\varepsilon = (y, y) \in \Gamma'$, $\alpha\varepsilon = \alpha$ et $\varepsilon\beta = \beta$ existent dans Γ' : d'après l'axiome II, il en est de même de $(\alpha\varepsilon)\beta = \alpha\beta = (x, z)$: deux éléments (x, y) et (y, z) de Γ' sont donc *composables dans Γ'* , leur produit est (x, z) et $\mathcal{R}$ est *transitive*. Enfin, d'après III, (y, x) , seul inverse possible de (x, y) , appartient à Γ' en même temps que (x, y) : $\mathcal{R}$ est donc *symétrique*; cette relation $\mathcal{R}$ est bien une *équivalence dont Γ' est l'ensemble représentatif*.

Une autre généralisation intéressante consiste à considérer une *opération multiforme*, associant à chaque couple (x, y) d'éléments de E une partie $Z = xy$ de E (s'il peut arriver que cette partie soit vide, l'opération multiforme sera dite partielle). Nous en verrons un exemple important au chapitre IV (§ 6, p. 167, notion d'*hypergroupe*).

Après ces indications, revenons à l'étude des opérations proprement dites, et de leurs principales propriétés.

3. Complexes. — On donne le nom de *complexe* à tout sous-ensemble *non vide* d'un groupoïde E. Le calcul des parties s'applique, en particulier, aux complexes, avec cette réserve que l'intersection $A \cap B$ de deux complexes A, B n'est un complexe que si A et B ne sont pas disjoints. Le complexe formé par un seul élément a est désigné par $\{a\}$, ou, si aucune confusion n'est à craindre, par a .

Pour simplifier les notations, supposons que le groupoïde E soit multiplicatif. Le *produit* A. B ou AB de deux complexes A et B est, par définition, l'ensemble des produits ab , où $a \in A$ et $b \in B$. En particulier, le produit aH d'un élément a par un complexe H désigne l'ensemble des produits ah , où $h \in H$. On désigne ordinairement par H^2 le produit HH ⁽¹⁾.

Si A et B sont finis et ont m et n éléments, le complexe AB est fini et a au plus mn éléments distincts.

(1) On a donc la même notation abrégée H^2 pour désigner le *complexe-produit* HH et l'*ensemble-produit* $H \times H$ (voir chap. I). Pratiquement, en tenant compte de la nature de la question, aucun risque de confusion n'est à craindre; on peut d'ailleurs, au besoin, revenir aux notations développées.

Les relations $A_1 \subseteq A$, $B_1 \subseteq B$ entraînent $A_1 B_1 \subseteq AB$. D'autre part, on a, pour le produit d'un complexe A par une réunion, la formule (de distributivité)

$$A \left(\bigcup_{M \in \mathcal{F}} M \right) = \bigcup_{M \in \mathcal{F}} AM$$

Soit, en effet, $x \in A \left(\bigcup_{M \in \mathcal{F}} M \right)$. On a $x = ar$, où $a \in A$ et $r \in \bigcup_{M \in \mathcal{F}} M$, donc il existe au moins un complexe M de $\mathcal{F}$ tel que $r \in M$. Nous avons alors $x \in AM$ et, par suite, $x \in \bigcup_{M \in \mathcal{F}} AM$.

Inversement, soit $x \in \bigcup_{M \in \mathcal{F}} AM$, donc $x = am$, où $a \in A$ et où m appartient à un certain complexe $M \in \mathcal{F}$. On a

$$m \in \bigcup_{M \in \mathcal{F}} M$$

et, par conséquent,

$$x \in A \left(\bigcup_{M \in \mathcal{F}} M \right).$$

Pour le produit d'un complexe A par une *intersection*, on a seulement la formule

$$A \left(\bigcap_{M \in \mathcal{F}} M \right) \subseteq \bigcap_{M \in \mathcal{F}} AM,$$

dont la démonstration est immédiate.

Exercice. — On considère trois droites D, D', D'' *coplanaires* et non parallèles deux à deux. On désigne par Λ , Λ' , Λ'' les ensembles des translations parallèles respectivement à D, D', D''. Comparer les complexes $\Lambda (\Lambda' \cap \Lambda'')$ et $(\Lambda \Lambda') \cap (\Lambda \Lambda'')$, la multiplication étant la composition des translations.

B. — PROPRIÉTÉS REMARQUABLES.

4. Propriétés de fermeture. — Un complexe S d'un groupoïde (multiplicatif) E est dit *multiplicativement fermé* ⁽¹⁾, ou est appelé

(1) Si l'opération O de E est quelconque, on dira *fermé par rapport à O*.

sous-groupeïde ou *sous-système* de E , si l'on a

$$S^2 \subseteq S,$$

en d'autres termes, si les relations $x \in S$, $y \in S$ entraînent $xy \in S$.

Un élément a de E est *idempotent* si le complexe $\{a\}$ constitué par ce seul élément est multiplicativement fermé; il faut et il suffit pour cela que l'on ait

$$a^2 = a.$$

Si pour l'opération considérée, tout élément de E est idempotent, l'opération elle-même et le groupeïde E sont dits *idempotents*; dans un treillis, par exemple, l'intersection et l'union ont cette propriété; en particulier, l'intersection et l'union des parties d'un ensemble, la formation du p. g. c. d. et du p. p. c. m. des nombres naturels, sont des opérations idempotentes.

L'ensemble $\mathcal{S}$ formé par les sous-groupeïdes d'un groupeïde (multiplicatif) E et par la partie vide $\emptyset$ vérifie les *conditions de Moore* (chap. I, § 11, p. 52), puisque : *a.* $E \in \mathcal{S}$; *b.* Toute intersection de sous-groupeïdes est vide ou est un sous-groupeïde, donc toute intersection d'éléments de $\mathcal{S}$ est un élément de $\mathcal{S}$. Par conséquent, $\mathcal{S}$ est un *treillis complet*; l'union, dans $\mathcal{S}$, d'une famille $\mathcal{F}$ de sous-groupeïdes X , ... est, comme on l'a vu, l'intersection des sous-groupeïdes S contenant chaque X de $\mathcal{F}$.

A ce treillis complet $\mathcal{S}$ des sous-groupeïdes et de la partie vide de E correspond, dans $\mathcal{X}(E)$, une *fermeture* (au sens général du chapitre I, § 11)

$$A \rightarrow \bar{A}$$

associant à toute partie A le plus petit élément $\bar{A}$ de $\mathcal{S}$ contenant A :

$$\bar{A} = \bigcap_{A \subseteq S \in \mathcal{S}} S.$$

Si, en particulier, A est un *complexe* H ($H \neq \emptyset$), $\bar{H}$, non vide, est le *plus petit sous-groupeïde* contenant H . $\bar{H}$ contient évidemment l'ensemble H' des éléments de H et des produits d'un nombre fini quelconque d'éléments de H : $H' \subseteq \bar{H}$. Il faut remarquer que ces produits diffèrent, non seulement par le choix et l'ordre des facteurs, mais aussi, dans le cas le plus général, par la manière dont ces facteurs sont associés : ainsi $(x_1 x_2) x_3$ et $x_1 (x_2 x_3)$ peuvent être différents, de même $x_1 (x_2 (x_3 x_4))$ et $(x_1 x_2) (x_3 x_4)$.

Mais inversement, l'ensemble H' des éléments de H et des produits d'un nombre fini d'entre eux est, visiblement, un sous-groupeïde de E , contenant H , ce qui entraîne $\bar{H} \subseteq H'$, d'où l'égalité.

Par définition, $\bar{H} = H'$ est le sous-groupeïde engendré par le complexe H . On le désigne encore par (H) ou, si H est fini, $H = \{h_1, \dots, h_n\}$, par $(h_1, \dots, h_n)$.

Un sous-groupeïde (a) engendré par un seul élément est *cyclique*. Ses éléments sont les *puissances* de a .

Exemples. — 1. Dans l'ensemble N des nombres naturels, regardé comme un groupeïde additif, l'ensemble des nombres pairs est un sous-groupeïde; l'ensemble des nombres impairs n'en est pas un. Dans N considéré comme groupeïde multiplicatif, l'ensemble des nombres pairs et l'ensemble des nombres impairs sont tous les deux des sous-groupeïdes.

2. Le groupeïde multiplicatif N_0 des nombres naturels, zéro compris, admet deux éléments idempotents 0 et 1.

3. Dans le groupeïde défini par la table

	a	b
a	b	a
b	b	a

on a

$$(a \times a) \times a \neq a \times (a \times a).$$

Exercices. — 1. Pour qu'un élément a soit idempotent, il faut et il suffit que l'on ait

$$(a) = \{a\}.$$

2. Le groupeïde $E_3 = \{a, b, c\}$, défini plus haut (p. 68) par sa table de multiplication, a tous ses éléments idempotents. Montrer que E_3 n'a pas d'autres sous-groupeïdes véritables que les sous-groupeïdes cycliques (a) , (b) , (c) .

3. Dans le groupeïde multiplicatif des entiers naturels, on considère les complexes $A = \{2\}$ et $B = \{3\}$. Former le complexe AB et les sous-groupeïdes (AB) et $(A \cup B)$. Pour deux complexes A, B d'un groupeïde quelconque, on a

$$AB \subseteq (AB) \subseteq (A \cup B).$$

4. On suppose qu'il existe, dans un groupeïde multiplicatif E , un élément idempotent a : montrer que la famille $\mathcal{A}$ des sous-groupeïdes de E qui contiennent a est un treillis complet. Quel est l'élément minimum de $\mathcal{A}$?

Un complexe C d'un groupeïde multiplicatif E est *permis à droite* dans E si

$$a \in C \quad \text{entraîne} \quad ax \in C \quad \text{pour tout } x \in E.$$

On définit de même un complexe *permis à gauche* (en remplaçant ax par xa). Un complexe est *permis* s'il est permis à droite et permis à gauche. *Tout complexe permis à droite (par exemple) est un sous-groupeïde*. Un élément a est *permis à droite*, par exemple, si l'on a $ax = a$ pour tout $x \in E$. S'il existe à la fois, dans E , un élément permis à droite a et un élément permis à gauche a' , ces deux éléments sont égaux et constituent l'*unique* élément permis de E . On a, en effet,

$$aa' = a = a'.$$

Un complexe I , multiplicativement permis dans E , est encore appelé *idéal du groupeïde E* (*idéal à droite* si I est seulement permis à droite, *idéal* ou *idéal bilatère* si I est permis des deux côtés). Il faut noter, cependant, que, s'il existe dans E une autre opération que la multiplication, on associera généralement au terme d'idéal une condition supplémentaire concernant cette opération (il en sera ainsi, comme nous le verrons, dans le cas où E est un anneau). L'ensemble $\mathcal{I}$ formé des idéaux, bilatères par exemple, et de la partie vide de E vérifie les conditions de Moore : c'est donc un *treillis complet*. Tout idéal étant un sous-groupeïde, $\mathcal{I}$ est une partie de $\mathcal{S}$; l'intersection, dans $\mathcal{I}$ comme dans $\mathcal{S}$, est l'intersection au sens de la Théorie des Ensembles; mais, en général, l'union dans $\mathcal{I}$ et l'union dans $\mathcal{S}$ sont différentes ⁽¹⁾.

Dans un groupeïde E , dont nous désignons l'opération par O , le complexe EOE , ensemble des éléments de la forme xOy (dans la notation multiplicative, l'ensemble E^2 des produits xy) est un *idéal bilatère*, donc un sous-groupeïde.

Si l'on a $EOE = E$, le groupeïde E est dit *globalement idempotent*. Tout groupeïde idempotent (c'est-à-dire dans lequel *chaque* élément x est idempotent : $xOx = x$), l'est globalement. Tel est le cas, notamment, pour un $\cup$ -demi-treillis ou un $\cap$ -demi-treillis.

L'ensemble des nombres naturels, $N = \{1, 2, \dots, n, \dots\}$, est globalement idempotent si on le considère comme groupeïde multiplicatif; il ne l'est pas si on le considère comme groupeïde additif ($1 \notin N + N$).

Exemples. — 1. Dans le groupeïde additif, N , des nombres naturels, l'ensemble S_n des entiers supérieurs à n est permis.

2. Dans le groupeïde multiplicatif N_0 des nombres naturels, zéro compris, le complexe des nombres pairs est permis. Le complexe des nombres impairs, qui est un sous-groupeïde, n'est pas permis. Zéro est élément permis.

⁽¹⁾ Pour une étude plus complète des idéaux d'un groupeïde ou d'une algèbre, nous renverrons aux *Leçons sur la Théorie des Treillis...*, de M. L. DUBREIL-JACOTIN, L. LESIEUR et R. CROISOT, 2^e partie, chap. IV, §§ 9 et 10.

5. **Règles de calcul.** — Dans un groupoïde E , un élément e est dit *neutre à droite* pour l'opération O si l'on a

$$x O e = x \quad \text{pour tout } x \in E.$$

On définit de même un élément *neutre à gauche* ($e O x = x$). Un élément neutre à droite et à gauche est dit *neutre*.

Un groupoïde possédant un élément neutre, bilatère ou seulement d'un côté, est globalement idempotent.

Si E est écrit sous forme multiplicative, un élément neutre (à droite) est ordinairement désigné sous le nons d'*élément-unité* (à droite). Un élément-unité à droite et à gauche est appelé *élément-unité bilatère*. Tout élément-unité à droite (par exemple) est idempotent. Si E est écrit sous forme additive, un élément neutre est appelé *élément-zéro*.

Si l'on a à la fois, dans E , un élément neutre à droite e , et un élément neutre à gauche e' , ces deux éléments sont égaux et constituent l'*unique* élément neutre de E . On a, en effet,

$$e' O e = e' = e.$$

Exemples. — 1. Le groupoïde multiplicatif des nombres naturels admet l'élément unité 1. Le groupoïde additif des nombres naturels, zéro compris, admet l'élément neutre 0.

2. Dans l'ensemble des parties d'un ensemble E , l'ensemble vide $\emptyset$ est neutre pour la réunion, E lui-même est neutre pour l'intersection. D'une façon plus générale, l'élément minimum (ou nul) d'un treillis, s'il existe, est neutre pour l'union, l'élément maximum (ou universel), s'il existe, est neutre pour l'intersection.

3. Considérons le groupoïde des transformations d'un ensemble S , l'opération étant la composition des transformations. La *transformation identique*, c'est-à-dire celle qui applique chaque élément sur lui-même, est un élément-unité bilatère.

4. Si un groupoïde n'a pas d'élément neutre à gauche, il peut avoir plusieurs éléments neutres à droite. C'est ce qui a lieu pour le groupoïde E_2 défini par la table

(E_2)		a	b
	a	a	a
	b	b	b

Exercices. — 1. L'ensemble des parties $\mathcal{P}(E)$ d'un ensemble E admet-il un élément neutre pour la différence symétrique ?

2. Dans l'ensemble des nombres naturels, la formation du p. g. c. d. et celle du p. p. c. m. sont deux opérations : existe-t-il des éléments neutres ?

Un groupoïde E , que nous écrirons sous forme multiplicative, est appelé *demi-groupe* et son opération est dite *associative* ⁽¹⁾ si l'on a

$$(1) \quad a(bc) = (ab)c,$$

quels que soient $a, b, c \in E$. Les deux membres de la relation (1) sont désignés par le symbole unique abc , qui est le *produit* des trois éléments a, b, c , pris dans cet ordre.

Considérons plus généralement n éléments $a_1, a_2, \dots, a_n$, non nécessairement distincts, et posons

$$\{[(a_1 a_2) a_3) \dots] a_{n-1}\} a_n = a_1 a_2 \dots a_n = P.$$

Tout autre produit P' formé au moyen des facteurs $a_1, a_2, \dots, a_n$ pris dans cet ordre, et avec des parenthèses disposées d'une manière quelconque, est égal à P . Par exemple

$$(a(bc))(de) = abcde.$$

Cette proposition, d'après (1), est vraie pour $n = 3$. Supposons-la établie pour m facteurs, $m < n$. Nous pouvons alors supprimer dans P' tous les couples de parenthèses sauf deux au plus, ce qui nous donne

$$P' = P'_1 P'_2,$$

avec

$$P'_1 = a_1 \dots a_h, \quad P'_2 = a_{h+1} \dots a_n.$$

Si $h = n - 1$, le théorème est démontré. Sinon, on a, d'après (1),

$$\begin{aligned} P' &= (a_1 \dots a_h) [(a_{h+1} \dots a_{n-1}) a_n] \\ &= [(a_1 \dots a_h) (a_{h+1} \dots a_{n-1})] a_n = (a_1 \dots a_{n-1}) a_n = P. \end{aligned}$$

Dans un demi-groupe, les *puissances* d'un élément a ne dépendent que du nombre m des facteurs : on les représente par la notation a^m ($a^1 = a$). De plus, on a les deux règles de calcul fondamentales

$$a^m a^n = a^{m+n}, \quad (a^m)^p = a^{mp}.$$

La première résulte de la proposition précédente; la seconde s'établit immédiatement par récurrence sur p .

Si le demi-groupe considéré est *additif*, on représente les multiples $a + a + \dots + a$ de l'élément a , qui ne dépendent que du nombre m

(1) On dit aussi que E est un *associatif* [cf. F. KLEIN-BARMEN, *Ueber Verbände mit einer weiteren assoziativen und kommutativen Elementverknüpfung* (*Math. Zeitschr.*, t. 47, 1940, p. 85, en particulier p. 82), et *Halbverbände und kommutative Semigruppen* (*Math. Zeitschr.*, t. 48, 1942, p. 27)]. N. BOURBAKI emploie le terme *monoïde*.

des termes, par la notation $m.a$, ($1.a = a$); on a les règles de calcul

$$ma + na = (m + n)a \\ m(na) = mna.$$

D'autre part, les éléments-unités à droite, $e, e', \dots$ d'un demi-groupe D , s'il en existe, forment un sous-demi-groupe.

On a, en effet, pour tout $x \in D$,

$$x.ee' = xe.e' = xe' = x$$

(même propriété pour les éléments-unités à gauche éventuels).

Exemples. — 1. L'addition et la multiplication des nombres naturels sont associatives.

2. L'intersection et la réunion des parties d'un ensemble sont associatives, et il en est de même, plus généralement, pour l'intersection et l'union d'un treillis : par exemple, $a \cup (b \cap c)$ et $(a \cup b) \cap c$ sont égaux, l'un et l'autre, au plus petit majorant de l'ensemble $\{a, b, c\}$ (voir chap. I, § 41, lemme, p. 49).

3. La composition des transformations d'un ensemble E est associative; soient, en effet, $\sigma_1, \sigma_2, \sigma_3$ trois transformations et x un élément quelconque de E . Posons

$$\sigma_1 x = x_1, \quad \sigma_2 x_1 = x_2, \quad \sigma_3 x_2 = x_3,$$

on a

$$(\sigma_2 \sigma_1)x = x_2, \quad (\sigma_3 \sigma_2)x_1 = x_3,$$

d'où

$$\sigma_3(\sigma_2 \sigma_1)x = x_3, \quad (\sigma_3 \sigma_2)\sigma_1 x = x_3,$$

et, par conséquent,

$$\sigma_3(\sigma_2 \sigma_1) = (\sigma_3 \sigma_2)\sigma_1.$$

Les transformations d'un ensemble E forment donc un demi-groupe : nous verrons au Chapitre III l'importance de cette propriété.

4. Le produit transitif des relations binaires définies dans un ensemble E est une opération associative : cette propriété résulte immédiatement de l'exercice 2 du paragraphe 12 (chap. I, p. 60).

5. La multiplication vectorielle, dans l'espace euclidien à trois dimensions, n'est pas associative, car, de la formule de Gibbs ⁽¹⁾

$$\vec{a} \wedge (\vec{b} \wedge \vec{c}) = \vec{b}(\vec{a} \cdot \vec{c}) - \vec{c}(\vec{a} \cdot \vec{b}),$$

résulte, en permutant circulairement les trois vecteurs, et en ajoutant membre à membre, l'identité de Jacobi

$$\vec{a} \wedge (\vec{b} \wedge \vec{c}) + \vec{b} \wedge (\vec{c} \wedge \vec{a}) + \vec{c} \wedge (\vec{a} \wedge \vec{b}) = 0.$$

⁽¹⁾ Voir, par exemple, A. CHATELET et J. KAMPÉ DE FÉRIET, *Calcul vectoriel*, chap. I, p. 49, G. JULIA, *Cours de Géométrie à l'École Polytechnique*, chap. I, n° 9.

d'après laquelle la différence $\vec{a} \wedge (\vec{b} \wedge \vec{c}) - (\vec{a} \wedge \vec{b}) \wedge \vec{c}$ est en général différente de zéro.

Exercices. — 3. Le groupoïde E_2 défini page 77 est-il un demi-groupe ? Même question pour le groupoïde E_3 , défini page 68.

4. Dans l'ensemble des parties d'un ensemble E , la différence symétrique (chap. I, § 2, ex. 4, p. 9) est une opération associative. On pourra d'abord montrer que $(A \circ B) \circ C$ est l'ensemble des éléments de E qui appartiennent soit aux trois ensembles A, B, C , soit à un seul d'entre eux; l'associativité en résulte. Plus généralement, $A_1 \circ A_2 \circ \dots \circ A_n$ est l'ensemble des éléments de E qui appartiennent à un nombre impair d'ensembles A_i .

Si E est un demi-groupe, la multiplication des complexes de E est associative.

B. A. Hausmann et O. Ore ont énoncé ⁽¹⁾ un certain nombre de lois plus générales que l'associativité, dites *lois d'associativité faibles*, moyennant lesquelles certaines conséquences de l'associativité restent valables. Parmi ces lois, dont certaines avaient déjà été indiquées par d'autres auteurs ⁽²⁾, citons les suivantes, où $\bar{x}$ désigne une puissance quelconque de x

$$\text{LOI } A_3 \dots \dots \dots a(bc) = (ab)c,$$

$$\text{LOI } A_5 \dots \dots \dots (ab)c = a(\bar{b}\bar{c}),$$

$$\text{LOI } A_6 \dots \dots \dots (ab)c = \bar{a}(\bar{b}\bar{c}).$$

Une opération O dans un groupoïde E est *commutative* et E est dit *abélien* si l'on a

$$aOb = bOa,$$

quels que soient $a, b \in E$.

Soit, dans un *demi-groupe abélien* (multiplicatif), $P = a_1 a_2 \dots a_n$ un produit de n facteurs : on peut y *permuter les facteurs d'une manière quelconque sans changer le produit*.

On peut passer, en effet, d'une permutation des facteurs à une autre par une suite d'échanges d'éléments consécutifs ⁽³⁾. Il suffit donc de

⁽¹⁾ *Theory of Quasi-groups* (Amer. J. of Math., t. 59, 1937, p. 983).

⁽²⁾ SUSCHKEWITSCH, *On a generalisation of the associative law* (Trans. Amer. Math. Soc., t. 31, 1929, p. 204); R. MUFANG, *Struktur von Alternativkörpern* (Math. Ann., t. 110, 1935, p. 415).

⁽³⁾ On le voit facilement par récurrence sur n . La proposition est évidente pour $n = 2$. Cela étant, nous pouvons amener à la première place, par des échanges d'éléments consécutifs, le facteur a_1 qui doit s'y trouver. Et pour le produit des $n-1$ autres facteurs, la proposition est vraie par hypothèse.

Cette propriété résulte aussi de la décomposition d'une substitution en produit de transpositions, qui sera vue plus loin comme conséquence de théorèmes plus généraux (p. 163).

montrer qu'un produit ne change pas quand on échange deux facteurs consécutifs

$$a_1 a_2 \dots a_i a_{i+1} \dots a_n = a_1 a_2 \dots a_{i+1} a_i \dots a_n.$$

Or, si nous posons

$$a_1 a_2 \dots a_{i-1} = \alpha, \quad a_i a_{i+1} = \beta = a_{i+1} a_i, \quad a_{i+2} \dots a_n = \gamma \quad (i \neq 1, n-1),$$

les deux membres de l'égalité à démontrer ne sont autres que $\alpha\beta\gamma$. Raisonnement analogue dans le cas $i = 1$ ou $n-1$.

Cette proposition entraîne pour les puissances la règle de calcul

$$(ab)^m = a^m b^m$$

(dont la vérification directe, par récurrence, est immédiate). Avec la notation additive, on a, pour les multiples, la relation

$$m(a+b) = ma + mb.$$

Il est commode de n'employer la notation multiplicative que pour les demi-groupes, la notation additive que pour les demi-groupes abéliens.

Exemples. — 1. L'intersection et la réunion des parties d'un ensemble sont des opérations commutatives.

2. Le demi-groupe additif ou multiplicatif des nombres naturels est abélien.

3. La multiplication vectorielle n'est pas commutative, mais *antisymétrique*, c'est-à-dire

$$\vec{a} \wedge \vec{b} = -\vec{b} \wedge \vec{a}.$$

4. D'un exercice vu plus haut (chap. I, § 7, ex. p. 29) résulte que le produit de deux substitutions n'est pas commutatif.

Exercice 5. — On désigne par $\mathcal{S}$ et $\mathcal{S}'$ les symétries, dans un plan, par rapport à deux points distincts O et O' . Montrer que les produits $\mathcal{S}'\mathcal{S}$ et $\mathcal{S}\mathcal{S}'$ sont deux transformations différentes. Même question pour deux symétries, dans le plan, par rapport à deux droites concourantes.

Un demi-groupe abélien H est appelé *holoïde* ⁽¹⁾ s'il possède les deux propriétés suivantes :

1° Il existe dans H un élément-unité;

2° Les relations $a = bx$ et $b = ay$ entraînent $a = b$.

(1) Cf. F. KLEIN-BARMEN, *Halbverbände und kommutative Semigruppen* (*Math. Zeitschr.*, t. 48, 1942, p. 275; *ibid.*, 1943, p. 715); *Ein Beitrag zur Theorie der linearen Holoïde* (*Math. Zeitschr.*, t. 51, 1948, p. 355).

Exemple. — L'ensemble des nombres naturels est un holoïde par rapport à la formation du p. p. c. m. et par rapport à la multiplication ordinaire.

Exercice 6. — Un holoïde fini possède un élément permis et un seul (Voir note ⁽¹⁾, p. 81.

Si E est un *groupeïde abélien*, la multiplication des complexes de E est une opération commutative : $AB = BA$.

Si E est un *demi-groupe abélien* et si A et B sont deux sous-groupeïdes ou *sous-demi-groupes*, on a l'égalité

$$(2) \quad AB = (AB),$$

qui entraîne la proposition suivante : *dans un demi-groupe abélien, le complexe-produit de deux sous-groupeïdes est un sous-groupeïde.*

Pour établir l'égalité (2), il suffit, puisque le premier membre est contenu dans le second, de remarquer qu'un élément $x \in (AB)$ est de la forme

$$x = a_1 b_1 a_2 b_2 \dots a_n b_n, \quad \text{avec } a_i \in A, \quad b_i \in B;$$

d'où

$$x = a_1 a_2 \dots a_n b_1 b_2 \dots b_n = ab, \quad \text{avec } a = \prod a_i \in A, \quad b = \prod b_i \in B.$$

Dans un *demi-groupe E non abélien*, on peut obtenir, de la manière suivante, une condition suffisante pour que la relation (2) soit valable et que le complexe-produit de deux sous-demi-groupes soit un sous-demi-groupe.

Soient A et B deux complexes. Si

$$BA \subseteq AB,$$

on dit que B est *permutable à gauche* avec A, et A *permutable à droite* avec B. Si B est permutable à gauche et à droite avec A, donc si $AB = BA$, A et B sont dits *permutables*.

Cela étant, si un sous-demi-groupe A est permutable à droite avec un sous-demi-groupe B, $BA \subseteq AB$, on a

$$(2) \quad AB = (AB),$$

et le complexe AB est, par suite, un *sous-demi-groupe*.

Soit $x \in (AB)$, donc $x = a_1 b_1 a_2 b_2 \dots a_n b_n$. On a, en tenant compte de l'hypothèse,

$$b_1 a_2 = a'_1 b'_2,$$

d'où

$$x = a''_1 b''_1 a_3 b_3 \dots a_n b_n, \quad \text{avec } a''_1 = a_1 a'_1 \in A, \quad b''_1 = b'_1 b_2 \in B,$$

et il suffit de répéter le raisonnement pour obtenir

$$x = ab, \quad \text{où } a \in A \text{ et } b \in B.$$

Exercice 7. — Dans un demi-groupe multiplicatif E possédant un élément-unité e , on considère deux complexes A, B contenant e .

1° Établir les égalités

$$(A \cup B) = (AB) = (BA).$$

2° Si A et B sont des sous-demi-groupes et si A est permutable à droite avec B , AB est le plus petit sous-demi-groupe contenant A, B et BA .

L'ensemble Z des éléments z d'un groupoïde multiplicatif E qui sont permutables avec tout élément de E ,

$$az = za \quad \text{pour tout } a \in E,$$

est appelé le *centre* de E . Un élément-unité, un élément permis appartiennent au centre. Le centre Z d'un demi-groupe, s'il n'est pas vide, est un *sous-groupoïde*, car les relations $z \in Z, z' \in Z$ entraînent

$$a.zz' = az.z' = za.z' = z.az' = z.z'a = zz'.a,$$

d'où

$$zz' \in Z.$$

On voit en passant que l'ensemble des éléments d'un demi-groupe permutables avec un élément donné a est un sous-groupoïde; cet ensemble n'est pas vide puisqu'il contient a et ses puissances.

Soit $E = \{a_1, a_2, \dots, a_n\}$ un groupoïde multiplicatif *fini*. Posons

$$a_i a_j = a_{ij},$$

et supposons écrite la table de multiplication de E .

Si E est *abélien*, sa table de multiplication est *symétrique* par rapport à la diagonale principale

$$a_{ij} = a_{ji},$$

et inversement.

D'autre part, la condition nécessaire et suffisante pour que E soit un *demi-groupe* est que l'on ait

$$(3) \quad a_{ij} a_k = a_i a_{jk},$$

quels que soient les indices i, j, k .

Si E est un *demi-groupe abélien*, nous avons

$$a_{ij} a_{pq} = a_i a_j a_p a_q = a_p a_j a_i a_q = a_{pj} a_{iq},$$

donc, si quatre éléments se trouvent, dans la table, placés aux sommets d'un rectangle, le produit de deux éléments situés en des sommets opposés est égal au produit des deux autres, c'est ce qu'on appelle la *propriété du rectangle*.

Pour un groupoïde admettant un élément-unité à droite, e , la propriété du rectangle

$$(4) \quad a_{ij} a_{pq} = a_{pj} a_{iq}$$

entraîne, réciproquement, la commutativité et l'associativité. Prenons, en effet, dans la construction de la table $a_i = e$, ce qui donne

$$a_{i1} = a_i \quad (i = 1, 2, \dots, n).$$

Remplaçons dans (4) j et q par 1; nous obtenons

$$a_i a_p = a_p a_i,$$

c'est-à-dire la *commutativité*. D'autre part, en prenant dans (4) $j = 1$, nous avons

$$a_i a_{pq} = a_p a_{iq},$$

et, en tenant compte de la commutativité,

$$a_{pq} a_i = a_p a_{qi},$$

c'est-à-dire l'associativité.

Exemple. — Les groupoïdes

$$(E_2) \quad \begin{array}{c|cc} & e & a \\ \hline e & e & a \\ a & a & a \end{array}$$

$$(E'_3) \quad \begin{array}{c|ccc} & e & a & b \\ \hline e & e & a & b \\ a & a & a & b \\ b & b & b & b \end{array}$$

sont des demi-groupes abéliens.

Une propriété plus faible que la commutativité et qui en constitue une généralisation souvent commode, est la suivante. Un complexe S d'un groupoïde E est *réversible à droite* ⁽¹⁾ si, pour chaque couple s_1, s_2

⁽¹⁾ Cf. P. DUBREIL, *Contribution à la Théorie des demi-groupes* (Mémoires de l'Académie des Sciences de l'Institut de France, t. 63, 1941, p. 1). On trouvera au théorème 30 de ce Mémoire (p. 34) une condition suffisante pour que le produit de deux sous-groupoïdes réversibles à droite dans un demi-groupe soit un sous-groupoïde réversible à droite. Pour l'exercice 8, on pourra se reporter au théorème 31 du même travail (p. 35) ainsi qu'au chapitre II d'un Mémoire portant le même titre, *Rendiconti di Matematica e delle sue applicazioni*, s. V, t. X, 1951, p. 183-200.

d'éléments de S , il existe au moins un couple s'_1, s'_2 d'éléments de S vérifiant l'égalité

$$s'_1 s_1 = s'_2 s_2.$$

Cette définition peut s'appliquer en particulier à un sous-groupeïde, ou éventuellement au groupeïde E lui-même : dans ce dernier cas, elle exprime que deux éléments quelconques de E ont au moins un multiple commun à gauche.

On définit de même un complexe, ou un groupeïde, *réversible à gauche*. Un complexe, ou un groupeïde, réversible à droite et à gauche, est dit *réversible*.

Tout complexe S d'un groupeïde *abélien* est évidemment réversible ($s'_1 = s_2, s'_2 = s_1$). Dans tout demi-groupe réversible à droite, n éléments $s_1, s_2, \dots, s_n$ admettent un multiple commun à gauche

$$s'_1 s_1 = \dots = s'_n s_n = m \in S$$

(démonstration immédiate par récurrence sur n).

Exercice 8. — A partir d'un complexe H d'un groupeïde E , on définit dans E une relation P_H en posant

$$a P_H a' \quad \text{si} \quad ha = h' a', \quad \text{où} \quad h \text{ et } h' \in H.$$

1° P_H est réflexive et symétrique.

2° Si E est un *demi-groupe*, P_H est régulière à droite, c'est-à-dire

$$a P_H a' \quad \text{entraîne} \quad (ax) P_H (a'x) \quad \text{pour tout } x \in E.$$

3° Si H est un sous-groupeïde réversible à droite dans le demi-groupe E , la relation P_H est transitive : c'est, par conséquent, une équivalence.

Un élément a d'un groupeïde E est dit *simplifiable* (ou *cancellable*) *à droite* si l'égalité

$$x O a = y O a \quad \text{entraîne} \quad x = y,$$

simplifiable (ou *cancellable*) *à gauche* si l'égalité

$$a O x = a O y \quad \text{entraîne} \quad x = y,$$

simplifiable (ou *cancellable*) s'il possède à la fois les deux propriétés précédentes (qui coïncident si E est abélien).

Un groupeïde E , ou son opération O , vérifient la *règle de simplification* (ou la *loi de cancellation*), *à droite* par exemple, si tout élément de E est simplifiable à droite.

Un *demi-groupe* S vérifiant la *règle de simplification* (à droite et à gauche) est appelé *semi-groupe* ⁽¹⁾.

Un semi-groupe S réversible à droite, c'est-à-dire dans lequel deux éléments quelconques a, a' ont toujours un multiple commun à gauche

$$ma = m'a',$$

est dit *régulier à gauche* ⁽²⁾, ou appelé *demi-groupe régulier à gauche* ⁽³⁾.

Pour un groupoïde fini E , la règle de simplification à droite équivaut à la condition suivante : chaque élément de E figure une fois et une seule dans chaque *colonne* de la table de multiplication. La règle de simplification à gauche équivaut à la propriété analogue pour les *lignes*.

THÉORÈME. — Soit, dans un demi-groupe D , s un élément simplifiable à droite. S'il existe un élément e tel que

$$es = s,$$

e est élément-unité à droite ⁽⁴⁾.

On a, en effet, pour tout élément x de D , $x.es = xs$ ou $xe.s = xs$, ce qui entraîne $xe = x$ (en particulier, $se = s$).

COROLLAIRES. — 1. Si s est simplifiable (des deux côtés), un élément e vérifiant $es = s = se$ est élément-unité bilatère. En particulier, si l'on a, dans un semi-groupe S , une égalité de la forme $es = s = se$, où s est un élément particulier, e est élément-unité bilatère.

2. Dans un demi-groupe D vérifiant la règle de simplification à droite, tout élément idempotent est élément-unité à droite ⁽¹⁾.

(1) Le terme anglais *Semigroup* doit être traduit par *demi-groupe*; le mot de semi-groupe, dans le sens où nous l'employons, n'a pas d'équivalent : on énonce explicitement l'hypothèse de la règle de simplification.

(2) Cf. O. ORE, *Linear Equations in non commutative Fields* (*Annals of Math.*, t. 32, 1931, p. 463), où sont définis, d'une façon un peu moins générale, les *anneaux réguliers*. Pour exprimer la propriété dissymétrique dont il s'agit, l'emploi du terme régulier à gauche est préférable pour la *théorie de l'immersion*, dont nous nous occuperons plus loin (chap. V, § 6, p. 266) et pour celle des *Modules* (vol. II), tandis que l'expression réversible à droite semble s'imposer dans la Théorie des équivalences dans un demi-groupe (chap. V, § 4, p. 230).

(3) Dans cette deuxième expression, les mots « à gauche » concernent seulement l'existence d'un multiple commun; la règle de simplification est supposée valable des deux côtés, puisqu'il s'agit d'un semi-groupe.

(4) Nous nous dispensons d'énoncer la proposition symétrique.

Puisqu'un élément-unité à droite et un élément-unité à gauche sont nécessairement égaux (p. 77), un *semi-groupe* S ne peut pas contenir plus d'un élément idempotent.

On dit qu'un sous-demi-groupe S d'un demi-groupe D est un *semi-groupe dans* D , ou un *D-semi-groupe* si chaque élément s de S est *simplifiable dans* D à gauche et à droite, donc si (avec la notation multiplicative)

$$\begin{aligned} xs = ys \quad (x, y \in D, s \in S) & \quad \text{entraîne} \quad x = y, \\ sx' = sy' \quad (x', y' \in D, s \in S) & \quad \text{entraîne} \quad x' = y'. \end{aligned}$$

Un D-semi-groupe est, en particulier, un semi-groupe.

Exemples. — 1. Dans l'ensemble N des nombres naturels, *zéro exclu*, la règle de simplification est vérifiée par l'addition et la multiplication. Elle ne l'est pas par la formation du p. g. c. d. ou du p. p. c. m.

2. Dans l'ensemble N_0 des nombres naturels *et de zéro*, la règle de simplification est vérifiée par l'addition, mais non par la multiplication, puisqu'on a $0a = 0b$ avec $a \neq b$. Dans tout groupoïde contenant plus d'un élément, l'existence d'un élément permis à droite *exclut* la règle de simplification à gauche.

3. Dans N_0 considéré comme un demi-groupe multiplicatif D , l'ensemble N des entiers non nuls est un D-semi-groupe.

Exercices. — 9. Soit E un ensemble. Dans l'ensemble des parties $\mathcal{P}(E)$, l'intersection, la réunion, la différence symétrique vérifient-elles la règle de simplification?

10. Si la règle de simplification à gauche est valable dans un groupoïde E , il y a au plus un élément-neutre à droite.

11. Soit E un groupoïde vérifiant la règle de simplification à gauche. Si A est un sous-groupoïde permis à droite dans E , A a nécessairement même puissance que E ⁽¹⁾.

12. Dans un demi-groupe, les éléments cancellables à gauche (par exemple), s'il en existe, forment un sous-demi-groupe.

Soit E un *domaine* où sont définies deux opérations, par exemple une addition et une multiplication. Nous supposons *l'addition associative et commutative*, sans faire nécessairement les hypothèses analogues pour la multiplication.

(1) On rappelle la proposition suivante : Soient trois ensembles U, V, W ; si l'on a $U \subseteq V \subseteq W$ et si U et W ont même puissance, V et W ont aussi même puissance. C'est là une conséquence immédiate du théorème suivant de F. Bernstein. Si une partie E , de E a même puissance que E' et si une partie E'_1 de E' a même puissance que E , E et E' ont même puissance (cf. Note V, th. 8, p. 451).

La multiplication est dite :

Distributive à gauche par rapport à l'addition si l'on a

$$(5) \quad a(b + b') = ab + ab';$$

Distributive à droite si l'on a

$$(6) \quad (a + a')b = ab + a'b,$$

Enfin *distributive* si elle possède simultanément les deux propriétés précédentes. Quand la multiplication est commutative, les notions de distributivité à droite et de distributivité à gauche coïncident.

Les relations (5) et (6) entraînent immédiatement

$$\begin{aligned} a(b_1 + b_2 + \dots + b_n) &= ab_1 + ab_2 + \dots + ab_n, \\ (a_1 + a_2 + \dots + a_m)b &= a_1b + a_2b + \dots + a_mb \end{aligned}$$

qui, combinées, donnent la règle de calcul

$$\left(\sum_{i=1}^m a_i \right) \left(\sum_{j=1}^n b_j \right) = \sum_{i=1, j=1}^{mn} a_i b_j.$$

Exemples. — 1. La multiplication des nombres naturels est distributive par rapport à l'addition, par rapport à la formation du p. g. c. d. et à celle du p. p. c. m.

2. La multiplication vectorielle dans l'espace à trois dimensions est distributive par rapport à l'addition géométrique.

On appelle *treillis distributif* un treillis T dans lequel chacune des opérations *intersection*, *union* est distributive par rapport à l'autre :

$$x \cap (y \cup z) = (x \cap y) \cup (x \cap z), \quad x \cup (y \cap z) = (x \cup y) \cap (x \cup z)$$

quels que soient $x, y, z \in T$. Par exemple, le treillis des parties d'un ensemble E est distributif, puisque l'intersection et la réunion des parties sont distributives l'une par rapport à l'autre (chap. I, § 2, p. 6).

Exercices. — 13. Pour qu'un treillis T soit distributif, il suffit que l'intersection soit distributive par rapport à l'union (ou, d'une façon duale, que l'union soit distributive par rapport à l'intersection) ⁽¹⁾.

14. Soient a, b deux entiers naturels, $m = [a, b]$ leur p. p. c. m., $d = (a, b)$ leur p. g. c. d., x un entier quelconque. Établir la relation

$$\frac{(x, m)}{(x, a)} = \left(\frac{x}{(x, a)}, \frac{m}{a} \right).$$

⁽¹⁾ Voir G. BIRKHOFF, *Lattice Theory*, chap. IX, p. 133; M. L. DUBREIL-JACOTIN, L. LESIEUR, R. CROISOT, *Leçons sur la Théorie des Treillis*, ..., 1^{re} partie, chap. VI, p. 73. On trouvera dans ces deux Ouvrages une théorie détaillée des treillis distributifs.

En déduire que $\frac{(x, m)}{(x, a)}$ et $\frac{(x, m)}{(x, b)}$ sont premiers entre eux et établir la formule de distributivité du p. g. c. d. par rapport au p. p. c. m.

$$(x, [a, b]) = [(x, a), (x, b)].$$

En tenant compte de l'exercice 13, on déduit de ce qui précède que l'ensemble N des entiers naturels, ordonné par la relation $a \mid b$, est un treillis distributif.

Directement d'ailleurs, on peut, avec les mêmes notations, établir la relation

$$\frac{[x, a]}{[x, d]} = \frac{a}{a'd'},$$

où a' est entier, en déduire que $\frac{[x, a]}{[x, d]}$ et $\frac{[x, b]}{[x, d]}$ sont premiers entre eux et que le p. p. c. m. est distributif par rapport au p. g. c. d.

$$[x, (a, b)] = ([x, a], [x, b]).$$

13. Le produit (ordinaire) des relations binaires définies dans un ensemble E donné est distributif par rapport à l'union; l'est-il par rapport à l'intersection?

Étudier le cas particulier suivant. E est l'ensemble des points d'une droite, dont O désigne un point particulier. $\mathcal{R}$, $\mathcal{R}'$, $\mathcal{S}$ sont les relations définies par :

$x\mathcal{R}y$ si x et y ne sont pas de part et d'autre de O;

$x\mathcal{R}'y$ si x et y sont à la même distance de O;

$x\mathcal{S}y$ si la distance des points x, y est au moins égale à une longueur donnée a .

Comparer les relations

$$\mathcal{T} = (\mathcal{R} \cap \mathcal{R}')\mathcal{S} \quad \text{et} \quad \mathcal{T}_1 = (\mathcal{R}\mathcal{S}) \cap (\mathcal{R}'\mathcal{S}).$$

16. 1° Une chaîne est-elle un treillis distributif?

2° Les treillis représentés par les diagrammes

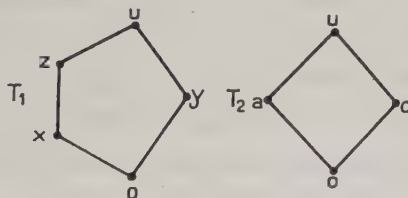


Fig. 6.

sont-ils distributifs (1)?

6. Propriétés d'inversion. — Considérons, dans un groupoïde E, deux éléments a et m . On appelle *complémentaire à droite de a par*

(1) Cf. *Leçons sur la Théorie des Treillis...*, chap. VI, § 1, p. 78. On remarquera qu'on a, dans tout treillis, les relations

$$x \cap (x \cup y) = x, \quad x \cup (x \cap y) = x$$

(voir le théorème 2 à la fin du paragraphe 6 de ce chapitre, p. 96).

rapport à m ou, si E est un groupoïde multiplicatif, *quotient à droite de m par a* , tout élément x vérifiant la relation

$$(7) \quad a \circ x = m;$$

complémentaire à gauche de a par rapport à m , ou *quotient à gauche de m par a* , tout élément y vérifiant la relation

$$(8) \quad y \circ a = m;$$

enfin *complémentaire de a par rapport à m* ou *quotient de m par a* à tout élément vérifiant à la fois les deux relations précédentes. Ces notions se confondent dans un groupoïde abélien.

Dans un groupoïde E quelconque, les complémentaires ou quotients n'existent pas nécessairement, et, s'il en existe pour un couple donné (m, a) , ils ne sont pas forcément uniques. Si E vérifie la règle de simplification à gauche, il y a *au plus* un complémentaire à droite de a par rapport à m .

Exemples. — 1. Dans le groupoïde *additif* des nombres naturels, zéro compris, a admet un complémentaire, unique, par rapport à m , si l'on a $a \leq m$ et seulement dans ce cas.

2. Dans le groupoïde *multiplicatif* des nombres naturels, zéro exclu, a admet un complémentaire, unique, par rapport à m , si a divise m , et seulement dans ce cas.

Exercices. — 1. A quelle condition une partie A d'un ensemble E admet-elle par rapport à une autre partie M un complémentaire vis-à-vis de la réunion? A et M vérifiant cette condition, quels sont tous les complémentaires possibles?

2. Dans l'ensemble des vecteurs libres de l'espace à trois dimensions, l'opération étant la multiplication vectorielle, à quelle condition un vecteur $\vec{a}$ admet-il un complémentaire à droite par rapport à un vecteur $\vec{m}$? Cette condition étant vérifiée, quels sont tous les complémentaires possibles?

Un groupoïde E vérifie *l'axiome des quotients à droite* si, pour chaque couple d'éléments (m, a) de E , il existe un complémentaire ou quotient à droite x et un seul

$$a \circ x = m.$$

De même, *l'axiome des quotients à gauche* exprime l'existence et l'unicité du complémentaire à gauche y

$$y \circ a = m.$$

Lorsque ces deux conditions sont satisfaites simultanément, on dit que E vérifie l'axiome des quotients ou qu'il est un *quasi-groupe*. Un quasi-groupe ayant un élément-unité bilatère prend le nom de *boucle* (en anglais *loop*) ⁽¹⁾.

L'axiome des quotients à droite entraîne la règle de simplification à gauche, car si l'on avait

$$ar = as, \quad \text{avec } r \neq s,$$

l'élément $m = ar = as$ aurait deux quotients à droite distincts par a . La règle de simplification est donc valable dans tout quasi-groupe.

Pour qu'un groupoïde fini vérifie l'axiome des quotients à droite, il faut et il suffit que chaque élément figure une fois et une seule dans chacune des lignes de la table définissant l'opération : il y a donc *équivalence, pour les groupoïdes finis, entre l'axiome des quotients à droite et la règle de simplification à gauche* et, par suite, entre l'axiome des quotients et la règle de simplification ⁽²⁾.

Dans un quasi-groupe, on appelle *opération inverse à droite* ou, s'il s'agit d'un quasi-groupe multiplicatif, *division à droite*, l'opération qui fait correspondre au couple (m, a) le complémentaire à droite x de a par rapport à m . On définit de même l'opération inverse à gauche, dont le résultat est y . Les deux opérations inverses coïncident si le quasi-groupe est abélien.

Exemple. — Par rapport à l'addition géométrique, l'ensemble des vecteurs libres est un quasi-groupe.

Quand les quotients n'existent pas nécessairement, on peut faire intervenir utilement les notions suivantes ⁽³⁾. Un complexe X d'un groupoïde G est dit *unitaire à droite dans G* si les relations

$$x \in X, \quad a \in G \quad \text{et} \quad ax = x' \in X$$

⁽¹⁾ Cf. B. A. HAUSSMANN et O. ORE, *Theory of quasi-groups* (Amer. J. Math., t. LIX, 1937, p. 986), ainsi que G. BIRKHOFF, *Lattice Theory*, p. 85, où l'on trouvera des indications bibliographiques concernant notamment les travaux de A. Suschkewitch et de A. A. Albert.

⁽²⁾ Pour les groupoïdes infinis, cette équivalence disparaît : le demi-groupe multiplicatif N des nombres naturels (zéro exclu) vérifie la règle de simplification sans être un quasi-groupe.

⁽³⁾ Voir, par exemple, chap. IV, § 6, th. III (p. 171); chap. V, § 1 et 4, ainsi que les Mémoires intitulés : *Contribution à la Théorie des demi-groupes*, I, *Mémoires de l'Académie des Sciences*, t. 63, 1941; II, *Rendiconti di Matem. e. d. s. applicazioni*, s. V, vol X, p. 183-200.

entraînent

$$a \in X.$$

On définit symétriquement un complexe unitaire à gauche; un complexe unitaire à droite et à gauche est dit unitaire.

Exemples. — 1. Le complexe $\{e\}$ formé par un élément-unité à droite e de G , est unitaire à droite.

2. Dans le demi-groupe multiplicatif N des entiers naturels, l'ensemble X_2 des carrés, l'ensemble X_n des puissances $n^{\text{ièmes}}$ sont des complexes, et même des sous-demi-groupes unitaires.

Dans un groupoïde G , on appelle *quotient à droite* d'un complexe H par un élément a l'ensemble des éléments x de G vérifiant la relation

$$ax \in H.$$

Ce quotient est désigné par $(H:a)_d$ ou, si le complexe H est donné une fois pour toutes, par Q_a . H est dit *net à droite* si l'on a $Q_a \neq \emptyset$ pour tout $a \in G$. On définit d'une façon symétrique le *quotient à gauche* $(H:a)_g$ ou ${}_aQ$ et les complexes *nets à gauche* ⁽¹⁾.

Le complexe H est *net* s'il est à la fois net à droite et net à gauche.

Si le complexe H n'est pas net à droite, il existe au moins un élément w de G pour lequel la relation $wx \in H$ n'a aucune solution x . L'ensemble W_H de ces éléments est appelé *résidu à droite* de H . Si G est un demi-groupe, le résidu à droite W_H est un ensemble permis à droite, car la relation

$$wr.x = w.r x \in H$$

n'a, également, aucune solution x et $wr \in W_H$. On définit symétriquement le *résidu à gauche* ${}_H W$.

Exemples. — Dans le demi-groupe multiplicatif des nombres naturels, l'ensemble H des carrés parfaits est net; l'ensemble $K(n)$ des nombres supérieurs à un nombre donné n l'est aussi; l'ensemble $L(n)$ des nombres inférieurs ou égaux à n ne l'est pas et a pour résidu $K(n)$ qui est bien un complexe permis.

Soit E un groupoïde admettant un élément-unité e (à droite, à gauche

(1) On emploie aussi les notations $H \cdot a$ pour le quotient à droite et $H \cdot a$ pour le quotient à gauche. Ces dernières notations, plus simples, sont celles du calcul des résiduels (cf. *Leçons sur la Théorie des Treillis...*, 2^e partie, chap. II, p. 152), et les quotients peuvent être regardés comme des résiduels particuliers dans l'ensemble des parties de G (voir P. DUBREIL, *Contribution à la Théorie des Demi-groupes* (III), Bull. Soc. Math. de France, t. 81, 1953, p. 289).

ou bilatère). On donne le nom d'*inverse à droite* d'un élément $a \in E$, par rapport à l'opération O et à l'élément-unité e , à tout complémentaire à droite a' de a par rapport à e ,

$$a O a' = e.$$

On dit aussi que a' *neutralise* a à droite, et l'on emploie alors la notation $a \nu (= a')$.

De même, on appelle *inverse à gauche* tout complémentaire à gauche a^* ou ν_a de a par rapport à e , et *inverse* un élément a^- , « a moins » ⁽¹⁾, qui est à la fois inverse à droite et inverse à gauche. Un élément a de E qui admet au moins un inverse à droite a' par rapport à l'élément-unité e considéré, est dit *inversible à droite* par rapport à e . La règle de simplification à gauche entraîne l'unicité de l'inverse à droite pour les éléments qui en possèdent un. Un élément a est *inversible* s'il possède au moins un inverse.

LEMME. — Dans un demi-groupe multiplicatif D possédant un élément-unité bilatère e , si un élément x a un inverse à droite x' et un inverse à gauche x^* , on a $x' = x^*$.

En effet les relations $xx' = e = x^*x$ entraînent

$$x^*xx' = x^*e = x^*$$

et

$$x^*xx' = ex' = x'.$$

De ce lemme résulte qu'un tel élément x a un seul inverse à droite; de plus, dans un demi-groupe D avec élément-unité, un élément a ne peut avoir qu'un inverse.

Un élément x est dit *involutif* s'il est à lui-même son inverse

$$x^2 = e.$$

Dans la notation additive, réservée généralement au cas commutatif, l'inverse d'un élément a est appelé *élément opposé* et désigné par $-a$.

Exemples. — 1. Dans le demi-groupe multiplicatif des nombres naturels, l'élément-unité, 1, est le seul élément admettant un inverse.

2. Soit σ une transformation d'un ensemble E . Posons

$$m' = \sigma(m).$$

L'application $m' \rightarrow m$ est encore une application de E sur lui-même, donc une transformation, évidemment inverse de σ .

(1) Voir plus loin (p. 138) la notation définitive, a^{-1} .

Si l'on a, par exemple,

$$E = \{1, 2, 3\} \quad \text{et} \quad \sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix},$$

on a

$$\sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}.$$

3. Les symétries (par rapport à un point, à une droite ou à un plan), les inversions, sont des transformations involutives.

Exercice. — 3. Considérons l'ensemble des parties $\mathcal{P}(E)$ d'un ensemble E comme un groupoïde par rapport à la différence symétrique.

1° Tout élément de $\mathcal{P}(E)$ est involutif.

2° $\mathcal{P}(E)$ est un quasi-groupe, l'opération inverse étant la différence symétrique elle-même.

Dans les *treillis*, en raison de l'existence de *deux opérations*, l'intersection $\cap$ et l'union $\cup$, les propriétés d'inversion se présentent d'une façon un peu différente.

Soit T un treillis possédant un élément minimum, ou nul, o , et un élément maximum, ou universel, u . On appelle *complément* d'un élément x de T un élément x' , *s'il existe*, tel que

$$x \cap x' = o \quad \text{et} \quad x \cup x' = u.$$

Un élément ayant au moins un complément est dit *complémenté*; s'il en est ainsi pour chaque élément x de T , T lui-même est dit *complémenté*.

Le complément de o est u , celui de u est o .

Exemples. — 4. Dans le treillis $\mathcal{P}(E)$ des parties d'un ensemble E , toute partie X admet un complément qui est précisément le complément au sens de la théorie des ensembles, $E - X$.

2. Le treillis représenté par le diagramme ci-dessous est complémenté; a_1 admet deux compléments, a'_1 , a'_2 , qui sont aussi compléments de a_2 .

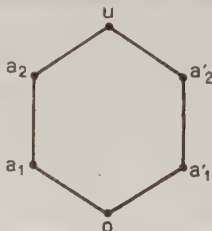


Fig. 7.

3. Une chaîne finie $\{o, a_1, \dots, u\}$ ayant plus de deux éléments n'est pas complémentée.

THÉORÈME 1. — Si le treillis T , avec 0 et u , est distributif, un élément complémenté x de T a un seul complément x' . Si a et b ont des compléments a' , b' , $a \cap b$ et $a \cup b$ ont les compléments

$$(a \cap b)' = a' \cup b', \quad (a \cup b)' = a' \cap b'.$$

Les éléments complémentés de T forment un sous-treillis T' de T .

Supposons que x admette les compléments x' , y' :

$$\begin{aligned} x \cap x' &= 0, & x \cup x' &= u; \\ x \cap y' &= 0, & x \cup y' &= u. \end{aligned}$$

Nous avons, en tenant compte de la distributivité,

$$x' = 0 \cup x' = (x \cap y') \cup x' = (x \cup x') \cap (y' \cup x') = u \cap (y' \cup x') = y' \cup x'.$$

De même, $y' = x' \cup y'$ et, par conséquent, $x' = y'$: un élément complémenté x a donc un complément unique dont, inversement, il est le complément unique : $(x')' = x$.

Soient a et b deux éléments complémentés. Nous avons

$$(a \cap b) \cap (a' \cup b') = (a \cap b \cap a') \cup (a \cap b \cap b') = 0 \cup 0 = 0$$

et

$$(a \cap b) \cup (a' \cup b') = (a \cup a' \cup b') \cap (b \cup b' \cup a') = u \cap u = u,$$

par conséquent, $a' \cup b'$ est complément (unique) de $a \cap b$; d'une façon duale, on voit que $a \cup b$ a pour complément $a' \cap b'$: l'ensemble T' des éléments complémentés de T est donc un sous-treillis de T ⁽¹⁾.

D'après le théorème précédent, un cas remarquable est celui d'un treillis, avec élément nul et élément universel, à la fois distributif et complémenté : $T = T'$. Un tel treillis est appelé *treillis de Boole* ⁽²⁾.

(1) L'application biunivoque $x \rightarrow x'$ de T' sur lui-même est ce qu'on appelle un *automorphisme dual* ou une *dualité* : toute relation entre éléments entraîne, pour les compléments, la relation correspondante où le signe $\cap$ est remplacé par $\cup$ et inversement (relation duale).

La première partie du théorème 1 est aussi une conséquence immédiate d'une remarquable propriété caractéristique des treillis distributifs : pour qu'un treillis soit distributif, il faut et il suffit que

$$x \cap a = x \cap b \quad \text{et} \quad x \cup a = x \cup b$$

entraînent $a = b$. Voir M. L. DUBREIL-JACOTIN, L. LESIEUR et R. CROISOT, *Leçons sur la Théorie des Treillis*..., 1^{re} partie chap. VIII, § 4, p. 106 et chap. VI, § 1, p. 75.

(2) Dès le milieu du XIX^e siècle, dans *The mathematical Analysis of Logic* (Cambridge, 1847) et *An investigation in to the laws of thought* (Londres, 1854), Boole a découvert cette importante notion, premier type de treillis mis en évidence.

Le treillis $\mathfrak{L}(E)$ des parties d'un ensemble E est une treillis de Boole ⁽¹⁾.

Dans un treillis T , soient a et b deux éléments vérifiant $a \subseteq b$ et x un élément compris entre a et b . Un élément x' , s'il existe, vérifiant

$$x \cap x' = a, \quad x \cup x' = b$$

est appelé *complément relatif* de x par rapport à a et b . On voit, comme plus haut, que cet élément x' est nécessairement *unique dans un treillis distributif* (il suffit de remplacer o par a et u par b).

Ce qui précède montre que certains types de treillis ont d'importantes propriétés *algébriques*, liées, non à la relation d'ordre, mais essentiellement aux *opérations* $\cap$ et $\cup$. Il est donc tout indiqué de caractériser les treillis par un *système d'axiomes portant sur ces opérations*. Nous avons déjà vu qu'elles sont *associatives, commutatives et idempotentes*. Mais, en général, elles ne sont pas distributives l'une par rapport à l'autre (voir § 5, exer. 16, p. 89). On a cependant une *propriété de distributivité affaiblie*, valable dans tout treillis, appelée *loi d'absorption*; elle s'exprime par les deux relations

$$(9) \quad x \cap (x \cup y) = x$$

et

$$(9') \quad x \cup (x \cap y) = x$$

vérifiées quels que soient $x, y \in T$, et conséquences immédiates de $x \cap y \subseteq x \subseteq x \cup y$.

THÉORÈME 2. — *Un ensemble T dans lequel sont définies deux opérations $\cap$ et $\cup$, associatives, commutatives, idempotentes et vérifiant la loi d'absorption (9) et (9'), est un treillis dans lequel $a \cup b$ et $a \cap b$ sont respectivement la borne supérieure et la borne inférieure de a et b .*

D'après (9), l'égalité $x \cup y = y$ entraîne $x \cap y = x$; inversement, d'après (9'), où l'on permute x et y , $x \cap y = x$ entraîne $x \cup y = y$. Les deux égalités $x \cup y = y$, $x \cap y = x$ sont donc *vérifiées en même temps*; posons dans ce cas $x \subseteq y$.

⁽¹⁾ Inversement, tout treillis de Boole est isomorphe à un treillis d'ensembles, comme l'a établi M. H. STONE, *Boolean algebras and their relation to topology* (Proc. Nat. Acad. Sc., t. 20, 1934, p. 197); *the Theory of representations for Boolean algebras* (Trans. Amer. Math. Soc., t. 40, 1936, p. 37).

La relation $\subseteq$ ainsi définie est *réflexive*, en raison de l'idempotence, et *transitive*, car $x \subseteq y$ et $y \subseteq z$ entraînent

$$x \cup z = x \cup (y \cup z) = (x \cup y) \cup z = y \cup z = z,$$

c'est-à-dire $x \subseteq z$. Elle est évidemment *propre*; c'est donc une *relation d'ordre partiel*.

On a $a \subseteq a \cup b$, de même $b \subseteq a \cup b$; et $a \subseteq r$, $b \subseteq r$, c'est-à-dire $a \cup r = r = b \cup r$, entraînent

$$r \cup (a \cup b) = (r \cup a) \cup b = r, \quad \text{c'est-à-dire} \quad a \cup b \subseteq r;$$

$a \cup b$ est donc majorant minimum de a et b . On verrait, de même, que $a \cap b$ est minorant maximum.

Remarque. — On voit, d'une façon analogue, qu'un ensemble E dans lequel est définie une opération $\cap$ associative, commutative et idempotente, est un $\cap$ -demi-treillis. La relation d'ordre $\subseteq$ est définie par

$$x \subseteq y \quad \text{si} \quad x = x \cap y$$

et $a \cap b$ est la borne inférieure de a et b .



CHAPITRE III.

GROUPES.

A. — DÉFINITION DES GROUPES.

1. Propriétés d'inversion dans un demi-groupe : notion de groupe. —

On appelle *groupe* tout ensemble G vérifiant les trois conditions suivantes :

- (Σ)
- I. Dans G est définie une *opération associative* (G est un *demi-groupe*);
 - II. G possède, par rapport à cette opération, un *élément-unité bilatère*, e ;
 - III. Tout élément a de G possède un *inverse unique*, a^{-1} :
 $aa^{-1} = a^{-1}a = e$.

Mais, comme nous allons le voir, on peut former un système d'axiomes (Σ_1) équivalent au précédent et se composant de conditions analogues, dont certaines, prises individuellement, seront *plus faibles* : ce système (Σ_1) va d'ailleurs apparaître naturellement grâce à une étude systématique des *propriétés d'inversion d'un demi-groupe* (que nous noterons multiplicativement). Nous serons conduits, en outre, à d'autres systèmes d'axiomes, formés de conditions variées.

LEMME 1. — *Dans un demi-groupe D possédant un élément-unité à droite e , tout élément a inversible à droite par rapport à e est simplifiable à droite.*

L'égalité $xa = ya$ entraîne, en effet, $xa.a' = ya.a'$. Or nous avons, a' désignant un inverse à droite de a ,

$$xa.a' = x.aa' = xe = x \quad \text{et, de même,} \quad ya.a' = y,$$

d'où

$$x = y.$$

LEMME 2. — Dans un demi-groupe D possédant un élément-unité à droite e , l'ensemble des éléments inversibles à droite est un sous-groupe S_d .

Les égalités $aa' = bb' = e$ entraînent

$$ab.b'a' = a.bb'.a' = ae.a' = aa' = e;$$

$b'a'$ est donc un inverse à droite de ab ⁽¹⁾.

Un cas remarquable est celui où $S_d = D$. D'après le lemme 1, nous avons la proposition suivante :

THEOREME 1. — Si un demi-groupe D possède un élément-unité à droite e et si tout élément de D est inversible à droite par rapport à e , la règle de simplification à droite est valable dans D .

L'énoncé précédent entraîne l'unicité du quotient à gauche y d'un élément m par un élément a ($m = ya$), dans la mesure où de tels quotients existent. On a immédiatement une condition suffisante pour que cette existence soit assurée.

LEMME 3. — Dans un demi-groupe D possédant un élément-unité à droite e , il existe, pour tout élément $m \in D$ et pour tout élément a inversible à gauche par rapport à e , au moins un quotient à gauche.

On a, en effet, a^* désignant un inverse à gauche de a ,

$$ma^*.a = m.a^*.a = me = m.$$

Il y a intérêt à se ramener aux hypothèses du théorème 1, ce que le lemme suivant permet de faire.

LEMME 4. — Si, dans un demi-groupe D possédant un élément-unité à droite e , un élément a' inversible à droite est l'inverse à droite d'un élément a , $aa' = e$, il en est aussi inverse à gauche, $a'a = e$.

(1) On a évidemment un énoncé analogue en remplaçant les mots « à droite » par les mots « à gauche ». On peut remarquer, en outre, que l'ensemble des éléments inversibles à droite par rapport à un élément-unité à gauche $\bar{e}$ est un sous-groupe, puisque $aa' = bb' = \bar{e}$ entraînent

$$ab.b'a' = a.bb'.a' = a.\bar{e}a' = aa' = \bar{e}.$$

L'ensemble des éléments inversibles à droite et à gauche par rapport à un élément-unité quelconque, n'est pas vide, puisqu'il contient cet élément-unité : c'est l'intersection de deux sous-groupes, donc un sous-groupe.

Soit a'' un inverse à droite de a' : $a'a'' = e$. En multipliant à droite par a'' les termes extrêmes des égalités

$$a' = a'e = a'.aa' = a'a.a',$$

nous obtenons

$$e = a'a.a'a'' = a'a.e = a'a,$$

ce qu'il fallait démontrer.

THÉOREME 2. — *Si un demi-groupe D possède un élément-unité à droite e et si tout élément $a \in D$ est inversible à droite par rapport à e , tout inverse à droite est inverse à gauche, e est élément-unité bilatère, et la règle de simplification est valable dans D.*

Soit, en effet, $aa' = e$; a' est lui-même inversible à droite : nous avons donc, d'après le lemme 4, $a'a = e$. Tout élément $a \in D$ est donc inversible à gauche par rapport à e . On le voit aussi, directement, de la façon suivante : posons $a'a = b$; nous avons $b^2 = a'aa'a = a'ea = b$, d'où, b' désignant un inverse à droite de b ,

$$b = be = b^2b' = bb' = e, \quad \text{c'est-à-dire} \quad a'a = e$$

L'élément-unité e est bilatère (donc seul élément-unité) puisqu'on a

$$ea = aa'.a = a.a'a = ae = a.$$

La règle de simplification et, par conséquent, l'unicité des inverses et des quotients, résulte du théorème 1 et de l'énoncé qui s'en déduit en remplaçant « à droite » par « à gauche ».

Premier système d'axiomes des groupes. — Considérons un ensemble G vérifiant les trois conditions suivantes :

- (Σ_1) $\left\{ \begin{array}{l} \text{I. Dans } G \text{ est définie une opération associative (} G \text{ est un demi-} \\ \text{groupe);} \\ \text{II}_d. G \text{ possède, par rapport à cette opération, au moins un élément-} \\ \text{unité à droite, } e; \\ \text{III}_d. \text{ Tout élément } a \in G \text{ possède au moins un inverse à droite, } a', \text{ par} \\ \text{rapport à } e. \end{array} \right.$

On a, d'après le théorème 2, les propositions suivantes :

IV. G est un *semi-groupe* (la règle de simplification est valable).

II. L'élément-unité e de G est bilatère et seul élément-unité.

III. Tout élément $a \in G$ a un *inverse unique* a^{-} , d'où, en tenant compte en outre du lemme 3 et de l'énoncé qui s'en déduit en permutant « à droite » et « à gauche » :

V. G est un *quasi-groupe*, c'est-à-dire vérifie l'axiome des quotients (chap. II, § 6, p. 91).

Puisque le système d'axiomes (Σ_1) comprend la condition I et entraîne II et III, il est équivalent au système (Σ) : G est un groupe.

On voit, de plus, qu'un groupe G est à la fois un semi-groupe et un quasi-groupe. La réciproque est vraie, et l'on peut même, comme nous allons le voir, partir d'hypothèses beaucoup plus faibles.

Considérons un groupoïde E possédant par rapport à son opération les deux propriétés suivantes :

- $(\Sigma_2) \left\{ \begin{array}{l} \text{I. } E \text{ est un demi-groupe ;} \\ \text{V'. Pour chaque couple d'éléments } a, m \in E, \text{ il existe au moins un} \\ \text{quotient à droite } x \text{ et un quotient à gauche } y \end{array} \right.$

$$m = ax = ya$$

et, d'une façon encore plus générale, remplaçons la propriété V' par la propriété plus faible

V". Le sous-ensemble E' des éléments a de E tels que, pour tout $m \in E$ chacune des équations

$$m = ax = ya$$

ait au moins une solution, n'est pas vide.

LEMME 3. — Les propriétés I et V" entraînent l'existence d'un élément-unité bilatère e . L'ensemble E^* des éléments inversibles coïncide avec E' . De plus, E' est un groupe.

Soit a un élément de E' .

D'après V", il existe au moins un élément e vérifiant l'égalité

$$ae = a.$$

Soit maintenant x un élément quelconque de E : il existe, d'après V", un élément r tel que l'on ait

$$x = ra,$$

d'où, en utilisant I,

$$xe = ra.e = r.ae = ra = x \quad \text{pour tout } x \in E;$$

e est donc élément-unité à droite.

Les hypothèses symétriques I et V" entraînent également l'existence d'au moins un élément-unité à gauche e' : e et e' sont égaux, comme

nous le savons ⁽¹⁾, et il n'y a pas d'autre élément-unité : nous avons donc la propriété II.

Tout élément a de E' est, d'après V'' (où l'on prend $m = e$), inversible à droite et à gauche; d'après le lemme (p. 93) tout inverse à droite de a est égal à tout inverse à gauche, et a possède un *inverse unique* a^- .

Réciproquement, tout élément a ayant un inverse a^- appartient à E' , puisque la condition V'' est vérifiée par $x = a^-m$ et $y = ma^-$. E' est donc l'ensemble des éléments inversibles. Or, le produit ab de deux éléments inversibles, a un inverse : $b^-a^- = (ab)^-$. E' est donc un sous-demi-groupe de E . Comme E' vérifie le système d'axiomes (Σ) , E' est un groupe.

Cela posé, si E vérifie le système (Σ_2) , nous avons $E' = E$: E est un groupe.

Il en résulte que les propriétés I et V' entraînent non seulement II, mais III (*existence et unicité de l'inverse*) ⁽²⁾, IV (*règle de simplification*), et l'*unicité des quotients*, donc l'*axiome des quotients* V.

Les propriétés caractéristiques I et V' constituent le *second système d'axiomes des groupes* (Σ_2) . On peut évidemment, dans le premier système, remplacer les axiomes II_d , III_d par les conditions symétriques II_g , III_g en substituant les mots « à gauche » aux mots « à droite ».

Comme l'a remarqué G. Thierrin ⁽³⁾, un autre système d'axiomes est le suivant :

$${}^4\Sigma_3) \left\{ \begin{array}{l} \text{I et IV. } G \text{ est un semi-groupe;} \\ \text{VI. Pour tout } x \in G, \text{ il existe au moins un } x' \in G \text{ tel que } xx'x = x. \end{array} \right.$$

En d'autres termes, *pour qu'un semi-groupe (infini) soit un groupe, il faut et il suffit qu'il vérifie la condition VI* (comme nous le verrons au paragraphe 2, un semi-groupe fini est toujours un groupe). La condition est *nécessaire* : si G est un groupe, et si x' désigne l'inverse de x , on a bien $xx'x = x$. Pour montrer qu'elle est *suffisante*, remarquons

⁽¹⁾ $e'e = e = e'$ (cf. chap. II, § 5 p. 77).

⁽²⁾ Il est facile d'établir directement la propriété III à partir de I, II et V' : tout élément a admet, par rapport à e , au moins un inverse à droite a' et au moins un inverse à gauche a^* . Or, comme nous l'avons vu (p. 93), de tels inverses, dans un demi-groupe, sont égaux dès qu'ils existent :

$$\begin{aligned} a^*aa' &= a^*.aa' = a^*e = a^* \\ &= a^*a.a' = ea' = a'. \end{aligned}$$

⁽³⁾ G. THIERRIN, *Sur une condition nécessaire et suffisante pour qu'un semi-groupe soit un groupe* (C. R. Acad. Sc., t. 232, 1951, p. 376).

que, dans un semi-groupe, la relation $xx'.x = x$ entraîne (d'après le corollaire 2, chap. II, § 5, p. 86) que xx' est élément-unité bilatère. On sait, d'autre part, qu'un tel élément est unique, et l'on voit que tout élément x a un inverse à droite x' : le système (Σ_1) est vérifié, et nous avons bien un groupe.

Établissons enfin l'indépendance des axiomes des groupes pour chacun des trois systèmes énoncés ⁽¹⁾.

1° Le demi-groupe abélien déjà rencontré (chap. II, § 5, p. 84)

$$(E'_2) \quad \begin{array}{c|cc} & e & a \\ \hline e & e & a \\ a & a & a \end{array}$$

vérifie I et II_d , mais non III_d , puisque a n'a pas d'inverse à droite.

Le groupoïde

$$(E'_2) \quad \begin{array}{c|cc} & e & a \\ \hline e & e & e \\ a & a & e \end{array}$$

vérifie II_d et III_d , sans être un demi-groupe, car on a

$$(aa)a = ea = e, \quad a(aa) = ae = a.$$

La propriété III_d n'a pas de sens indépendamment de II_d .

2° Les propriétés I et V' sont indépendantes, car, dans le demi-groupe

$$(E''_2) \quad \begin{array}{c|cc} & a & b \\ \hline a & a & a \\ b & a & a \end{array}$$

les quotients de b par a ou par b n'existent pas. D'autre part, le grou-

⁽¹⁾ Pour une étude plus complète des nombreuses et intéressantes questions soulevées par l'axiomatique des groupes, on pourra consulter notamment : R. BAER et F. LEVI, *Vollständige irreduzible Systeme von Gruppenaxiomen*, (*Sitzungsber. der Heidelberger Akad. der Wiss.*, Math. Natur. Kl., t. 18, 1932, p. 3); P. LORENZEN, *Ein Beitrag zur Gruppenaxiomatik*, (*Math. Zeitschr.*, t. 49, 1943, p. 313); B. STOLT, *Über Axiomensysteme die eine abstrakte Gruppe bestimmen*, Uppsala, Almqvist et Wicksells, 1953; R. CROISOT, *Demi-groupes et axiomatique des groupes* (*C. R. Acad. Sc.*, t. 237, 1953, p. 778).

poïde (abélien)

		a	b	c
	a	a	c	b
(E ₃)	b	c	b	a
	c	b	a	c

vérifie l'axiome des quotients $V = V' + V''$ sans être un demi-groupe, car nous avons

$$a(bc) = aa = a, \quad (ab)c = cc = c.$$

3° Les propriétés I et IV n'entraînent pas VI, puisqu'il existe des semi-groupes (infinis) qui ne sont pas des groupes : comme nous l'avons vu plus haut, (p. 91), le demi-groupe multiplicatif N des nombres naturels (zéro exclu) vérifie la règle de simplification, donc est un semi-groupe, mais ne vérifie pas l'axiome des quotients, donc n'est pas un groupe.

Les axiomes I et VI caractérisent une classe de demi-groupes, les *demi-groupes inversifs*, qui ont été étudiés par G. Thierrin (*loc. cit.*) et ne vérifient pas nécessairement la règle de simplification.

Un groupe est *abélien* si son opération est *commutative*.

Lorsqu'il n'est pas précisé qu'un groupe est abélien, on donne ordinairement à son opération, comme nous venons de le faire, le nom de multiplication et l'on utilise les notations correspondantes.

Pour un *groupe abélien*, on utilise très souvent la *notation additive*. Le groupe est dit alors *additif*, ou bien est appelé *module*. L'élément-unité prend le nom d'*élément-zéro* et est représenté par le signe O, l'élément-inverse de a est appelé *élément-opposé* et désigné par $-a$.

Exemples. — 1. Les transformations d'un ensemble M constituent un groupe, l'opération étant la composition des transformations : le premier système d'axiomes des groupes est, en effet, vérifié.

En particulier, l'ensemble des *substitutions* que l'on peut effectuer sur n objets distincts est un groupe, appelé *groupe symétrique* et désigné par S_n . Ce groupe est fini et son ordre est $n!$

Ces cas particuliers montrent déjà clairement l'importance de la notion de groupe, surtout si l'on veut bien les rapprocher des propriétés remarquables qui sont apparues à propos des axiomes des groupes, et des facilités de calcul qui en résultent.

2. Dans un demi-groupe D avec élément-unité e , l'ensemble G des *éléments inversibles* est un groupe : $e \in G$; $u \in G$ entraîne $u^{-1} \in G$, puisque

$$uu^{-1} = u^{-1}u = e;$$

$u_1 \in G, u_2 \in G$ entraînent $u_1 u_2 \in G$, puisque

$$(u_1 u_2) (u_2^{-1} u_1^{-1}) = u_1 (u_2 u_2^{-1}) u_1^{-1} = e$$

et

$$(u_2^{-1} u_1^{-1}) (u_1 u_2) = u_2^{-1} (u_1^{-1} u_1) u_2 = e.$$

3. L'ensemble des vecteurs libres du plan, ou de l'espace, est un groupe abélien par rapport à l'addition géométrique.

4. Construisons un groupe fini d'ordre 2, $G_2 = \{e, a\}$. Comme on a nécessairement

$$e^2 = e, \quad ea = ae = a,$$

G sera entièrement défini si nous fixons la valeur de a^2 . Or, nous ne pouvons pas prendre $a^2 = a$, car, dans ce cas, a n'aurait pas d'inverse. Posons donc $a^2 = e$, ce qui nous donne l'unique possibilité

(G_2)		e	a
	e	e	a
	a	a	e

On vérifie immédiatement que G_2 est bien un groupe, d'ailleurs abélien.

Exercices. — 1. Dans un groupe G , plus généralement dans tout semi-groupe admettant un élément-unité à droite, il n'y a pas d'autre élément idempotent que l'élément-unité.

2. L'ensemble des parties $\mathcal{X}(E)$ d'un ensemble E est un groupe par rapport à la différence symétrique (cf. chap. II, § 5, ex. 1, p. 77; 4, p. 80; 9, p. 87 et § 6, ex. 3, p. 94).

3. En considérant le groupoïde

	e	a	b	c	d	h
e	e	a	b	c	d	h
a	a	b	c	d	h	e
b	b	c	e	h	a	d
c	c	d	h	e	b	a
d	d	h	a	b	e	c
h	h	e	d	a	c	b

montrer que, même combiné avec la commutativité et l'existence d'un élément-unité, l'axiome des quotients n'entraîne pas l'associativité.

2. **Groupes finis.** — Pour un groupoïde fini, l'axiome des quotients V et la règle de simplification IV sont, comme nous l'avons vu, des propriétés équivalentes.

Nous avons donc, pour les groupes finis, le troisième système d'axiomes ⁽¹⁾

$$(\Sigma'_3) \quad \left\{ \begin{array}{l} \text{I. Associativité de l'opération;} \\ \text{IV. Règle de simplification.} \end{array} \right.$$

En d'autres termes, tout semi-groupe fini est un groupe.

Considérons un groupoïde fini E, possédant un élément-unité bilatère e, et dans lequel tout élément x possède un inverse unique x⁻ (propriétés II et III). Pour que E soit un groupe, il faut et il suffit que son opération soit associative. Nous allons transformer cette condition en considérant la table de multiplication de E. Désignons par e = a₁, a₂, ..., a_n les éléments de E. Inscrivons-les, dans cet ordre, dans la première colonne de la table; et, dans la première ligne, inscrivons, non plus ces éléments, mais leurs inverses, pris dans le même ordre. La table prend la forme suivante, dite *forme normale*

$$\begin{array}{cccc} e = a_1 & a_2 & \dots & a_n, \\ & a_2 & e & \dots \dots, \\ & \dots & \dots & \dots \dots, \\ & a_n & \dots & \dots e. \end{array}$$

En désignant par a_{ij} l'élément situé dans la i^{ème} ligne et la j^{ème} colonne, nous avons

$$a_{ij} = a_i \cdot a_j^- = a_{i1} a_{1j},$$

d'où

$$a_{is} a_{rj} = (a_i a_s^-) (a_r a_j^-).$$

Si E est un groupe, il vient, en prenant s = r et tenant compte de l'associativité,

$$a_{ir} a_{rj} = a_i a_r^- a_r a_j^- = a_{ij},$$

ce qui constitue la *propriété du rectangle pour la forme normale* (le sommet a_{rr} = e est sur la diagonale principale).

Inversement, cette propriété entraîne, avec II et III, l'associativité. Pour le voir, remarquons d'abord que tous les éléments d'une même ligne ou d'une même colonne sont différents, car l'égalité

$$a_{rj} = a_{rk} \quad (j \neq k),$$

par exemple, entraînerait, en multipliant à gauche par a_{1r},

$$a_{1j} = a_{1k} \quad (j \neq k).$$

⁽¹⁾ Les propriétés I et IV sont indépendantes, puisque IV équivaut à une propriété indépendante de I. Les exemples donnés plus haut (groupoïdes E₂'' et E₃) permettent d'ailleurs de vérifier cette indépendance.

Or, les éléments de la première colonne sont tous différents et il en est de même pour ceux de la première ligne, puisque chaque élément a un inverse unique.

Cela posé, soient x, y, z trois éléments quelconques de E . Il existe, d'après ce qui précède, des entiers i, j, k tels que l'on ait

$$x = a_i = a_{i1}, \quad y = a_{1j}, \quad z = a_{jk}.$$

Nous avons donc

$$(xy)z = (a_{i1}a_{1j})a_{jk} = a_{ij}a_{jk} = a_{ik},$$

$$x(yz) = a_{i1}(a_{1j}a_{jk}) = a_{i1}a_{1k} = a_{ik}$$

et l'opération est bien associative.

Exemple. — Dans l'ensemble $E = \{1, 2, 3, 4\}$, il existe trois substitutions qui, échangeant deux éléments, échangent aussi les deux autres. Ce sont :

$$a = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}, \quad b = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}, \quad c = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}.$$

Désignons par e la substitution identique; nous avons

$$a^2 = b^2 = c^2 = e$$

et

$$bc = cb = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = a.$$

De même,

$$ca = ac = b, \quad ab = ba = c.$$

Les quatre substitutions e, a, b, c forment donc un *groupe abélien* V_4 , dans lequel chaque élément est involutif. Ce groupe est désigné sous le nom de *groupe de Klein*.

B. — SOUS-GROUPES.

3. Conditions nécessaires et suffisantes. — On donne le nom de *sous-groupe* d'un groupe G à tout sous-ensemble *non vide* de G qui est lui-même un groupe par rapport à l'opération considérée dans G . L'ensemble $\{e\}$, constitué uniquement par l'élément-unité, et le groupe G lui-même sont des sous-groupes particuliers : on appelle *vrai sous-groupe*, *sous-groupe véritable*, ou *propre*, tout autre sous-groupe de G ⁽¹⁾. Précisons à quelles conditions un sous-ensemble non vide G' est sous-groupe de G .

(1) Un sous-groupe d'un module, c'est-à-dire d'un groupe abélien additif, prend le nom de *sous-module*.

1° Il faut d'abord évidemment que G' soit sous-groupe de G , c'est-à-dire contienne, avec deux éléments x et y , non forcément distincts, de G , leur produit xy ; autrement, l'opération de G ne serait pas une opération agissant dans G' . Si G' est un sous-groupe, l'opération, associative dans G , l'est aussi dans G' .

2° Il faut encore qu'il existe dans G' au moins un élément-unité à droite e' . Mais on aura alors, e désignant l'élément-unité de G

$$e'e' = e' = e'e,$$

ce qui exige

$$e' = e.$$

Par suite, G' doit contenir l'élément-unité, e , de G .

3° Il faut enfin que tout élément x de G' ait dans G' au moins un inverse à droite, x' . Or, la relation

$$xx' = e$$

admet dans G la solution unique $x' = x^{-}$, x^{-} étant l'inverse de x dans G : G' doit donc contenir x^{-} en même temps que x .

Dans leur ensemble, les trois conditions nécessaires que nous venons d'obtenir sont aussi suffisantes, puisqu'elles entraînent, pour G' , la validité du système d'axiomes Σ_1 . Mais la seconde condition est visiblement une conséquence des deux autres et du fait que G' n'est pas vide, ce qui nous conduit à l'énoncé suivant :

A. Pour qu'un sous-ensemble non vide G' d'un groupe G soit sous-groupe de G , il faut et il suffit que G' contienne en même temps que deux éléments x et y de G , distincts ou non, leur produit xy , et en même temps qu'un élément x son inverse x^{-} . Si G est donné sous forme additive, G' doit contenir $x + y$ en même temps que x et y et $-x$ en même temps que x .

On peut donner à cet énoncé une forme équivalente, souvent utilisée :

A'. Pour qu'un sous-ensemble non vide G' d'un groupe G soit sous-groupe de G , il faut et il suffit que G' contienne, en même temps que deux éléments x et y de G , le produit xy^{-} , ou la somme $x + (-y)$ si G est écrit sous forme additive.

L'énoncé A entraîne immédiatement la condition A'. Réciproquement, si A' est vérifiée, G' , n'étant pas vide, contient au moins un élément x et, par conséquent, aussi $xx^{-} = e$. Si y est un élément quelconque

de G' , G' contient $ey^- = y^-$, et $x \cdot (y^-)^- = xy$, et le système de conditions A est vérifié.

L'énoncé A' peut encore se mettre sous la forme équivalente :

A". Pour qu'un complexe H d'un groupe G soit un sous-groupe de G, il faut et il suffit que H soit unitaire à droite (par exemple).

Si H est un sous-groupe de G, les relations

$$h \in H, \quad x \in G, \quad xh = h' \in H$$

entraînent

$$x = h'h^- \in H,$$

d'après A' : H est bien unitaire à droite, et la condition A" est nécessaire. On voit symétriquement que tout sous-groupe est un complexe unitaire à gauche, donc un complexe unitaire.

Inversement, soit C un complexe unitaire à droite dans un groupe G. Si $x, y \in C$, on a

$$xy^-.y = x.y^-y = xe = x \in C,$$

d'où $xy^- \in C$: la condition A' étant vérifiée, C est bien un sous-groupe.

On voit que, dans un groupe, tout complexe unitaire d'un côté est aussi unitaire de l'autre.

Les énoncés A et A' sont utilisés, par exemple, pour reconnaître si un ensemble G' de transformations d'un ensemble E est un groupe; car l'ensemble G' est contenu dans le groupe G de toutes les transformations de E ⁽¹⁾.

Revenons à l'énoncé A. La première condition qui y figure exprime que G' est un sous-groupoïde de G. Il arrive qu'elle soit remplie d'elle-même (en raison de la définition même de G'). Nous avons alors l'énoncé suivant :

B. Pour qu'un sous-groupoïde G' d'un groupe G soit un sous-groupe de G, il faut et il suffit que G' contienne x^- en même temps que x .

Si G' est le groupoïde engendré par un certain ensemble E, fini (non vide) ou infini, d'éléments de G, tout élément x de G' est le produit d'un nombre fini de puissances d'éléments générateurs (qui ne sont pas

(1) C'est pour cette raison que l'associativité, qui jouait un rôle fondamental dans la définition d'un groupe, n'intervient pas ici. Ce fait, joint à l'importance des groupes de transformations, conduit trop souvent à donner, pour la définition des groupes, des systèmes de conditions incorrects.

forcément distincts deux à deux) :

$$x = a^\alpha b^\beta \dots l^\lambda \quad (a, b, \dots, l \in E).$$

Or, on a

$$x^- = (l^-)^\lambda \dots (b^-)^\beta (a^-)^\alpha,$$

et, par suite, x^- appartient à G' dès que a^- , b^- , ... eux-mêmes lui appartiennent, en particulier dès que E est la réunion d'un ensemble M constitué par certains éléments de G et de l'ensemble M^- constitué par les éléments inverses, d'où l'énoncé suivant :

B'. Le sous-groupoïde G' engendré par un ensemble $M \neq \emptyset$ d'éléments de G et par leurs inverses, est un sous-groupe de G , on l'appelle groupe, ou sous-groupe, engendré par l'ensemble M . Si M est fini, $M = \{a, b, \dots, l\}$, on écrit $G' = (a, b, \dots, l)$.

En particulier, le groupoïde engendré par un ensemble d'éléments *involutifs* d'un groupe G est un sous-groupe de G . Par exemple, dans le groupe de Klein V_4 (§ 2, p. 107), un élément a distinct de l'élément-unité, étant involutif, engendre un sous-groupe $\{e, a\}$ d'ordre 2. V_4 n'admet pas d'autres sous-groupes véritables que les trois sous-groupes ainsi obtenus, puisque nous avons les relations $ab = c, \dots$

Tout sous-groupe H contenant un sous-ensemble $M (\neq \emptyset)$ de G , contient le sous-groupe G' engendré par M ; G' est, par suite, *le plus petit sous-groupe de G contenant M* . On peut l'obtenir directement en remarquant que la famille $\mathcal{S}$ de tous les sous-groupes de G vérifie les conditions de Moore (chap. I, § 11, p. 52), puisque : *a.* $G \in \mathcal{S}$; *b.* l'intersection

$$I = \bigcap_{H \in \mathcal{S}} H$$

d'une famille non vide $\mathcal{F}$ de sous-groupes H de G est un sous-groupe, car, si deux éléments x, y de G appartiennent à I , donc à chaque groupe $H \in \mathcal{F}$, le produit xy appartient à chaque groupe H , donc à I .

Il en résulte que $\mathcal{S}$ est un treillis complet, dans lequel l'union d'une famille $\mathcal{F}$ de sous-groupes est l'intersection des sous-groupes S contenant chaque $A \in \mathcal{F}$. A ce treillis est associée une *fermeture* des complexes, associant à chaque complexe M de G le plus petit sous-groupe $\bar{M}$ contenant M :

$$\bar{M} = \bigcap_{M \subseteq H \in \mathcal{S}} H = G'.$$

Cette fermeture sera étudiée au paragraphe 5.

Exercice. — Soit G le groupe des vecteurs libres de l'espace par rapport à l'addition géométrique. L'ensemble des vecteurs de G parallèles à une droite ou à un plan sont des sous-groupes de G .

4. Groupes cycliques. — L'énoncé B' fournit un procédé général pour former des sous-groupes d'un groupe donné. Le cas le plus simple est celui du sous-groupe engendré par un seul élément a , on lui donne le nom de sous-groupe *cyclique*. Il se compose des puissances de a , de celles de a^{-} , et de l'élément-unité $e = aa^{-}$. Il est visiblement abélien. Si les éléments précédents sont tous distincts, le groupe cyclique engendré par a est *infini*, l'élément générateur a est dit d'*ordre infini*. Dans le cas contraire, on a entre ces éléments au moins une égalité qui, multipliée par une puissance convenable de a ou de a^{-} , peut se ramener à la forme

$$(1) \quad a^h = e,$$

où h est un nombre naturel. Soit n la plus petite valeur de h telle que (1) soit vérifiée. Si nous excluons le cas trivial du sous-groupe cyclique engendré par l'élément-unité, nous avons $n > 1$ et, par suite,

$$a \cdot a^{n-1} = e, \quad \text{donc} \quad a^{n-1} = a^{-},$$

de sorte que le groupe cyclique engendré par a n'est autre que le groupoïde engendré par cet élément. *Ce groupe est fini et d'ordre n .* On a, en effet, quel que soit l'entier k ,

$$a^{m+kn} = a^m,$$

et les n éléments

$$a, \quad a^2, \quad \dots, \quad a^{n-1} = a^{-}, \quad a^n = e$$

sont distincts, car une égalité de la forme

$$a^p = a^q, \quad \text{avec} \quad 1 \leq q < p \leq n$$

entraînerait

$$a^{p-q} = e,$$

contrairement à la définition de n . Le nombre naturel n est appelé *ordre* de l'élément a , l'ordre d'un élément est donc, par définition, l'ordre du groupe cyclique qu'il engendre.

Si G est un groupe fini, le groupe cyclique engendré par un élément quelconque a est, lui aussi, fini et, par suite, a^{-} est une puissance de a . Nous avons donc, d'après l'énoncé B. l'importante proposition suivante :

B". Tout sous-groupe d'un groupe fini G est sous-groupe de G ; et, plus généralement,

B". Dans un groupe G quelconque, tout sous-groupe engendré par des éléments d'ordre fini est un sous-groupe de G .

THÉORÈME. — Tout sous-groupe C' d'un groupe cyclique $C = (a)$ est lui-même cyclique.

Si $C' = (e)$, le théorème est vrai. Supposons $C' \neq (e)$; si $(a^{-})^m \in C'$, son inverse a^m appartient aussi à C' ; il existe donc au moins une puissance non nulle de a appartenant à C' ; soit n le plus petit nombre naturel vérifiant la relation $a^n \in C'$. Le groupe cyclique (a^n) est contenu dans C' . Inversement, si $x = a^m$ est un élément de C appartenant à C' , on a, en désignant par q et r le quotient et le reste de m par n

$$a^m[(a^n)^{-}]^q = a^r a^{nq} [(a^n)^{-}]^q = a^r \in C' \quad (0 \leq r < n),$$

ce qui exige

$$r = 0 \quad \text{et} \quad x = (a^n)^q.$$

Il en résulte que si $(a^{-})^m$ appartient à C' , il appartient à (a^n) . On a donc

$$C' \subseteq (a^n)$$

et, par conséquent, $C' = (a^n)$.

On peut définir un groupe G d'une manière abstraite en donnant un système $\{a, b, \dots\}$ d'éléments générateurs. Les éléments du groupe sont les produits que l'on peut former à partir de ces éléments et de leurs inverses formels $a^{-}, b^{-}, \dots$ en tenant compte des règles de calcul des groupes, c'est-à-dire de l'associativité et des formules

$$(2) \quad aa^{-} = bb^{-} = \dots = e,$$

Ces produits ne sont d'ailleurs pas nécessairement des éléments distincts : on peut leur imposer certaines relations d'égalité, dites *relations fondamentales*, qui ne sont pas des conséquences de (2), et qui achèvent de définir le groupe. Ainsi, un groupe cyclique d'ordre n est défini par un générateur a avec la relation fondamentale

$$a^n = e \quad (\text{ou } a^{-} = a^{n-1}).$$

S'il n'existe aucune relation fondamentale, le groupe est dit *libre*. Un groupe cyclique infini est libre.

Exercices. — 1. Montrer que tout sous-groupe cyclique infini G' d'un groupe G admet une infinité de sous-groupes, eux-mêmes cycliques et infinis.

2. Dans l'ensemble $E = \{1, 2, \dots, n\}$, on appelle *permutations circulaires* les substitutions de la forme

$$\sigma_i = \begin{pmatrix} 1 & 2 & \dots & n-i+1 & n-i+2 & \dots & n \\ i & i+1 & \dots & n & 1 & \dots & i-1 \end{pmatrix}.$$

Montrer que ces substitutions forment un groupe cyclique d'ordre n .

3. On considère le groupe G dont l'élément-unité est e , et qui est engendré par deux éléments a et b , vérifiant les relations fondamentales

$$a^3 = e, \quad b^2 = e, \quad aba = b.$$

Écrire la table de multiplication de G , sous la forme ordinaire, puis sous la forme normale. G est-il abélien? Quels sont les différents sous-groupes de G ?

4. Soit S un *demi-groupe cyclique*, c'est-à-dire engendré par un élément a , et fini.

1° Il existe deux entiers m et n tels que

$$a^m = a^n \quad (m < n).$$

2° n étant choisi *minimum* dans la relation précédente, on a

$$S = \{a, a^2, \dots, a^m, \dots, a^{n-1}\}$$

et l'ensemble $C = \{a^m, \dots, a^{n-1}\}$ est un *groupe cyclique*.

Cf. D. REES, *On semi-groups* (Proc. Cambridge Phil. Soc., t. 36, 1940, p. 388).

Déduire de ce qui précède qu'un *semi-groupe* dont tous les éléments sont d'ordre fini est un *groupe*.

5. **Complexes et sous-groupes d'un groupe.** — Dans un groupe G , on associe à tout complexe C le *complexe inverse* C^- ; qui est, par définition, l'ensemble des inverses des éléments de C .

On a

$$(C^-)^- = C,$$

et, en posant $E = \{e\}$,

$$E \subseteq C^-,$$

l'égalité n'ayant lieu que si C comprend un seul élément.

La relation $C \subseteq C_1$, entraîne $C^- \subseteq C_1^-$. L'inverse du complexe-produit AB est B^-A^- ; les inverses de $A \cap B$ et de $A \cup B$ sont respectivement $A^- \cap B^-$ et $A^- \cup B^-$.

Si H est un sous-groupe de G , on a

$$H^2 = H, \quad H^- = H.$$

Inversement, les conditions pour qu'un complexe H soit sous-groupe

de G s'expriment par l'un des systèmes de relations suivants :

$$\begin{aligned} H^2 \subseteq H \quad \text{et} \quad H^- \subseteq H \quad (\text{condition A}), \\ HH^- \subseteq H \quad (\text{condition A}'). \end{aligned}$$

et, dans le cas où G est fini

$$HH^2 \subseteq H \quad (\text{condition B}').$$

THÉOREME 1. — Soient H un sous-groupe de G , et K un complexe contenu dans H , $K \subseteq H$. On a

$$HK = H$$

(et, de même, $KH = H$).

Nous avons, en effet,

$$HK \subseteq H^2 = H,$$

et, de même, puisque K^- est contenu dans $H^- = H$, $HK^- \subseteq H$. D'autre part, nous pouvons écrire, en posant toujours $E = \{e\}$,

$$H = HE \subseteq HK^-K \subseteq HK,$$

d'où l'égalité $HK = H$.

Ce théorème est particulièrement utile quand K est un sous-groupe H' de H , on se réduit à un seul élément h de H .

Considérons un ensemble $\mathcal{M}$ non vide de complexes K d'un groupe G , et, d'autre part, un ensemble Σ de sous-groupes de G vérifiant les deux conditions de Moore : 1° toute intersection de sous-groupes de Σ appartient à Σ ; 2° $G \in \Sigma$. Σ est donc un treillis complet, sous-ensemble du treillis de tous les sous-groupes de G .

Soit $\mathcal{M}'$ l'ensemble des sous-groupes $A \in \Sigma$ tels que l'on ait

$$K \subseteq A \quad \text{pour tout } K \in \mathcal{M}.$$

On a $G \in \mathcal{M}'$, donc $\mathcal{M}'$ n'est pas vide. L'intersection

$$L_{\Sigma} = \bigcap_{A \in \mathcal{M}'} A$$

est un sous-groupe de G appartenant à Σ , appelé *groupe composé dans Σ des complexes $K \in \mathcal{M}$* . On a $K \subseteq L_{\Sigma}$, pour tout $K \in \mathcal{M}$; donc le groupe L_{Σ} appartient à l'ensemble $\mathcal{M}'$: c'est le plus petit sous-groupe de l'ensemble Σ contenant tous les complexes de l'ensemble $\mathcal{M}$ ⁽¹⁾.

(1) Cette définition générale nous sera utile plus loin.

Si, $\mathcal{M}$ étant fixe, nous remplaçons Σ par un autre ensemble de sous-groupes $\Sigma' \subseteq \Sigma$, nous avons évidemment

$$L_{\Sigma'} \supseteq L_{\Sigma}.$$

Si nous prenons, en particulier, comme ensemble Σ l'ensemble de tous les sous-groupes de G , nous obtenons un groupe L , appelé *groupe composé* des complexes $K \in \mathcal{M}$, et qui est le plus petit de tous les groupes L_{Σ} possibles; si les complexes K sont des sous-groupes, leur groupe composé L est leur union dans le treillis des sous-groupes de G .

THÉOREME 2. — *Le groupe composé L d'un ensemble $\mathcal{M}$ de complexes K coïncide avec le groupe L_1 engendré par la réunion $U = \bigcup_{K \in \mathcal{M}} K$ de ces complexes. En désignant par $\overline{K}$ le groupe engendré par K , on a :*

$$L = \overline{\bigcup_{K \in \mathcal{M}} K} = \overline{\bigcup_{K \in \mathcal{M}} K}$$

L'ensemble $\mathcal{M}'$ des sous-groupes contenant tous les complexes $K \in \mathcal{M}$ n'est autre que l'ensemble $\mathcal{M}'_1$ des sous-groupes contenant la réunion de ces complexes : comme on a

$$L = \bigcap_{H \in \mathcal{M}'} H \quad \text{et} \quad L_1 = \bigcap_{H \in \mathcal{M}'_1} H$$

il vient

$$L = L_1 = \overline{\bigcup_{K \in \mathcal{M}} K}.$$

L'égalité $\overline{\bigcup_{K \in \mathcal{M}} K} = \overline{\bigcup_{K \in \mathcal{M}} \overline{K}}$ est un cas particulier d'une formule générale concernant les *fermetures* (cf. chap. I, §, 11, exerc. 3, p. 55) : $K \subseteq \overline{K}$ entraîne

$$\bigcup_{K \in \mathcal{M}} K \subseteq \bigcup_{K \in \mathcal{M}} \overline{K}, \quad \text{d'où} \quad \overline{\bigcup_{K \in \mathcal{M}} K} \subseteq \overline{\bigcup_{K \in \mathcal{M}} \overline{K}};$$

inversement, $K \subseteq \bigcup_{K \in \mathcal{M}} K$ entraîne

$$\overline{K} \subseteq \overline{\bigcup_{K \in \mathcal{M}} K}, \quad \text{d'où} \quad \bigcup_{K \in \mathcal{M}} \overline{K} \subseteq \overline{\bigcup_{K \in \mathcal{M}} K}$$

et, en prenant les fermetures, $\bigcup_{K \in \mathcal{K}} \overline{K} \subseteq \overline{\bigcup_{K \in \mathcal{K}} K}$ et, par conséquent, l'égalité.

En raison du théorème précédent, on donne encore au groupe L le nom de *réunion complète* des complexes K .

THÉOREME 3. — 1° *Le groupe composé L d'un ensemble $\mathcal{S}$ de sous-groupes S de G coïncide avec l'ensemble C de tous les produits FINIS $x_1, x_1x_2, \dots, x_1x_2\dots x_\lambda, \dots$ d'éléments x_i de groupes S_i (distincts ou non) appartenant à $\mathcal{S}$.*

2° *Si $\mathcal{S}$ est fini, $\mathcal{S} = \{S_1, \dots, S_n\}$, L coïncide également avec le groupe $\bar{P}$ engendré par le complexe-produit $P = S_1S_2\dots S_n$.*

1° L'ensemble C est un sous-groupe de G , puisque, si

$$x = x_1 \dots x_\lambda \quad (x_i \in S_i, \quad S_i \in \mathcal{S})$$

et

$$y = y_1 \dots y_\mu \quad (y_j \in S'_j, \quad S'_j \in \mathcal{S})$$

sont des éléments de C , $xy^{-1} = x_1 \dots x_\lambda y_\mu^{-1} \dots y_1^{-1}$ en est un aussi. D'autre part, ce groupe C contient chaque groupe S de la famille $\mathcal{S}$, d'où $L \subseteq C$. Or, dans chaque produit $x = x_1 \dots x_\lambda$, on a $x_i \in S_i \subseteq L$: cela entraîne $x \in L$, donc $C \subseteq L$, d'où l'égalité $C = L$.

2° Puisque l'élément-unité e de G appartient à chacun des groupes S_i , nous avons $S_i \subseteq P$ ($i = 1, \dots, n$), d'où

$$\bigcup_{i=1, \dots, n} S_i \subseteq P \subseteq C = L,$$

ce qui entraîne

$$L \subseteq \bar{P} \subseteq \bar{L} = L,$$

d'où l'égalité $L = \bar{P}$.

Remarque. — Le complexe $P = S_1 \dots S_n$ dépend, en général, de l'ordre dans lequel les groupes S_i sont numérotés; $\bar{P} = L$, au contraire, n'en dépend pas; on a, en particulier, pour deux sous-groupes A et B de G , $\overline{AB} = \overline{BA}$.

COROLLAIRE. — *Si le complexe AB produit de deux sous-groupes A et B est un groupe, ce groupe est le groupe composé de A et de B .*

Le théorème suivant indique précisément à quelle condition le complexe AB produit de deux sous-groupes A et B est un groupe.

THÉOREME 4. — *Pour que le complexe produit $P = AB$ de deux sous-groupes de G soit un sous-groupe, il faut et il suffit que A et B soient permutables, ce qui a toujours lieu si G est abélien.*

Si, en effet, AB est un sous-groupe, il coïncide avec le complexe inverse $B^{-1}A^{-1} = BA$, donc A et B sont permutables.

Inversement, si A et B sont permutables, nous avons

$$\begin{aligned} P^{-1} &= B^{-1}A^{-1} = BA = AB = P, \\ P^2 &= ABAB = A^2B^2 = AB = P; \end{aligned}$$

P est donc un sous-groupe de G .

Nous ferons encore la remarque suivante. Pour que deux sous-groupes A et B soient permutables, il suffit que l'on ait, par exemple, $BA \subseteq AB$, c'est-à-dire que A soit permutable à droite avec B . Cette condition entraîne, en effet, en prenant les inverses,

$$A^{-1}B^{-1} \subseteq B^{-1}A^{-1},$$

c'est-à-dire

$$AB \subseteq BA, \quad \text{d'où} \quad AB = BA.$$

Exercices. — 1. Dans le groupe G des vecteurs libres de l'espace, par rapport à l'addition géométrique, on considère les sous-groupes A et B des vecteurs parallèles respectivement à deux plans P et Q . Quels sont l'intersection et le groupe composé de A et B ?

2. Soit G le groupe des transformations ponctuelles du plan euclidien. Les rotations de centre O forment un sous-groupe A de G ; les homothéties de centre O forment un sous-groupe B . Le complexe AB est-il un groupe?

6. Groupes de transformations; propriétés d'invariance. — Une transformation σ d'un ensemble $E = \{a, b, \dots\}$ laisse invariant un élément a de E si elle le transforme en lui-même

$$\sigma a = a.$$

Plus généralement, σ laisse invariant un sous-ensemble A de E si l'ensemble image σA coïncide avec A

$$\sigma A = A.$$

Pour cela, il faut et il suffit que l'on ait

$$(1) \quad \sigma x \in A \quad \text{et} \quad \sigma^{-1}x \in A \quad \text{pour tout } x \in A.$$

La première de ces conditions exprime, en effet, que l'on a

$$\sigma A \subseteq A;$$

la seconde exprime que

$$A \subseteq \sigma A.$$

c'est-à-dire que tout élément de A est obtenu comme image.

Dans le cas particulier d'un *élément invariant*, $A = \{a\}$, les deux conditions (1) se confondent. Plus généralement, il en est ainsi dès que A est fini.

Exemples. — 1. E étant l'ensemble des points du plan, une rotation σ de centre O laisse invariant le point O ; elle laisse également invariant l'ensemble des points d'une circonférence quelconque de centre O , ou l'ensemble des points intérieurs à une telle circonférence.

2. E étant l'ensemble des points d'un axe $x'Ox$, la translation τ définie par

$$\tau x = x + 1$$

ne laisse pas invariant l'ensemble A des points situés à droite de O ($x > 0$). On a

$$\tau A \subset A.$$

On dit qu'un ensemble H de transformations, en particulier un demi-groupe ou un groupe, laisse invariant un sous-ensemble A de E si *chaque transformation de H laisse A invariant*

$$\sigma A = A \quad \text{pour tout } \sigma \in H.$$

L'ensemble de toutes les transformations de E qui laissent un sous-ensemble donné A invariant, est un groupe Γ_A . En effet, les conditions (1) étant symétriques en σ et σ^{-1} , cet ensemble contient σ^{-1} dès qu'il contient σ . D'autre part, il contient le produit $\tau\sigma$ en même temps que σ et τ . Si maintenant nous nous donnons également un ensemble M de transformations, l'ensemble des transformations contenues dans M et qui laissent A invariant est l'intersection $M \cap \Gamma_A$. Si M est un groupe G , cet ensemble est le sous-groupe $G_A = G \cap \Gamma_A$.

L'ensemble H_A des transformations du groupe G qui laissent invariant *chaque* élément a de A est

$$H_A = \bigcap_{a \in A} G_a$$

et nous avons évidemment $H_A \subseteq G_A$.

Inversement, à tout sous-groupe H de G , associons la partie B_H de E formée des éléments invariants par toute transformation $\sigma \in H$. Nous avons ainsi, entre l'ensemble $\mathfrak{P}(E) = \mathfrak{P}$ des parties de E et l'ensemble $\mathfrak{S}$ des sous-groupes de G une double correspondance, définie par deux

fonctions uniformes f, φ :

$$(C) \quad A \rightarrow H_A = fA, \quad H \rightarrow B_H = \varphi H.$$

Cette correspondance (C) possède les propriétés suivantes, qui s'obtiennent immédiatement à partir des définitions :

1. $A \subseteq A_1$ entraîne $fA \supseteq fA_1$;
- 1'. $H \subseteq H_1$ entraîne $\varphi H \supseteq \varphi H_1$;
2. On a $A \subseteq \varphi fA$;
- 2'. On a $H \subseteq f\varphi H$.

D'une façon générale, on appelle *correspondance de Galois* entre deux ensembles partiellement ordonnés $\mathcal{X} = \{A, \dots\}$, $\mathcal{S} = \{H, \dots\}$ toute correspondance, définie par deux applications uniformes f de $\mathcal{X}$ dans $\mathcal{S}$, φ de $\mathcal{S}$ dans $\mathcal{X}$:

$$A \rightarrow fA, \quad H \rightarrow \varphi H$$

qui vérifie les conditions 1, 1', 2, 2' ci-dessus ⁽¹⁾.

En prenant $H = fA$ dans 2', nous obtenons $f\varphi fA \supseteq fA$; or, d'après 2 et 1, nous avons $f\varphi fA \subseteq fA$, d'où

$$(3) \quad f\varphi fA = fA$$

et, par conséquent,

$$(4) \quad \varphi f\varphi fA = \varphi fA.$$

Il en résulte que, dans $\mathcal{X}$, l'application

$$A \rightarrow \varphi fA = \bar{A}$$

est une fermeture, puisqu'on a $A \subseteq \varphi fA$ d'après 2, $\bar{\bar{A}} = \bar{A}$, et que $A \subseteq A_1$ entraîne $\bar{A} \subseteq \bar{A}_1$, d'après 1 et 1'. L'égalité $f\varphi fA = fA$ exprime

⁽¹⁾ On rencontre dans la Théorie de Galois (relative à la résolution des équations algébriques) une telle correspondance entre certains ensembles A (qui sont des corps) et certains groupes H (d'automorphismes) : de là vient le nom attribué à ces correspondances.

La notion générale de correspondance de Galois a été dégagée par O. ORE, *Galois Connexions* (Trans. Amer. Math. Soc., t. 55, 1944, p. 493); G. BIRKHOFF avait étudié (*Lattice Theory*, 1^{re} éd., 1940, § 32) de telles correspondances définies à partir de relations linéaires (voir l'exercice 2 ci-dessous); M. KRASNER en avait également rencontré dans une généralisation abstraite de la théorie de Galois : *Une généralisation de la notion de Corps* (J. Math. pures et appl., t. 17, 1938, p. 266). Le cas qui nous a servi de point de départ a été signalé par J. RIGUET, C. R. Acad. Sc., t. 229, 1949, p. 409. On pourra consulter, d'une façon générale, G. BIRKHOFF, *Lattice Theory*, 2^e éd., chap. IV, § 5 et 6, où l'on trouvera d'autres références.

que chaque élément A de $\mathcal{X}$ a même image dans $\mathcal{S}$ que sa fermeture $\bar{A}$.

On a, de même, $\varphi f \varphi H = \varphi H$ et l'application $H \rightarrow f \varphi H = \bar{H}$ est une fermeture dans $\mathcal{S}$.

D'après (3), toute image fA est un élément fermé dans $\mathcal{S}$: $fA = \bar{H}$; réciproquement, tout élément fermé de $\mathcal{S}$, $\bar{H} = f \varphi H$, est évidemment une image.

La relation (4), écrite

$$(4') \quad \varphi f \bar{A} = \bar{A}$$

et la relation analogue

$$(4'') \quad f \varphi \bar{H} = \bar{H}$$

montrent que les éléments fermés se correspondent biunivoquement et que les applications f et φ , restreintes aux ensembles d'éléments fermés, sont inverses l'une de l'autre.

Il est intéressant d'interpréter ces résultats en introduisant l'application multiforme θ définie de la façon suivante : θA ($A \in \mathcal{X}$) est l'ensemble des éléments H de $\mathcal{S}$ qui ont $\bar{A}$ pour image dans $\mathcal{X}$, c'est-à-dire vérifient

$$\varphi H = \bar{A} = \varphi f A,$$

ce qui entraîne

$$f \varphi H = f \varphi f A = f A = \bar{H};$$

on voit donc, en tenant compte de la symétrie évidente, que les relations

$$\varphi H = \bar{A} = \varphi f A, \quad f A = \bar{H} = f \varphi H$$

ont lieu en même temps : la première définit la fonction θ , la deuxième définit la fonction inverse θ^{-1} . Nous avons

$$\theta = \varphi^{-1} \varphi f, \quad \theta^{-1} = f^{-1} f \varphi.$$

L'application θ est semi-uniforme : $H \in \theta A \cap \theta B$ entraîne, en effet,

$$\varphi H = \bar{A} = \bar{B}, \quad \text{donc} \quad \theta A = \theta B.$$

La relation $\mathcal{C}$ définie par $\theta A \times \theta B$ coïncide avec sa fermeture transitive, c'est-à-dire avec l'équivalence $\mathcal{C}$ décomposant $\mathcal{X}$ en ensembles stables minimaux (chap. I, § 8 et 12); un tel ensemble est une image $\theta^{-1}H$, donc se compose de tous les éléments A de $\mathcal{X}$ ayant une fermeture donnée $\bar{A}$, et la correspondance biunivoque

$$\mathcal{X}/\mathcal{C} \leftarrow \rightarrow \mathcal{S}/\mathcal{C}'$$

exprime, ici, la même propriété que la correspondance biunivoque

$$\{\bar{A}\} \leftarrow \rightarrow \{\bar{H}\}$$

entre les ensemble d'éléments fermés.

Les correspondances de Galois sont d'autant plus importantes qu'on les rencontre encore sous une autre forme. Entre deux ensembles partiellement ordonnés, E (par $\subseteq$), E' (par $\preceq$), considérons une correspondance définie par deux applications uniformes, f de E dans E', φ de E' dans E :

$$x \rightarrow fx, \quad x' \rightarrow \varphi x'$$

et possédant les propriétés suivantes :

$$1 \text{ a. } x \subseteq x_1 \text{ entraîne } fx \preceq fx_1;$$

$$1' \text{ a. } x' \preceq x'_1 \text{ entraîne } \varphi x' \subseteq \varphi x'_1$$

(f et φ sont *isotones*);

$$2 \text{ a. } x \subseteq \varphi fx;$$

$$2' \text{ a. } x' \preceq f\varphi x'.$$

Il suffit de remplacer l'ordre $\preceq$ de E' (par exemple), par l'ordre inverse, noté $\supseteq$, pour retrouver les conditions définissant une correspondance de Galois : une correspondance possédant les propriétés 1 a, 1' a, 2 a, 2' a sera désignée sous le nom de *correspondance de Galois inversée*⁽¹⁾. Les relations

$$(3 \text{ a}) \quad f\varphi fx = fx,$$

$$(4 \text{ a}) \quad \varphi f\varphi fx = \varphi fx$$

subsistent; l'application

$$x \rightarrow \varphi fx = \bar{x}$$

est une fermeture dans E, tandis que l'application

$$x' \rightarrow f\varphi x' = \bar{x'},$$

dans E', est une *fermeture inversée* (on dit aussi *ouverture*) : les deux propriétés

$$x' \preceq y' \quad \text{entraîne} \quad \bar{x'} \preceq \bar{y'},$$

$$\bar{\bar{x'}} = \bar{x'}$$

⁽¹⁾ Voir O. ORE, *loc. cit.*, § 3.

La correspondance de Grell entre les idéaux d'un anneau et ceux d'un sous-anneau est une correspondance de ce type (voir chap. IV, § 11, p. 193).

subsistent, mais on a

$$x' \supseteq \bar{x'}.$$

Pour simplifier, appelons encore éléments *fermés* les éléments $\bar{x'}$ de E' ; la correspondance biunivoque entre éléments fermés

$$fx = \bar{x'}, \quad \varphi \bar{x'} = x,$$

est ici isotone.

Un cas important est celui où l'ensemble T des éléments fermés de E , ordonné par $\subseteq$, et l'ensemble T' des éléments fermés de E' , ordonné par $\subseteq$, sont des treillis complets. Utilisons le lemme suivant ⁽¹⁾.

LEMME. — *Toute application biunivoque f d'un treillis complet T sur un treillis complet T' , qui est isotone ainsi que son inverse f^{-1} , est un isomorphisme généralisé ⁽²⁾ pour les opérations $\cap$ et $\cup$, et réciproquement.*

1° Considérons une partie non vide (finie ou infinie), X , de T , et son image $X' = fX$ dans T' , et montrons que $i = \bigcap_{x \in X} x$ a pour image $j' = \bigcap_{x' \in X'} x' (x' = fx)$. La relation $i \subseteq x$ pour tout $x \in X$ entraîne $fi = i' \subseteq x'$ pour tout $x' \in X'$, donc $i' \subseteq j'$. De même, $j' \subseteq x'$ entraîne $j = f^{-1}j' \subseteq x$ pour $x \in X$, d'où $j \subseteq i$ et, par conséquent, $j' \subseteq i'$, donc enfin $j' = i' = fi$. Un raisonnement analogue montre que $\bigcup_{x \in X} x$ a pour image $\bigcup_{x' \in X'} x'$.

2° Inversement, si f est un isomorphisme pour $\cup$ (par exemple), la relation $x \subseteq y$, qui équivaut à $x \cup y = y$, entraîne $x' \cup y' = y'$, donc $x' \subseteq y'$: f est isotone. Il en est de même de f^{-1} .

En utilisant ce lemme et le théorème de Moore (chap. I, § 11, p. 53), d'après lequel T et T' sont des treillis complets dès que E , E' sont eux-mêmes des treillis complets ⁽³⁾, nous obtenons le résultat suivant.

(1) Ce lemme est une variante, concernant les treillis complets, d'une proposition analogue valable pour les treillis ou demi-treillis. Cf. M. L. DUBREIL-JACOIN, L. LESIEUR, R. CROISOT, *Leçons sur la Théorie des treillis...*, 1^{re} partie, chap. IV, § 3, prop. 4, p. 49.

(2) C'est-à-dire valable aussi pour l'intersection et l'union d'un ensemble infini d'éléments : l'image d'une intersection quelconque est l'intersection des images; de même pour l'union. L'étude systématique des isomorphismes sera faite au § 7.

(3) Le théorème de Moore reste évidemment valable dans E' pour la fermeture inversée que nous considérons ici.

THEOREME. — *S'il existe une correspondance de Galois inversée*

$$x \rightarrow fx, \quad x' \rightarrow \varphi x'$$

entre deux treillis complets E, E', les éléments fermés de E et de E' constituent des treillis complets T, T'; f est non seulement une application biunivoque isotone de T sur T', ayant φ pour inverse, mais un isomorphisme pour les opérations $\cap$ et $\cup$.

Exercices. — 1. Considérons l'ensemble E des points de l'espace euclidien. Appelons *renversement* d'axe D et désignons par (D) la transformation qui consiste à effectuer une symétrie par rapport à la droite D. On sait que le groupe engendré par les renversements est le *groupe des déplacements* G (ceci peut d'ailleurs être pris comme définition de ce groupe).

1° Le produit σ de deux renversements (D_1) , (D_2) est l'identité si D_1 et D_2 sont confondues, une rotation si D_1 et D_2 sont concourantes, une translation si D_1 et D_2 sont parallèles, un déplacement hélicoïdal proprement dit si D_1 et D_2 ne sont pas coplanaires. Dans le premier cas, tout point est invariant, dans le second, tout point de l'axe de rotation est invariant, dans le troisième et le quatrième, il n'y a pas de points invariants.

2° Tout déplacement est le produit de deux renversements convenablement choisis.

3° L'ensemble des déplacements qui laissent invariant un point O est un groupe, dont les éléments sont les rotations autour d'axes passant par O.

4° Quel est le groupe des déplacements qui laissent une droite Δ donnée invariante? Par quel ensemble de renversements peut-on l'engendrer?

2. On considère deux ensembles E, E' (pouvant coïncider) et une relation binaire $\mathcal{R}$ portant sur les éléments x de E et les éléments x' de E'. A chaque partie X de E, on associe dans E' la partie $f(X) = \mathcal{R}[X]$, coupe de seconde espèce, c'est-à-dire ensemble des éléments x' de E' vérifiant $x\mathcal{R}x'$ pour tout $x \in X$. A chaque partie X' de E' on associe de même, dans E, la partie $\varphi(X') = \mathcal{R}^{-1}[X']$, ensemble des x vérifiant $x\mathcal{R}x'$ pour tout $x' \in X'$.

Montrer que la double correspondance

$$X \rightarrow f(X), \quad X' \rightarrow \varphi(X')$$

est une correspondance de Galois.

Considérons maintenant une équivalence $\mathcal{R}$ définie dans l'ensemble E. Une transformation σ de E *respecte* $\mathcal{R}$ si l'on a

$$(5) \quad \sigma x \equiv x \quad (\mathcal{R}) \quad \text{pour tout } x \in E.$$

S'il en est ainsi, on a en particulier pour tout $x \in E$

$$\sigma(\sigma^{-1}x) \equiv \sigma^{-1}x \quad (\mathcal{R}).$$

d'où

$$(5') \quad \sigma^{-1}x \equiv x \quad (\mathcal{R}) \quad \text{pour tout } x \in E.$$

Par suite, quand une transformation σ respecte $\mathcal{R}$, il en est de même de son inverse σ^{-1} . Comme, d'autre part, le produit $\tau\sigma$ respecte $\mathcal{R}$ dès que σ et τ ont cette propriété, l'ensemble de toutes les transformations qui respectent une équivalence donnée $\mathcal{R}$ est un groupe $\Gamma_{\mathcal{R}}$ ⁽¹⁾.

On a visiblement

$$\Gamma_{\mathcal{R}} \subseteq \Gamma_{\mathcal{R}'} \quad \text{dès que} \quad \mathcal{R} \subseteq \mathcal{R}',$$

car une transformation respectant $\mathcal{R}$ respecte toute équivalence contenant $\mathcal{R}$. Inversement,

$$\Gamma_{\mathcal{R}} \subseteq \Gamma_{\mathcal{R}'} \quad \text{entraîne} \quad \mathcal{R} \subseteq \mathcal{R}'.$$

Soit, en effet, $y \equiv x(\mathcal{R})$; considérons la transformation σ qui laisse invariant tout élément de E autre que x ou y , mais échange x avec y . Cette transformation respectant $\mathcal{R}$, appartient à $\Gamma_{\mathcal{R}}$, donc à $\Gamma_{\mathcal{R}'}$, d'où

$$y = \sigma x \equiv x(\mathcal{R}'),$$

et, par conséquent, $\mathcal{R} \subseteq \mathcal{R}'$.

Il y a donc *correspondance biunivoque* entre l'ensemble des équivalences $\mathcal{R}$ et l'ensemble Σ des groupes de transformation $\Gamma_{\mathcal{R}}$ qui viennent d'être définis ⁽²⁾. Le groupe Γ de toutes les transformations de E correspond à l'équivalence absolue : $\Gamma \in \Sigma$.

Nous avons d'autre part, d'après (5),

$$\Gamma_{\mathcal{R} \cap \mathcal{S}} = \Gamma_{\mathcal{R}} \cap \Gamma_{\mathcal{S}},$$

et d'une manière générale, si $\mathcal{M}$ est un ensemble d'équivalences définies dans E

$$(6) \quad \Gamma_{\bigcap \mathcal{M}} = \bigcap_{\mathcal{R} \in \mathcal{M}} \Gamma_{\mathcal{R}}.$$

L'ensemble Σ des groupes $\Gamma_{\mathcal{R}}$ contient donc, en même temps que plusieurs groupes, leur intersection.

(1) Un exemple de groupe défini par ce procédé peut être emprunté à la Physique théorique. Des corpuscules de même espèce sont indiscernables; en les regardant comme équivalents, on introduit, dans un système de corpuscules donné, une équivalence $\mathcal{R}$: le groupe $\Gamma_{\mathcal{R}}$ correspondant est le *groupe d'indiscernabilité*. Cf. J.-L. DES-TOUCHES, *Corpuscules et systèmes de corpuscules*, p. 33, Paris, Gauthier-Villars, 1941.

(2) Cette correspondance biunivoque a été introduite pour la première fois par G. BIRKHOFF, *On the Structure of abstract Algebra* (*Proc. Cambridge Phil. Soc.*, t. 31, 1935, p. 433-454). Voir aussi P. DUBREIL et M.-L. DUBREIL-JACOTIN, *Théorie algébrique des relations d'équivalence* [*J. Math. pures et appl.*, t. 18, 1939, p. 63; en particulier la note (2) de la page 64].

Il en résulte que le groupe $\Gamma_{\mathcal{R}}$ correspondant au produit transitif

$$\mathcal{R} = \prod_{\mathcal{R} \in \mathcal{M}}' \mathcal{R}$$

des équivalences d'un ensemble $\mathcal{M}$ coïncide avec le groupe composé dans Σ , L_{Σ} , des groupes $\Gamma_{\mathcal{R}} (\mathcal{R} \in \mathcal{M})$ correspondant à ces équivalences.

En effet, L_{Σ} est l'intersection des groupes $\Gamma_{\mathcal{R}} \in \Sigma$ contenant tous les groupes $\Gamma_{\mathcal{R}} (\mathcal{R} \in \mathcal{M})$: c'est donc, d'après (6), le groupe $\Gamma_{\mathcal{Z}}$ correspondant à l'équivalence $\mathcal{Z}$ intersection des équivalences $\mathcal{R}$ contenant toutes les équivalences $\mathcal{R} \in \mathcal{M}$. Or on a $\mathcal{Z} = \mathcal{R}$, d'après la définition même du produit des équivalences.

Un groupe H , plus généralement un ensemble $\mathcal{H}$ de transformations de E , respectent une équivalence $\mathcal{R}$ définie dans E , si chaque transformation du groupe H ou de l'ensemble $\mathcal{H}$ respecte $\mathcal{R}$, donc si l'on a

$$H \subseteq \Gamma_{\mathcal{R}}, \quad \mathcal{H} \subseteq \Gamma_{\mathcal{R}}.$$

L'ensemble des transformations d'un groupe donné G qui respectent $\mathcal{R}$, est le sous-groupe $G_{\mathcal{R}} = G \cap \Gamma_{\mathcal{R}}$.

Notons encore la proposition suivante. *Pour qu'une transformation σ respecte une équivalence $\mathcal{R}$, il faut et il suffit que σ laisse invariante chaque classe modulo $\mathcal{R}$.*

La condition est évidemment suffisante. Elle est également nécessaire. Si, en effet, σ respecte $\mathcal{R}$ et si A désigne une classe modulo $\mathcal{R}$, la relation (5) entraîne $\sigma A \subseteq A$, (5') entraîne $\sigma^{-1} A \subseteq A$ donc $A \subseteq \sigma A$ (1) et, par conséquent, $\sigma A = A$.

Exemple. — Regardons comme équivalents deux points de l'espace s'ils sont à la même distance d'un point donné O . Toute rotation autour d'un axe passant par O respecte l'équivalence $\mathcal{R}$ ainsi définie. Les classes modulo $\mathcal{R}$, qui sont les surfaces des sphères de centre O et le point O lui-même, sont bien des sous-ensembles invariants.

Exercice. — 3. Deux points de l'espace sont regardés comme équivalents s'ils sont à la même distance d'un plan donné P . Quels sont les déplacements qui respectent l'équivalence ainsi définie? Indiquer une génération de leur groupe.

(1) On peut aussi présenter le raisonnement de la manière suivante. Si $x \in A$, $y = \sigma^{-1} x$ est, d'après (5'), équivalent à x , donc $y \in A$. Par suite, $x = \sigma y \in \sigma A$, et nous avons bien

$$A \subseteq \sigma A.$$

Donnons-nous maintenant un groupe G de transformations de l'ensemble E . La relation $\mathfrak{G}$ définie dans cet ensemble par

$$a \mathfrak{G} b$$

s'il existe une transformation $\sigma \in G$ telle que l'on ait

$$b = \sigma a,$$

est une *équivalence*. Elle est en effet *réflexive*, puisque G contient la transformation identique, *symétrique* puisque G contient en même temps qu'une transformation σ son inverse σ^{-1} , et *transitive* puisque les égalités $b = \sigma a$, $c = \tau b$ entraînent $c = \tau \sigma a$, où le produit $\tau \sigma$ appartient à G en même temps que σ et τ .

On donne à l'équivalence $\mathfrak{G}$ le nom d'*équivalence de transitivité* du groupe G . Cette notion conduit à l'importante définition suivante :

Définition. — Si l'équivalence de transitivité $\mathfrak{G}$ du groupe G est l'équivalence absolue, G est dit *transitif*. Si $\mathfrak{G}$ est distincte de l'équivalence absolue, G est dit *intransitif*. L'ensemble E est alors décomposé effectivement en plusieurs classes modulo $\mathfrak{G}$, qui sont appelées *classes de transitivité* (ou encore domaines, systèmes de transitivité).

Si le groupe G est *transitif*, il existe, pour tout couple d'éléments x et y de E au moins une transformation σ de G telle que l'on ait $y = \sigma x$. Mais inversement, pour que G soit transitif, il *suffit* qu'étant donné un élément fixe a de E , il existe, pour tout $x \in E$, au moins une transformation ξ de G transformant a en x . Les relations

$$x = \xi a, \quad y = \eta a \quad (\xi, \eta \in G)$$

entraînent, en effet,

$$y = \eta \xi^{-1} x, \quad \text{où } \eta \xi^{-1} \in G,$$

donc

$$x \equiv y(\mathfrak{G}), \quad \text{quels que soient } x, y \in E.$$

Si G' est un sous-groupe de G , l'équivalence de transitivité $\mathfrak{G}'$ de G' est contenue dans l'équivalence de transitivité $\mathfrak{G}$ de G . Donc la transitivité de G' entraîne celle de G , l'intransitivité de G entraîne celle de G' .

Exemples. — 1. Dans l'ensemble E des points de l'espace, le groupe des translations est transitif. Celui des déplacements l'est *a fortiori*. Le groupe des translations parallèles à un plan donné P est intransitif; les classes de transitivité sont les plans parallèles à P .

2. Le groupe des rotations autour d'un point O est intransitif; les classes de transitivité sont les sphères de centre O et le point O .

Exercices. — 4. Le groupe de Klein V_4 (cf. § 2, exemple, p. 107) est-il transitif?

5. Les déplacements parallèles à un plan donné P , c'est-à-dire transformant tout point M en un point M' tel que $\overrightarrow{MM'}$ soit nul ou parallèle à P , forment un groupe G intransitif. Quelles sont les classes de transitivité?

Soit G un groupe *intransitif*. Chaque classe de transitivité A est invariante par G , tandis qu'aucun sous-ensemble véritable de A n'est invariant. Par suite, pour que G laisse invariant un ensemble M , il faut et il suffit que M soit une *réunion de classes de transitivité* par rapport à ce groupe. En particulier, pour qu'un élément a soit invariant par G , il faut et il suffit qu'il constitue à lui seul une classe de transitivité.

Tout groupe de transformations G , opérant dans un ensemble E , respecte sa propre équivalence de transitivité $\mathfrak{G}$. Si, en effet, $\sigma \in G$, on a, d'après la définition même de $\mathfrak{G}$.

$$x \equiv \sigma x(\mathfrak{G}) \quad \text{pour tout } x \in E.$$

De ce qui précède résulte qu'un groupe G respecte toute équivalence contenant son équivalence de transitivité. Inversement, si G respecte une équivalence $\mathcal{R}$, on a $\mathfrak{G} \subseteq \mathcal{R}$. Soit, en effet,

$$x \equiv y(\mathfrak{G}), \quad \text{donc} \quad y = \sigma x, \quad \text{avec } \sigma \in G.$$

Appartenant à G , la transformation σ respecte $\mathcal{R}$, c'est-à-dire

$$\sigma x \equiv x(\mathcal{R}), \quad \text{donc} \quad y \equiv x(\mathcal{R})$$

et, par suite,

$$\mathfrak{G} \subseteq \mathcal{R}.$$

Les équivalences respectées par un groupe donné G sont donc celles qui contiennent l'équivalence de transitivité de ce groupe.

Exercice 6. — On donne dans un ensemble E une équivalence $\mathcal{R}$ et l'on considère le groupe $\Gamma_{\mathcal{R}}$ de toutes les transformations respectant $\mathcal{R}$. Quelle est l'équivalence de transitivité de $\Gamma_{\mathcal{R}}$?

C. — ISOMORPHISME.

7. Notion d'isomorphisme. — Soient

$$E = \{a, b, \dots\} \quad \text{et} \quad E' = \{a', b', \dots\}$$

deux groupoïdes dont les éléments se correspondent *biunivoquement* dans une application σ de E sur E' :

$$(1) \quad a \longleftrightarrow a' = \sigma a.$$

Désignons par O l'opération de E , par O' celle de E' . Si toute relation de la forme

$$(2) \quad aOb = c$$

entre éléments de E entraîne, pour les éléments-images a' , b' , c' dans E' , la relation

$$(2') \quad a'O'b' = c' \quad \text{ou} \quad \sigma(aOb) = (\sigma a)O'(\sigma b),$$

l'application biunivoque σ est dite *régulière* pour les opérations O et O' ; on lui donne le nom d'*isomorphisme de groupoïdes*; on dit que E et E' sont des *groupoïdes isomorphes* et l'on écrit

$$E \overset{O}{\leftarrow} \overset{O'}{\rightarrow} E' \quad \text{ou, plus simplement,} \quad E \leftarrow \rightarrow E',$$

ou encore

$$E \cong E', \quad E \simeq E'.$$

Plus généralement, deux ensembles

$$S = \{a, b, \dots\} \quad \text{et} \quad S' = \{a', b', \dots\},$$

dans lesquels sont définies, en même nombre, des opérations $O_1, O_2, \dots, O'_1, O'_2, \dots$, sont des *domaines isomorphes* s'il existe entre eux une correspondance biunivoque σ

$$(1) \quad a \leftarrow \rightarrow a' = \sigma a$$

régulière pour les opérations O_i et O'_i , pour les différentes valeurs de l'indice i .

On donne le nom d'*automorphisme* à tout isomorphisme d'un groupoïde ou d'un domaine avec lui-même.

On représente souvent par le même signe les opérations correspondantes O_i, O'_i , de deux groupoïdes ou domaines isomorphes. Si, par exemple, deux opérations correspondantes sont des multiplications, la condition pour que la correspondance biunivoque σ soit régulière pour ces multiplications s'écrit

$$(ab)' = a'b' \quad \text{ou} \quad \sigma(ab) = \sigma a \cdot \sigma b.$$

L'isomorphisme des groupoïdes est une propriété *transitive*. C'est aussi une propriété *symétrique*. Posons, en effet, $a'O'b' = c'$ et soient a, b, c les images de a', b', c' dans le groupoïde E . En posant $aOb = d$, nous avons

$$d' = a'O'b' = c',$$

d'où, puisque (1) est une application *biunivoque*, $d = c$, c'est-à-dire $aOb = c$.

Si deux groupoïdes ou domaines S, S' sont isomorphes, toute relation entre éléments de S faisant intervenir, avec le signe $=$, les signes des opérations considérées, entraîne, pour les éléments-images dans S' , la relation analogue, où les opérations de S sont remplacées par les opérations correspondantes de S' , et inversement. Par suite, toute propriété (propriété de fermeture, règle de calcul, ou propriété d'inversion) d'une ou de plusieurs opérations de S appartient également à l'opération ou aux opérations correspondantes de S' : deux groupoïdes ou domaines isomorphes ont donc des propriétés algébriques identiques.

En particulier, si S est un groupe par rapport à O , S' en est un par rapport à O' . Si $e' = \sigma e$ désigne l'image de l'élément-unité e de S , nous avons, pour tout $x' \in E'$, en posant $x = \sigma^{-1}x'$ et en adoptant pour O et O' la notation multiplicative,

$$e'x' = \sigma e \cdot \sigma x = \sigma(ex) = \sigma x = x';$$

e' est donc élément-unité à gauche (par exemple) dans E' . D'autre part, x' admet l'élément $\sigma(x^{-})$ comme inverse à gauche (par exemple), puisqu'on a

$$\sigma(x^{-}) \cdot x' = \sigma(x^{-}) \cdot \sigma(x) = \sigma(x^{-}x) = \sigma e = e'.$$

Exemples. — 1. Soient P et P' deux plans non perpendiculaires. A tout vecteur libre $\vec{V}$ de P , associons sa projection orthogonale $\vec{V}'$ sur P' . Soient G et G' les groupes constitués par les vecteurs $\vec{V}$ et par les vecteurs $\vec{V}'$ par rapport à l'addition géométrique; on a

$$G \simeq G'.$$

2. La symétrie par rapport à un plan est un automorphisme pour le groupe additif des vecteurs libres de l'espace.

3. Deux groupes cycliques infinis G et G' , engendrés respectivement par les éléments a et a' , sont isomorphes, la correspondance entre leurs éléments étant définie par les relations

$$\begin{aligned} a &\leftrightarrow a', & a^{-} &\leftrightarrow (a')^{-}; \\ a^m &\leftrightarrow (a')^m, & (a^{-})^m &\leftrightarrow [(a')^{-}]^m, \end{aligned}$$

où m désigne un entier naturel arbitraire. Si les groupes sont écrits sous la forme additive, ces dernières relations doivent être remplacées par

$$ma \leftrightarrow ma', \quad m(-a) \leftrightarrow m(-a').$$

4. Un autre exemple de groupes isomorphes est fourni par le groupe des rotations du plan qui laissent invariant un polygone régulier de n côtés, et le groupe des permutations circulaires de n lettres. Du point de vue algébrique, ces deux groupes constituent un seul et même groupe, le groupe cyclique d'ordre n ⁽¹⁾.

(1) « Ce qui est fécond », écrit Jacques Hadamard (*Encyclopédie française, Mathé-*

5. Deux treillis T, T' sont isomorphes si l'on a entre leurs éléments une correspondance biunivoque

$$x \longleftrightarrow x'$$

respectant l'intersection et l'union :

$$(x \cap y)' = x' \cap y', \quad (x \cup y)' = x' \cup y'.$$

Par exemple, le treillis des relations binaires définies sur deux ensembles E, F et celui des parties de l'ensemble produit $E \times F$ sont isomorphes (on rencontrera un autre exemple important de treillis isomorphes au chapitre IV, § 3, p. 153).

Étant donné un groupoïde ou un groupe *abstrait* G , par exemple un groupe défini formellement par des générateurs et un système de relations fondamentales, il peut être utile de définir un groupoïde ou un groupe G' *isomorphe* à G et dont les éléments sont d'une nature déterminée. On dit alors que G' est une *réalisation* ou une *représentation isomorphe* de G . Dans cet ordre d'idées, nous établirons la proposition suivante.

THÉOREME. — *Tout groupe G admet comme réalisation un groupe de transformations* ⁽¹⁾,

Désignons par $E = \{e, a, b, \dots\}$ l'ensemble des éléments de G . A tout élément a de G , nous faisons correspondre l'application α de E en lui-même définie par

$$x \rightarrow ax, \quad \text{c'est-à-dire} \quad \alpha(x) = ax.$$

Quel que soit $a \in G$, α est bien une application *biunivoque* de E sur lui-même, c'est-à-dire une *transformation* de E , car pour tout $y \in G$, il existe un x et un seul tel que l'on ait

$$a.x = y.$$

De plus, le produit $\beta\alpha$ des transformations correspondant à a et b , est la transformation correspondant au produit ba , puisqu'on a

$$\beta\alpha(x) = \beta(\alpha(x)) = \beta(ax) = b.ax = ba.x.$$

matique, 1-58-1). « c'est le rapprochement ainsi établi entre les propriétés d'être aussi divers ... qu'une figure géométrique et l'ordre dans lequel on range n lettres données. L'abstraction mathématique fait ainsi un pas nouveau et immense dont on ne soupçonnait pas, jusque-là, la possibilité et qui a donné à la Science mathématique une puissance toute nouvelle ».

(¹) Dans le cas où G est fini et où, par conséquent, la réalisation est un groupe de substitutions, ce théorème important a été établi par Cayley [*Phil. Mag.*, (4), t. 7, 1854, p. 40].

L'ensemble de ces transformations est, par suite, un groupoïde isomorphe au groupe G , donc un *groupe* isomorphe à G , c'est-à-dire une réalisation de G .

Exercices. — 1. Désignons par E l'ensemble des nombres naturels, par E' celui des nombres pairs. La correspondance biunivoque

$$x \rightarrow 2x \quad (x \in E)$$

est-elle un isomorphisme entre E et E' considérés comme groupoïdes par rapport à l'addition? En est-elle un lorsqu'on regarde E et E' comme groupoïdes par rapport à la multiplication?

2. On considère le groupe G dont l'élément-unité est e et qui est engendré par deux éléments a et b vérifiant les relations fondamentales

$$a^3 = e, \quad b^2 = e, \quad aba = b$$

(cf. § 4, ex. 3, p. 113). Indiquer une réalisation de G par un groupe de substitutions.

8. Application à la définition des groupes. Extensions. — L'existence d'une correspondance biunivoque

$$a \leftarrow \rightarrow a'$$

entre un *groupoïde*, ou plus généralement un *domaine* $S = \{a, b, \dots\}$ où sont définies des opérations $O_1, O_2, \dots$ et un simple *ensemble* $E' = \{a', b', \dots\}$, permet de définir dans E' des opérations O'_i en posant

$$a' O'_i b' = (a O_i b)'.$$

On fait ainsi de E' un groupoïde ou un domaine S' *isomorphe* à S . On dit que les opérations O'_i sont définies *par isomorphisme* à partir des opérations O_i .

Exemple. — L'addition géométrique des vecteurs libres se définit très simplement par l'addition numérique des composantes; mais on en donne souvent aussi une définition qui repose sur le principe précédent. La somme géométrique de deux segments OA, OB de même origine O est par définition le segment OS , diagonale du parallélogramme construit sur OA et OB ; les segments issus de O forment un groupe par rapport à cette opération. Comme les vecteurs libres sont représentés biunivoquement par les segments d'origine O , leur addition peut être définie par isomorphisme à partir de celle des segments, et les vecteurs libres forment eux aussi un groupe par rapport à cette opération.

La définition de groupoïdes, et en particulier de groupes, par isomorphisme, intervient dans la résolution de problèmes que nous rencon-

trons sous des formes variées, et qui consistent à construire une *extension* d'un domaine donné A . Si nous désignons par $O_1, O_2, \dots$ les opérations de A , une extension A^* est, par définition, un domaine contenant A , où sont définies des opérations $O_1^*, O_2^*, \dots$ correspondant aux O_i et telles que l'on ait

$$a O_i^* a' = a O_i a', \quad \text{dès que } a, a' \in A$$

(*principe de concordance*). On impose souvent à l'extension A^* des propriétés algébriques remarquables qui n'appartenaient pas à A , par exemple celle d'être un groupe par rapport à l'une ou l'autre des opérations O_i^* : la construction de l'extension A^* est alors ce qu'on appelle un *problème d'immersion*.

En fait, le plus souvent, les procédés de construction dont on dispose ne fournissent pas directement l'extension A^* , mais un domaine B^* qui, s'il possède par rapport aux opérations O_i^* qui y sont définies les propriétés imposées, contient, au lieu de A , un domaine B *isomorphe* à A :

$$(\sigma) \quad \begin{matrix} O_i O_i^* \\ A \leftarrow \rightarrow B. \end{matrix}$$

On lève ordinairement cette difficulté en disant qu'il suffit d'*identifier* les éléments de A et ceux de B ⁽¹⁾. Il convient de préciser ce qu'il faut entendre par là. En réalité, deux cas sont à distinguer.

1° *Le domaine A n'est défini qu'à un isomorphisme près*. On peut alors, sans rien changer, le remplacer par B , c'est-à-dire faire intervenir B partout où intervenait A : B^* est l'extension cherchée.

2° *La définition de A est telle qu'on ne peut pas le remplacer par un domaine isomorphe*. Alors, pour obtenir l'extension cherchée A^* , remplaçons dans B^* les éléments de B par ceux de A , c'est-à-dire posons ⁽²⁾

$$A^* = A \cup (B^* - B).$$

Cela fait, établissons entre A^* et B^* une correspondance biunivoque

$$(\sigma^*) \quad x \leftarrow \rightarrow y = \sigma^* x \quad (x \in A^*, y \in B^*)$$

⁽¹⁾ Par exemple, dans la définition des nombres complexes, on « identifie » à un certain moment, les nombres complexes dans lesquels le coefficient de i est nul avec les nombres réels.

⁽²⁾ Le signe $\cup$ est pris ici dans un sens un peu élargi, car A et $B^* - B$ ne sont pas nécessairement parties d'un même ensemble : ce signe exprime que, par définition, les éléments de A^* sont d'une part les éléments de A , d'autre part ceux de $B^* - B$. Cette définition de A^* est d'un emploi très général [voir, par exemple, S. LEFSCHETZ, *Algebraic Topology*, chap. I (2-7). p. 3]; il s'agit d'ailleurs de la réunion générale de deux ensembles (chap. I, § 1).

en posant, σ désignant toujours l'isomorphisme $A \simeq B$,

$$(3) \quad \begin{cases} \sigma^* x = x & \text{si } x \in B^* - B, \\ \sigma^* x = \sigma x & \text{si } x \in A. \end{cases}$$

Enfin, définissons l'opération O_i^* dans A^* par isomorphisme, à partir de Ω_i^* , au moyen de la correspondance (σ^*) , ce qui fait de A^* un domaine isomorphe à B^* : A^* possède bien les propriétés algébriques voulues, il contient A comme partie et enfin *le principe de concordance est respecté* puisqu'il l'est dans le passage de B à B^* et que A est isomorphe à B , A^* à B^* ; ou encore, en désignant par a et a' deux éléments quelconques de A , nous avons, d'après (3) et puisque σ et σ^* sont des isomorphismes

$$\sigma(a O_i a') = (\sigma a) \Omega_i^* (\sigma a') = (\sigma^* a) \Omega_i^* (\sigma^* a') = \sigma^*(a O_i^* a') \in B,$$

d'où puisque $\sigma(a O_i a') = \sigma^*(a O_i a')$

$$a O_i a' = a O_i^* a'.$$

A^* est donc bien une extension de A .

Deux extensions E, E' d'un domaine A sont dites *isomorphes sur A* ou *équivalentes par rapport à A* s'il existe entre elles un isomorphisme σ dans lequel tout élément de A se correspond à lui-même

$$\sigma x = x \quad \text{pour tout } x \in A.$$

On écrit

$$E \underset{(A)}{\simeq} E'$$

et σ est appelé *isomorphisme relatif par rapport à A* .

Plus généralement, soient A et A' deux domaines isomorphes dans un isomorphe σ_0 . Un isomorphisme σ entre une extension E de A et une extension E' de A' est appelé *prolongement* de σ_0 si l'on a

$$\sigma x = \sigma_0 x \quad \text{pour tout } x \in A.$$

Lorsque $A' = A$ et que σ_0 est l'identité, on retrouve la notion d'isomorphisme relatif.

9. Entiers relatifs. — Le domaine N_0 des nombres naturels (zéro inclus) est un semi-groupe abélien par rapport à l'addition et un demi-groupe abélien par rapport à la multiplication. L'ensemble des entiers relatifs (c'est-à-dire positifs, négatifs ou nuls) est une *extension* C de N_0 formant un *groupe par rapport à l'addition*. L'intérêt pratique d'une telle extension est évident pour la mesure des grandeurs orientées. Son

intérêt théorique n'est pas moindre. La construction du groupe additif C des entiers relatifs repose sur les notions fondamentales d'isomorphisme et de groupe cyclique infini ⁽¹⁾. D'autre part, la définition de la multiplication dans C en fait un domaine d'un type remarquable : la définition des entiers relatifs conduit à la notion d'*anneau*, fondamentale en Algèbre.

Le semi-groupe additif des entiers naturels est isomorphe au *groupe* G_1 engendré par l'élément générateur a d'un *groupe additif cyclique et infini* ⁽²⁾ G . Or G comprend, outre G_1 , l'élément neutre e et le groupe G_2 engendré par l'élément opposé $-a$. Considérons alors un ensemble C , réunion générale de deux ensembles dénombrables disjoints, que nous désignons par

$$D_+ = \{ +1, +2, \dots, +m, \dots \}, \quad D_- = \{ -1, -2, \dots, -m, \dots \}$$

et de l'élément *zéro* qui n'appartient ni à D_+ , ni à D_- : on donne aux éléments de C le nom d'*entiers relatifs* ou *rationnels*, ceux de D_+ étant les *entiers positifs*, ceux de D_- les *entiers négatifs*. Un entier relatif μ *différent de zéro* est donc, formellement, un entier naturel m affecté du signe $+$ ou du signe $-$; l'entier naturel m est la *valeur absolue* du nombre relatif μ : on écrit $m = |\mu|$. Deux nombres relatifs ne sont égaux que s'ils ont même valeur absolue et, s'ils sont différents de zéro, même signe ⁽³⁾.

D'après la construction de l'ensemble C , il est clair qu'on a, entre C et G , la correspondance biunivoque

$$(1) \quad \begin{cases} ma \leftrightarrow +m, \\ e \leftrightarrow 0, \\ m(-a) \leftrightarrow -m. \end{cases}$$

Convenons de poser

$$(2) \quad \begin{cases} ma = (+m).a, \\ e = 0.a, \\ m(-a) = (-m).a, \end{cases}$$

⁽¹⁾ Nous indiquerons plus loin une autre construction, qui est un cas particulier de celle d'un groupe contenant un semi-groupe donné, dans le cas abélien (p. 224).

⁽²⁾ Dans l'enseignement élémentaire, on utilise une représentation concrète du groupe G , en prenant, par exemple, le groupe additif engendré par un vecteur.

⁽³⁾ Le choix des deux signes permettant de distinguer les entiers positifs des entiers négatifs est, *a priori*, arbitraire : les signes $+$ et $-$ ont été adoptés en vue de simplifications d'écriture que nous verrons un peu plus loin.

ou, ce qui revient au même, μ désignant un entier relatif,

$$(2') \quad \begin{cases} \mu a = |\mu| a & \text{si } \mu \text{ est positif,} \\ \mu a = e & \text{si } \mu \text{ est nul,} \\ \mu a = |\mu| (-a) & \text{si } \mu \text{ est négatif.} \end{cases}$$

Tout élément du groupe G peut ainsi être considéré comme un multiple μa de l'élément générateur a , le facteur μ étant un *entier relatif*, et la correspondance biunivoque (1) entre G et C s'écrit sous la forme simple

$$(1') \quad \mu a \leftrightarrow \mu.$$

Cela posé, nous définissons dans C une *addition* par isomorphisme : la somme de deux éléments μa et νa de G est un certain élément σa de G

$$(3) \quad \mu a + \nu a = \sigma a,$$

nous posons dans C

$$(3') \quad \mu + \nu = \sigma.$$

Par rapport à l'addition ainsi définie, C est un groupe additif abélien, isomorphe à G , donc cyclique et infini. L'élément neutre de C est l'image, 0 , de e ; son élément générateur est l'image, $+1$, de a . De plus, les relations (3) et (3') entraînent, pour les multiples de a dans le groupe cyclique G , la loi de *distributivité*

$$(4) \quad \mu a + \nu a = (\mu + \nu) a.$$

En utilisant les définitions précédentes et les règles de calcul valables dans le groupe G , on donne immédiatement aux règles de l'addition dans C leur forme usuelle.

Si $\mu = +m$, $\nu = +n$, on a

$$\mu a + \nu a = ma + na = (m + n)a, \quad \text{d'où} \quad (+m) + (+n) = +(m + n).$$

Si $\mu = +m$, $\nu = -n$, on a

$$\mu a + \nu a = ma + n(-a) = \begin{cases} (m - n)a & \text{si } m > n, \\ e & \text{si } m = n, \\ (n - m)(-a) & \text{si } n > m; \end{cases}$$

d'où

$$(+m) + (-n) = \begin{cases} +(m - n) & \text{si } m > n, \\ 0 & \text{si } m = n, \\ -(n - m) & \text{si } n > m. \end{cases}$$

Si $\mu = -m$, $\nu = -n$, on a

$$\mu a + \nu a = m(-a) + n(-a) = (m+n)(-a),$$

d'où

$$(-m) + (-n) = -(m+n).$$

C étant un groupe additif, la soustraction y est possible d'une manière unique. L'élément opposé $-\mu$ du nombre relatif μ a même valeur absolue que μ et le signe contraire : on a $(-\mu)a = -(\mu a)$, et, pour retrancher μ d'un autre nombre, il suffit d'ajouter le nombre opposé.

Sous la forme précédente, les règles de l'addition et de la soustraction des entiers relatifs sont entièrement indépendantes du groupe cyclique G ; elles peuvent être posées *a priori*.

Définissons maintenant la *multiplication* des entiers relatifs. Un élément quelconque $a' = \lambda a$ du groupe G , distinct de l'élément neutre, engendre un sous-groupe cyclique G' de G qui est lui-même infini, donc isomorphe à G . En utilisant les formules (2'), où nous remplacerons a par a' , nous pouvons regarder tout élément de G' comme un multiple $\mu a'$ de a' , μ étant un entier relatif arbitraire. Mais cet élément $\mu a' = \mu \cdot \lambda a$ appartient à G , donc est un certain multiple, ωa , de a

$$(5) \quad \mu \cdot \lambda a = \omega a.$$

Cette relation fait correspondre à tout couple λ, μ d'entiers relatifs, un entier relatif ω bien déterminé (on prendra $\omega = 0$ si λ est nul) : elle définit donc dans C une opération qui est précisément la *multiplication* des entiers relatifs. Nous écrirons

$$(5') \quad \omega = \mu \lambda.$$

Le produit $\mu \lambda$ de deux nombres relatifs se calcule de la manière suivante. Nous avons, d'après (5) et (2') :

Pour $\mu = +m$, $\lambda = +l$:

$$\mu \cdot \lambda a = (+m)[(+l)a] = m \cdot la = mla, \quad \text{d'où} \quad \omega = +(ml);$$

Pour $\mu = -m$, $\lambda = +l$:

$$\mu \cdot \lambda a = (-m)[(+l)a] = m[-((+l)a)] = m[l(-a)] = ml(-a), \\ \text{d'où} \quad \omega = -(ml);$$

Pour $\mu = +m$, $\lambda = -l$:

$$\mu \cdot \lambda a = m[(-l)a] = m[l(-a)] = ml(-a), \quad \text{d'où} \quad \omega = -(ml);$$

Pour $\mu = -m$, $\lambda = -l$:

$$\mu \cdot \lambda a = (-m)[(-l)a] = m[-((-l)a)] = m[-(l(-a))] = m(la) = mla, \\ \text{d'où} \quad \omega = +(ml).$$

Nous obtenons ainsi la règle usuelle sur la valeur absolue et le signe du produit. Cette règle entraîne immédiatement la *commutativité* et l'*associativité* de la multiplication. L'ensemble C des entiers relatifs admet par rapport à la multiplication l'*élément-unité* $+1$. De plus, tout carré est positif ou nul.

On vérifierait facilement, à partir des règles précédentes, la *distributivité* de la multiplication par rapport à l'addition. Nous l'établirons plutôt en remarquant que les isomorphismes de groupes *additifs*

$$G' \simeq G, \quad \text{c'est-à-dire} \quad \mu a' = \mu \lambda a \leftarrow \rightarrow \mu a$$

et

$$G \simeq C, \quad \text{c'est-à-dire} \quad \mu a \leftarrow \rightarrow \mu$$

entraînent l'isomorphisme

$$G' \simeq C, \quad \text{c'est-à-dire} \quad \mu \lambda a = \omega a \leftarrow \rightarrow \mu.$$

Nous avons donc, en considérant deux nombres relatifs μ et μ' et les produits correspondants $\omega = \mu\lambda$, $\omega' = \mu'\lambda$, et en tenant compte de (4),

$$(\mu\lambda + \mu'\lambda)a = (\omega + \omega')a = \omega a + \omega' a \leftarrow \rightarrow \mu + \mu',$$

c'est-à-dire, puisque l'image de $\mu + \mu'$ dans G' est $(\mu + \mu')\lambda$,

$$\mu\lambda + \mu'\lambda = (\mu + \mu')\lambda.$$

D'après les règles de l'addition et de la multiplication, l'ensemble des entiers *positifs* est isomorphe au domaine des nombres naturels, qui n'est d'ailleurs défini qu'à un isomorphisme près (*voir* Note II, p. 420). Nous identifions donc ces deux ensembles, et nous supprimerons le signe $+$ associé jusqu'à présent à tout nombre positif.

D'autre part, puisqu'on retranche un nombre relatif en ajoutant le nombre opposé, toute suite d'additions et de soustractions peut être mise sous la forme d'une suite d'additions, dans laquelle on convient de remplacer le symbole $+(+m) = -(-m)$ par $+m$ et le symbole $+(-m) = -(+m)$ par $-m$.

On définit aisément dans l'ensemble C des entiers relatifs une *relation d'ordre* coïncidant pour les nombres positifs avec la relation d'ordre des nombres naturels : nous posons $\mu > \nu$ si la différence $\mu - \nu$ est positive. On vérifie immédiatement que cette relation est bien une relation d'ordre. Les nombres négatifs sont inférieurs à zéro, les nombres positifs sont supérieurs à zéro. On peut ajouter aux deux membres d'une inégalité un même entier relatif, ou les multiplier par un même entier *positif*, tandis que si on les multiplie par un même entier négatif, l'inégalité change de sens.

Les entiers relatifs fournissent une *notation définitive* d'un emploi commode pour un *groupe G quelconque*. Ce groupe étant écrit sous forme multiplicative, puisqu'il n'est pas forcément abélien, considérons un élément a de G et un entier naturel m . Posons

$$\begin{aligned} a^m &= a^{+m}, \\ e &= a^0, \\ (a^{-})^m &= a^{-m}. \end{aligned}$$

Nous définissons ainsi pour tout entier relatif μ , l'élément a^μ et nous avons les règles de calcul

$$(4') \quad a^\mu \cdot a^\nu = a^{\mu+\nu},$$

$$(6') \quad (a^\mu)^\nu = a^{\mu\nu}$$

valables aussi bien quand le groupe cyclique engendré par a est fini que lorsqu'il est infini. Cette notation (et la notation correspondante pour la forme additive) sera toujours utilisée à l'avenir. En particulier, nous désignerons l'inverse d'un élément x par x^{-1} , l'inverse d'un complexe H par H^{-1} .

10. Anneaux ; Corps. — L'ensemble G des entiers relatifs possède, en résumé, les propriétés suivantes :

1° Dans cet ensemble sont définies *deux opérations, une addition et une multiplication* ;

2° *Cet ensemble est un groupe abélien par rapport à l'addition* ;

3° *La multiplication est associative* ;

4° *La multiplication est distributive par rapport à l'addition*.

Tout domaine ayant ces quatre propriétés reçoit le nom d'*anneau* ; la multiplication d'un anneau n'est pas nécessairement commutative : si elle l'est, l'anneau est dit *commutatif*. On désigne l'ensemble des entiers relatifs sous le nom d'*anneau des entiers*.

De la définition résulte que tout anneau $\mathcal{A}$ contient un *élément-zéro* (neutre pour l'addition). On désigne cet élément par 0 ; on a

$$a - a = 0, \quad \text{quel que soit } a \in \mathcal{A}.$$

La distributivité de la multiplication par rapport à l'addition entraîne sa *distributivité par rapport à la soustraction*, c'est-à-dire que l'on a

$$(7) \quad (a - b)x = ax - bx$$

et

$$(7') \quad x(a - b) = xa - xb.$$

Pour établir, par exemple, la relation (7), nous remarquons qu'en désignant le premier membre par y , on a

$$y + bx = (a - b + b)x = ax, \quad \text{d'où} \quad y = ax - bx.$$

On a, en particulier,

$$0.x = (a - a)x = ax - ax = 0, \quad \text{quel que soit } x \in \mathcal{A},$$

et de même

$$x.0 = 0.$$

Donc, dans tout anneau, un produit est nul dès qu'au moins un des facteurs l'est. Nous verrons plus loin (chap. IV, § 9, p. 181) que cette condition suffisante n'est nécessaire que dans certains anneaux appelés, dans le cas commutatif, *domaines d'intégrité*, et, parmi lesquels figure l'anneau des entiers.

Un anneau avec élément-unité est un anneau dans lequel existe un élément-unité par rapport à la multiplication. On désigne ordinairement cet élément-unité par e ou par 1 ⁽¹⁾.

Un sous-anneau $\mathcal{A}'$ d'un anneau $\mathcal{A}$ est, par définition, un sous-ensemble de $\mathcal{A}$ qui constitue lui-même un anneau par rapport aux opérations de $\mathcal{A}$, donc un sous-groupe additif de $\mathcal{A}$, fermé par rapport à la multiplication.

Exercice. — L'ensemble des entiers relatifs pairs, zéro compris, est un sous-anneau de l'anneau des entiers $\mathbb{Z}$. Indiquer d'autres sous-anneaux de $\mathbb{Z}$.

Un anneau K ayant plus d'un élément, $K \neq \{0\}$, ne peut jamais être un groupe par rapport à la multiplication, car la règle de simplification est en défaut :

$$0.x = 0 = 0.0 \quad (x \neq 0).$$

Mais il peut arriver que l'ensemble $K - \{0\}$ soit un groupe K^* par rapport à la multiplication, c'est-à-dire que le produit, dans K , de deux éléments non nuls soit toujours différent de zéro (K^* est alors un sous-demi-groupe multiplicatif de K), qu'il existe un élément-unité e , $ex = xe = x$ pour tout x (de K^* donc de K), et que tout élément $x \neq 0$ ait un inverse x^{-1} :

$$xx^{-1} = x^{-1}x = e.$$

(1) Dans l'anneau qui se compose du seul élément zéro, zéro est élément-unité par rapport à la multiplication. Nous excluons implicitement ce cas lorsque nous parlerons d'un anneau avec élément-unité.

L'anneau est alors appelé *corps* dans le cas commutatif (également si rien n'est spécifié au sujet de la commutativité de la multiplication), *corps gauche* si la multiplication n'est pas commutative, *champ de Galois* ⁽¹⁾ si le corps n'a qu'un nombre fini d'éléments (il est alors nécessairement commutatif, d'après un théorème dû à J. H. M. Wedderburn).

Dans un corps, les équations

$$(8) \quad ax = b, \quad ya = b \quad (a \neq 0)$$

ont, chacune, une *solution unique* : $x = a^{-1}b$, $y = ba^{-1}$. Dans le cas commutatif, x et y coïncident : leur valeur commune est appelée *quotient* (exact) de b par a et désigné par b/a . Réciproquement, dès que, dans un anneau K , chacune des équations (8) a au moins une solution pour $a \neq 0$, l'ensemble K^* des éléments non nuls est un groupe multiplicatif d'après le lemme 5 (§ 1, p. 101), et K est un corps.

Exemples. — 1. L'un des corps les plus simples est le champ de Galois C_2 de deux éléments 0, e , dont les tables d'addition et de multiplication sont

+	0	e
0	0	e
e	e	0

$\times$	0	e
0	0	0
e	0	e

2. Des ensembles de nombres particulièrement importants, l'ensemble des *nombres rationnels*, celui des *nombres réels*, celui des *nombres complexes* sont des corps. Du point de vue algébrique, la définition de ces ensembles de nombres consiste justement à *construire un corps* satisfaisant à certaines conditions; cette construction se présente comme un problème typique d'*immersion* (cf. § 8) que nous traiterons ultérieurement.

Exercice 2. — Définir, par sa table d'addition et sa table de multiplication, un champ de Galois C_3 de trois éléments (on vérifiera la distributivité de la multiplication par rapport à l'addition).

(1) On a utilisé, dans le même sens que le mot *corps*, l'expression *domaine de rationalité*. En anglais, tout corps est appelé *field*; en allemand, les expressions *Körper*, *Schiefkörper*, *Galois-Feld* traduisent respectivement corps, corps gauche, champ de Galois.

CHAPITRE IV.

ÉQUIVALENCES RÉGULIÈRES.

A. — ÉQUIVALENCES RÉGULIÈRES DANS UN GROUPOÏDE.

1. **Équivalences régulières, équivalences simplifiables.** — Soient $E = \{a, b, \dots\}$ un groupoïde, O son opération. Une équivalence $\mathcal{R}$, définie dans E , et la décomposition correspondante, sont dites *régulières à droite* par rapport à l'opération O si

$$a \equiv a' \ (\mathcal{R}) \quad \text{entraîne} \quad a O x \equiv a' O x \ (\mathcal{R}) \quad \text{pour tout } x \in E.$$

On définit d'une manière analogue la *régularité à gauche* d'une équivalence et de la décomposition correspondante.

Une équivalence $\mathcal{R}$ régulière à droite et à gauche est dite régulière ⁽¹⁾. Si E est *abélien*, les notions de régularité à droite, de régularité à gauche et de régularité coïncident.

Supposons, pour simplifier l'écriture, que l'opération O soit une multiplication.

⁽¹⁾ Les équivalences régulières ont été considérées, sous le nom d'équivalences homomorphiques, par G. Birkhoff [*On the structure of abstract algebra* (*Proc. Cambridge Phil. Soc.*, t. 31, 1935, p. 433-454)] et, sous le nom de congruences, par H. Hasse (*Höhere Algebra, Sammlung Götschen*, n° 931, Berlin, 1926). Voir également V. S. Krishnan, *Binary relations, congruences and homomorphisms* (*J. Madras University*, B, t. 16, p. 16) et *Contribution à l'Étude des Algèbres partiellement ordonnées et de quelques structures abstraites* (*Bull. Soc. Math.*, t. 78, 1950, p. 234 ; *Thèse*, Paris, 1951).

On trouvera une généralisation et une étude très approfondie dans le Mémoire de A. Châtelet [*Algèbre des relations de congruence* (*Ann. Ec. Norm. Sup.*, (3), t. 64, 1947, p. 339-368)].

Enfin, les problèmes étudiées dans le présent chapitre pour les structures algébriques fondamentales, groupes, anneaux, demi-groupes, sont discutés d'une façon plus générale, et en tenant compte des propriétés d'ordre, dans les *Leçons sur la Théorie des treillis, des Structures algébriques ordonnées et des Treillis géométriques*, par M. L. DUBREIL-JACOTIN, L. LESIEUR et R. CROISOT (*Cahiers scientifiques*, fasc. XXI), 2^e partie, chap. III et chap. IV, § 9.

THÉOREME. — *La condition nécessaire et suffisante pour qu'on puisse multiplier membre à membre les congruences modulo $\mathcal{R}$ est que l'équivalence $\mathcal{R}$ soit régulière.*

La condition est évidemment nécessaire. Elle est également suffisante, car les relations

$$a \equiv a' \ (\mathcal{R}), \quad b \equiv b' \ (\mathcal{R})$$

entraînent, $\mathcal{R}$ étant régulière à droite,

$$ab \equiv a'b \ (\mathcal{R})$$

et, $\mathcal{R}$ étant régulière à gauche

$$a'b \equiv a'b' \ (\mathcal{R}),$$

d'où

$$ab \equiv a'b' \ (\mathcal{R}).$$

$\mathcal{R}$ étant une *équivalence régulière* dans le groupoïde E , considérons l'ensemble-quotient $Q = E/\mathcal{R} = \{A, B, \dots\}$. Si a et a' sont deux éléments d'une même classe A , b et b' deux éléments d'une même classe B , les deux produits ab et $a'b'$ appartiennent à la même classe. On peut donc *définir dans Q une multiplication des classes* : la classe AB est celle qui contient l'un quelconque des produits ab , où $a \in A$, $b \in B$. Cette multiplication fait de Q un groupoïde, appelé *groupoïde-quotient* ⁽¹⁾.

Remarque. — Il ne faut pas confondre la classe-produit AB avec le produit des complexes A, B effectué dans E : d'après le raisonnement précédent, le complexe-produit est indivisible modulo $\mathcal{R}$, et la classe qui le contient est précisément la classe-produit AB ; mais il peut y avoir dans celle-ci des éléments qui ne sont pas le produit d'un élément de A par un élément de B . Par exemple, si, dans l'anneau des entiers, $\mathcal{R}$ est la congruence arithmétique modulo 3, le produit de la classe 2 par elle-même est la classe 1 ; le nombre premier 7, qui appartient à cette classe-produit, n'est pas le produit de deux nombres situés dans la classe 2. La formation du complexe produit a ici peu d'intérêt ; par conséquent, malgré l'identité des notations, aucune confusion n'est à craindre ; il suffit d'ailleurs de rappeler s'il s'agit d'une classe ou d'un complexe.

Exemples. — 1. Dans tout groupoïde, l'égalité et l'équivalence absolue sont régulières.

2. Dans l'anneau C des entiers, la congruence arithmétique modulo m [$x \equiv y(m)$ si $x - y = km$, où k est un entier] est, quel que soit m , régulière par rapport à l'addition et à la multiplication. La définition de ces deux opérations sur les

⁽¹⁾ M. O. BORŮVKA emploie l'expression de *factoroïde*. Cf. O. BORŮVKA, *Ueber Ketten von Faktoröiden* (*Math. Ann.*, t. 118, 1942, p. 41).

classes résiduelles en résulte. Pour $m = 4$, par exemple, les tables d'addition et de multiplication dans l'ensemble-quotient $Q = \{0, 1, 2, 3\}$, sont les suivantes :

+	0	1	2	3
0	0	1	2	3
1		2	3	0
2			0	1
3				2

×	0	1	2	3
0	0	0	0	0
1		1	2	3
2			0	2
3				1

THÉOREME. — L'intersection $\mathcal{J}$ et le produit (transitif) $\mathcal{P}$ d'un ensemble $\mathcal{M}$ d'équivalences $\mathcal{R}$ régulières à droite dans un groupoïde E , sont deux équivalences régulières à droite : les équivalences régulières à droite, dans E , forment donc un sous-treillis complet du treillis de toutes les équivalences.

Soit, en effet,

$$a \equiv a' \quad (\mathcal{J}) \quad \text{c'est-à-dire} \quad a \equiv a' \quad (\mathcal{R}) \quad \text{pour toute} \quad \mathcal{R} \in \mathcal{M}.$$

Il en résulte

$$ax \equiv a'x \quad (\mathcal{R}) \quad \text{pour toute} \quad \mathcal{R} \in \mathcal{M},$$

donc

$$ax \equiv a'x \quad (\mathcal{J}),$$

et $\mathcal{J}$ est régulière à droite.

Soit maintenant

$$a \equiv a' \quad (\mathcal{P}).$$

C'est dire qu'il existe une suite finie $a_1 = a, a_2, \dots, a_n = a'$ d'éléments de E , et des équivalences $\mathcal{R}_1, \mathcal{R}_2, \dots, \mathcal{R}_{n-1}$ de $\mathcal{M}$ telles que l'on ait

$$a_i \equiv a_{i+1} \quad (\mathcal{R}_i) \quad (i = 1, 2, \dots, n-1).$$

Il en résulte

$$a_i x \equiv a_{i+1} x \quad (\mathcal{R}_i) \quad (i = 1, 2, \dots, n-1)$$

et, par suite,

$$ax \equiv a'x \quad (\mathcal{P}).$$

Le produit $\mathcal{P}$ est donc aussi une équivalence régulière à droite.

On a des propositions analogues pour la régularité à gauche et la régularité bilatère.

Exercices. — 1. Deux vecteurs libres de l'espace à trois dimensions sont regardés comme équivalents s'ils ont même projection orthogonale sur un plan P . Cette équivalence est-elle régulière : 1° par rapport à l'addition géométrique ? 2° par rapport à la multiplication vectorielle ?

2. Soit $\mathcal{R}$ une équivalence régulière dans un groupoïde E . Si une classe A mod. $\mathcal{R}$ contient un sous-groupoïde, en particulier si A contient un élément idempotent, A est un sous-groupoïde.

3. Soit $\mathcal{R}$ une équivalence régulière à droite dans un groupoïde E . Si E admet un élément-unité à gauche u , la classe U contenant u est un sous-groupoïde unitaire à gauche. Si E possède un élément permis à droite z , la classe Z contenant z est un complexe permis à droite (donc un sous-groupoïde).

Dans un groupoïde E , écrit par exemple sous forme multiplicative, une équivalence $\mathcal{R}$ est par définition *simplifiable à droite* si toute relation de la forme

$$ax \equiv a'x \quad (\mathcal{R}) \quad \text{entraîne} \quad a \equiv a' \quad (\mathcal{R}).$$

On définit d'une manière analogue une équivalence *simplifiable à gauche*. Une équivalence est *simplifiable* si elle est simplifiable à droite et à gauche.

Exemples. — 1. L'équivalence absolue est toujours simplifiable. Dire que l'égalité est simplifiable à droite, par exemple, signifie que la règle de simplification à droite est valable dans E .

2. Dans l'anneau des entiers regardé comme groupoïde *additif*, la congruence arithmétique modulo m est simplifiable, quel que soit m .

3. Dans l'anneau des entiers regardé comme groupoïde *multiplicatif*, la congruence arithmétique modulo m n'est simplifiable en aucun cas, car si x n'est pas premier à m , en particulier si $x = 0$ ou m , la relation $ax \equiv a'x(m)$ n'entraîne pas $a \equiv a'(m)$.

On voit qu'en général la régularité et la simplifiabilité d'une équivalence $\mathcal{R}$ ne sont pas des propriétés équivalentes. Toutefois, *dans un groupe G et par rapport à l'opération du groupe, toute équivalence régulière à droite par exemple est simplifiable à droite* ⁽¹⁾, puisque simplifier à droite par l'élément x revient à multiplier à droite par l'élément inverse x^{-1} .

Soit $\mathcal{R}$ une équivalence régulière dans un groupoïde E . Pour que la règle de simplification à droite soit valable dans le groupoïde-quotient $Q = E/\mathcal{R}$ il faut et il suffit que $\mathcal{R}$ soit simplifiable à droite.

(¹) M. G. Thierrin a montré récemment qu'un *demi-groupe* dans lequel, inversement, toute équivalence régulière à droite est simplifiable à droite, et toute équivalence régulière à gauche simplifiable à gauche, est un groupe. Voir *Bull. Acad. Roy. de Belgique*. t. 39, 1953, p. 943, et *Thèse* (Paris, 1954).

La condition est *nécessaire* : soit $ax \equiv bx$ ($\mathcal{R}$) ; nous avons

$$\overline{ax} = \overline{bx} = \overline{bx} = \overline{bx}, \quad \text{d'où} \quad \overline{a} = \overline{b} \quad \text{et} \quad a \equiv b \quad (\mathcal{R})$$

$\mathcal{R}$ est simplifiable.

La condition est *suffisante* : l'égalité $\overline{ax} = \overline{bx}$ dans Q entraîne $ax \equiv bx$ ($\mathcal{R}$) dans E , d'où

$$a \equiv b \quad (\mathcal{R}) \quad \text{et} \quad \overline{a} = \overline{b}.$$

Exercices. — 3. Dans un groupoïde E , l'intersection $\mathcal{I}$ d'un ensemble $\mathcal{M}$ d'équivalences $\mathcal{R}$ simplifiables à droite, est une équivalence simplifiable à droite.

4. Dans un groupe G , toute équivalence simplifiable à droite est régulière à droite.

5. Dans un treillis T , les équivalences régulières par rapport à l'intersection et à l'union vérifient la *loi de distributivité générale* ⁽¹⁾ :

$$\mathcal{R} \cap \left(\bigcup_{s \in \Sigma} \mathcal{S} \right) = \bigcup_{s \in \Sigma} (\mathcal{R} \cap \mathcal{S})$$

donc forment un treillis distributif ⁽²⁾.

2. Homomorphismes. — Soient $E = \{a, b, \dots\}$, $\bar{E} = \{\bar{a}, \bar{b}, \dots\}$ deux groupoïdes dont nous désignerons les opérations respectives par O et $\bar{O}$.

Le groupoïde $\bar{E}$ est dit *homomorphe* à E ⁽³⁾ s'il existe une *application* α de E sur $\bar{E}$

$$(1) \quad a \rightarrow \bar{a} = \alpha a$$

respectant les opérations O et $\bar{O}$, c'est-à-dire telle que les relations

$$a \rightarrow \bar{a}, \quad b \rightarrow \bar{b},$$

entraînent

$$\alpha(aOb) = (\alpha a)\bar{O}(\alpha b) \quad \text{ou} \quad aOb \rightarrow \bar{a}\bar{O}\bar{b}.$$

On écrit alors

$$E \xrightarrow{\alpha} \bar{E},$$

⁽¹⁾ Ce résultat est dû à N. Funayama et T. Nakayama ; Cf. *On the congruence relations on lattices* (Proc. Imp. Acad. Tokyo, t. 18, 1942, p. 530) et *On the distributivity of a lattice of lattice-congruences* (ibid., p. 533). Voir aussi G. BIRKHOFF, *Lattice theory*, theorem 5, p. 24.

⁽²⁾ *Leçons sur la Théorie des treillis...*, 2^e partie, chap. III, th. 10, p. 183.

⁽³⁾ On employait autrefois les expressions : isomorphe mériédriquement, isomorphisme mériédrique. Les isomorphismes proprement dits étaient appelés isomorphismes holoédriques.

ou, plus brièvement,

$$E \rightarrow \bar{E} \quad \text{ou} \quad E \sim \bar{E}.$$

Cette dernière notation, qui s'énonce E homomorphe à $\bar{E}$, est la plus employée. La correspondance (1) est désignée sous le nom d'*homomorphisme* dans le cas général, d'*endomorphisme* si $\bar{E}$ est une partie de E . Il est essentiel de remarquer que, dans un homomorphisme, les deux groupoïdes $E, \bar{E}$ jouent des rôles *dissymétriques*, à moins que la correspondance (1) ne soit biunivoque, cas dans lequel l'homomorphisme devient un isomorphisme.

Le plus souvent, on représente par un même signe les opérations O et $\bar{O}$. Si ces opérations sont par exemple des multiplications, la condition pour que l'application (1) les respecte s'écrit

$$\overline{ab} = \bar{a}, \bar{b} \quad \text{ou} \quad \alpha(ab) = \alpha a . \alpha b.$$

Exemple. — Si, étant donné un plan P dans l'espace, nous faisons correspondre à tout vecteur libre $\vec{V}$ sa projection orthogonale $\vec{V}_1$ sur P , nous avons l'homomorphisme

$$G \sim G_1$$

entre le groupe G des vecteurs libres de l'espace et le groupe G_1 des vecteurs libres du plan P , par rapport à l'addition géométrique.

Considérons une équivalence régulière, $\mathcal{R}$, dans un groupoïde multiplicatif E .

Le groupoïde-quotient $Q = E/\mathcal{R}$ est homomorphe à E .

Si, en effet, A désigne la classe contenant l'élément a , l'application $a \rightarrow A$ de E sur Q respecte les multiplications, puisqu'on a

$$ab \rightarrow AB,$$

d'après la définition même de la multiplication dans Q . Cette application est donc un *homomorphisme*, et nous avons, pour toute équivalence régulière $\mathcal{R}$ de E ,

$$E \sim E/\mathcal{R}.$$

Inversement, tout homomorphisme

$$E \sim \bar{E}$$

peut, d'après le théorème suivant, être défini à partir d'une équivalence régulière opérant dans le groupoïde E .

THÉORÈME D'HOMOMORPHISME (cas des groupoïdes). — *Si E est un groupoïde homomorphe à E, il existe dans E une équivalence régulière $\mathcal{R}$ telle que l'on ait l'isomorphisme*

$$E/\mathcal{R} \simeq \bar{E}.$$

Soit, en effet, $\mathcal{R}$ l'équivalence d'application définie, dans E, par $a \equiv b (\mathcal{R})$ si et seulement si l'on a, dans $\bar{E}$, $\bar{a} = \bar{b}$ (cf. chap. I, § 7, p. 29). Cette équivalence $\mathcal{R}$, appelée ici *équivalence d'homomorphisme*, est *régulière à droite*, car $a \equiv b (\mathcal{R})$ entraîne $\bar{a} = \bar{b}$, d'où, x étant un élément quelconque de E, $\bar{a}x = \bar{b}x$, donc : $\overline{ax} = \overline{bx}$ et, par suite, $ax \equiv bx (\mathcal{R})$. On démontre de même que $\mathcal{R}$ est régulière à gauche et, par suite, régulière.

Comme les classes modulo $\mathcal{R}$ et les éléments de E se correspondent biunivoquement et que cette correspondance respecte les opérations de $\bar{E}$ et de $E/\mathcal{R}$, on a bien, entre ces deux groupoïdes, l'*isomorphisme*

$$E/\mathcal{R} \simeq \bar{E}.$$

Exemple. — Reprenons l'exemple du groupe G des vecteurs libres $\vec{V}$ de l'espace et du groupe homomorphe G_1 des vecteurs libres d'un plan P. Chaque vecteur $\vec{V}$ de G a pour image dans G_1 sa projection $\vec{V}_1$ sur P. Si $\mathcal{R}$ désigne l'équivalence d'homomorphisme, on a : $\vec{V} \equiv \vec{V}' (\mathcal{R})$ si ces deux vecteurs ont même projection sur P : $\vec{V}_1 = \vec{V}'_1$.

E, E', E'' étant trois groupoïdes, les relations

$$E \sim E', \quad E' \sim E'' \quad \text{entraînent} \quad E \sim E'';$$

autrement dit l'homomorphisme est une propriété transitive.

Étant donné un homomorphisme

$$E \sim \bar{E},$$

toute relation entre éléments de E s'exprimant au moyen du signe = et de l'opération O de E, entraîne la relation analogue dans $\bar{E}$, les éléments $a, b, \dots$ de E étant remplacés par leurs images respectives $\bar{a}, \bar{b}, \dots$, et l'opération O par l'opération $\bar{O}$.

Il en résulte que *certaines* propriétés algébriques sont valables dans $\bar{E}$ dès qu'elles le sont dans E : ainsi, l'associativité, la commutativité, si elles sont valables pour O, le sont pour $\bar{O}$.

THÉOREME 1. — Si E est un groupe, son image homomorphe $\bar{E}$ en est une aussi.

Si $\bar{e}$ est l'image de l'élément-unité e du groupe E et si nous désignons par $\bar{x}$ un élément quelconque de $\bar{E}$, par x un des éléments de E dont $\bar{x}$ est l'image, nous avons

$$\bar{e} \cdot \bar{x} = \overline{ex} = \bar{x} \quad \text{et, de même,} \quad \bar{x} \cdot \bar{e} = \bar{x}.$$

On voit de même que $\bar{x}$ admet pour inverse dans $\bar{E}$ l'image de l'élément x^{-1} .

$$x \cdot \overline{x^{-1}} = \overline{xx^{-1}} = e.$$

Si, en particulier, $\mathcal{R}$ est une équivalence régulière dans un groupe G , l'ensemble quotient $G/\mathcal{R}$ est, par rapport à la multiplication des classes, un groupe, appelé *groupe-quotient* ou *groupe-facteur*.

De même, le domaine-quotient d'un anneau A par une équivalence $\mathcal{R}$ définie dans A et régulière par rapport à l'addition et à la multiplication, est un anneau, appelé *anneau-quotient* : $A/\mathcal{R}$ est en effet un groupe abélien par rapport à l'addition des classes, un demi-groupe par rapport à leur multiplication, et celle-ci est visiblement distributive par rapport à l'addition. L'*anneau-quotient* $A/\mathcal{R}$ est homomorphe à A .

Si nous prenons comme anneau l'anneau C des entiers et comme équivalence régulière dans C la congruence arithmétique modulo m , nous obtenons comme anneau-quotient un domaine fini, de m éléments, appelé *anneau des classes résiduelles modulo m* et désigné par

$$C/(m) = \{0, 1, 2, \dots, m-1\}.$$

Dans l'exemple 2, page 143, nous avons construit les tables d'addition et de multiplication de l'anneau $C/(4)$.

Inversement, une propriété algébrique dans un groupoïde $\bar{E}$ image d'un groupoïde E dans un homomorphisme α peut entraîner, dans E , une propriété remarquable. Donnons-en deux exemples.

THÉOREME 2. — Si $\bar{A}$ est un sous-groupoïde de $\bar{E}$, son image inverse $A = \alpha^{-1} \bar{A}$, ensemble de tous les éléments a de E dont l'image αa appartient à $\bar{A}$, est un sous-groupoïde de E . En particulier, l'image inverse d'un élément idempotent de $\bar{E}$ est un sous-groupoïde de E ; celle d'un élément-unité à gauche (par exemple) $\bar{u}$, est un sous-groupoïde unitaire à gauche U .

Si a_1, a_2 sont deux éléments de A , nous avons

$$\overline{a_1 a_2} = \overline{a_1} \cdot \overline{a_2} \in \overline{A}, \quad \text{d'où} \quad a_1 a_2 \in A.$$

Si $ux = u'$, où u et $u' \in U$, on a $\overline{ux} = \overline{u'}$, c'est-à-dire $\overline{u} \cdot \overline{x} = \overline{u}$ ou $\overline{x} = \overline{u}$, donc $x \in U$.

THÉOREME 3. — *Si $\overline{Z}$ est un sous-ensemble permis à droite (par exemple) dans $\overline{E}$, son image inverse $Z = \alpha^{-1} \overline{Z}$, ensemble de tous les éléments z de E dont l'image αz appartient à $\overline{Z}$, est un sous-ensemble permis à droite dans E . En particulier, l'image inverse d'un élément permis, ou zéro, de $\overline{E}$ est un sous-ensemble permis (ou idéal, cf. chap. II, § 4, p. 76).*

Soient $z \in Z$, $x \in E$. Nous avons

$$\overline{zx} = \overline{z} \cdot \overline{x} \in \overline{Z}, \quad \text{d'où} \quad zx \in Z.$$

Il est essentiel de remarquer que, lorsqu'il s'agit d'un véritable homomorphisme (et non d'un isomorphisme), certaines propriétés algébriques peuvent appartenir à $\overline{E} = E/\mathcal{R}$ sans appartenir à E ; ce fait, qui est déjà mis en évidence par l'exercice 1 ci-dessous, apparaîtra clairement au paragraphe 9 (p. 179) où la différence des propriétés algébriques que possèdent d'une part l'anneau C des entiers et ses sous-anneaux, d'autre part les anneaux de classes résiduelles $C/(m)$, nous conduira aux notions fondamentales concernant la classification des anneaux.

Exercices. — 1. Montrer qu'il existe un groupe G homomorphe au demi-groupe D défini par la table de multiplication suivante :

	x_0	x_1	x_2	x_3
x_0	x_0	x_0	x_2	x_2
x_1	x_1	x_1	x_3	x_3
x_2	x_2	x_2	x_0	x_0
x_3	x_3	x_3	x_1	x_1

2. La correspondance $x \rightarrow x^2$ entre l'anneau des entiers C et l'ensemble des carrés $\overline{C}$, considérés comme groupoides *multiplicatifs*, est un homomorphisme. Appliquer le théorème d'homomorphisme.

B. — ÉQUIVALENCES RÉGULIÈRES À DROITE DANS UN GROUPE.

3. **Décomposition d'un groupe en classes à droite par rapport à un sous-groupe.** — Considérons, dans un groupe G , une équivalence régulière à droite, $\mathcal{R}$. Désignons par S la *classe-unité*, c'est-à-dire la classe modulo $\mathcal{R}$ qui contient l'élément-unité e de G . Soient s_1 et s_2 deux éléments de S . Les relations

$$s_1 \equiv e \quad (\mathcal{R}), \quad s_2 \equiv e \quad (\mathcal{R})$$

entraînent

$$s_1 s_2 \equiv e s_2 \quad (\mathcal{R}), \quad \text{où l'on a} \quad e s_2 = s_2 \equiv e \quad (\mathcal{R}),$$

donc

$$s_1 s_2 \equiv e \quad (\mathcal{R}), \quad \text{c'est-à-dire} \quad s_1 s_2 \in S.$$

S est donc un *sous-groupe* de G ⁽¹⁾.

D'autre part, si nous désignons par s^{-1} l'inverse, dans G , d'un élément s de S , nous avons

$$s s^{-1} \equiv e s^{-1} \quad (\mathcal{R}),$$

c'est-à-dire

$$e \equiv s^{-1} \quad (\mathcal{R}), \quad \text{d'où} \quad s^{-1} \in S,$$

la *classe-unité* S est donc un *sous-groupe* de G .

Cherchons maintenant de quelle forme sont les autres classes. Soit x un élément de la classe A qui contient un élément donné a . La relation $x \equiv a \quad (\mathcal{R})$ équivaut à

$$x a^{-1} \equiv e \quad (\mathcal{R}),$$

c'est-à-dire à

$$x a^{-1} \in S \quad \text{ou} \quad x \in S a,$$

Sa désignant le complexe des produits sa , où $s \in S$. La classe $A = Sa$ contenant a est appelée *classe à droite par rapport au sous-groupe* S ⁽²⁾. Pour que deux telles classes Sa , Sb coïncident, il faut et il suffit que

(1) Cf. § 1, exerc. 2. D'après cet exercice, le sous-groupe S est, de plus, unitaire à gauche; il en résulte que c'est un *sous-groupe* de G (propriété A'' , chap. III, § 3, p. 109).

(2) On emploie quelquefois le terme de *co-groupe* (Nebengruppe, coset). Signalons aussi que certains auteurs donnent aux complexes Sa , Sb , ... le nom de *classes à gauche* (ZASSENHAUS, *Lehrbuch der Gruppentheorie*, Leipzig-Berlin, 1937, p. 9 et 10).

a et b soient équivalents modulo $\mathcal{R}$, c'est-à-dire que l'on ait

$$a.b^{-1} \in S.$$

Nous avons ainsi établi le théorème suivant.

THÉORÈME 1. — *Dans toute décomposition régulière à droite d'un groupe G , la classe-unité S est un sous-groupe de G . Les autres classes sont les différents complexes Sa ($a \notin S$).*

Ce théorème admet une réciproque, également importante.

THÉORÈME 2. — *A tout sous-groupe S de G est associée une équivalence régulière à droite $\mathcal{R}_S$ telle que les classes modulo $\mathcal{R}_S$ soient les complexes Sa distincts.*

Considérons, dans G , la relation $\mathcal{R}_S$ définie par

$$x \mathcal{R}_S x_1 \quad \text{si} \quad x_1 x^{-1} \in S.$$

$\mathcal{R}_S$ est une *équivalence*. En effet, $\mathcal{R}_S$ est *réflexive*, puisqu'on a

$$xx^{-1} = e \in S,$$

symétrique, puisque l'élément

$$xx_1^{-1} = (x_1 x^{-1})^{-1}$$

appartient au sous-groupe S en même temps que $x_1 x^{-1}$. Enfin, $\mathcal{R}_S$ est *transitive*, puisque les relations

$$x_2 x_1^{-1} \in S, \quad x_1 x^{-1} \in S$$

entraînent

$$x_2 x_1^{-1} x_1 x^{-1} = x_2 x^{-1} \in S.$$

D'autre part, $\mathcal{R}_S$ est *régulière à droite*, car la relation

$$a_1 \equiv a \quad (\mathcal{R}_S), \quad \text{c'est-à-dire} \quad a_1 = sa, \quad \text{avec } s \in S,$$

entraîne, quel que soit $x \in G$,

$$a_1 x = sa.x = s.ax, \quad \text{c'est-à-dire} \quad a_1 x \equiv ax \quad (\mathcal{R}_S).$$

Il résulte de la définition même de $\mathcal{R}_S$ que les classes modulo $\mathcal{R}_S$ sont les complexes, ou classes à droite, Sa .

D'après les deux théorèmes précédents, il existe une *correspondance biunivoque* entre les équivalences régulières à droite dans un groupe G , et les sous-groupes de G .

On a des propositions analogues aux théorèmes 1 et 2 pour les *équivalences régulières à gauche* : chacune d'elles décompose G en classes à gauche par rapport au sous-groupe S classe-unité ; inversement, à tout sous-groupe S de G est associée une équivalence ${}_s\mathcal{R}$ régulière à gauche définie par

$$x {}_s\mathcal{R} x_1 \quad \text{si} \quad x^{-1}x_1 \in S.$$

La classe $\text{mod } {}_s\mathcal{R}$ (ou classe à gauche) qui contient a est ici le complexe aS .

Associons à un sous-groupe S du groupe G l'application multiforme f de G sur G définie par

$$f(a) = a^{-1}S \quad (a \in G);$$

$f(a)$ est donc l'ensemble des éléments x de G vérifiant la relation

$$(1) \quad ax \in S.$$

THÉOREME 3. — *L'application f ainsi définie est semi-uniforme, et les ensembles stables minimaux sont les classes à droite Sa .*

En effet, la relation $a \mathfrak{T} b$ (voir chap. I, § 8, p. 31), c'est-à-dire

$$f(a) \cap f(b) \neq \emptyset,$$

signifie $a^{-1}s = b^{-1}s'$, où $s, s' \in S$, d'où

$$ba^{-1} = s's^{-1} \in S,$$

et, par conséquent,

$$Sb = Sa, \quad \text{d'où} \quad f(a) = f(b);$$

l'application f est bien semi-uniforme.

La relation $\mathfrak{T}$ coïncide alors avec la relation d'équivalence $\mathcal{C}$ décomposant G en sous-ensembles stables minimaux (*loc. cit.*, th. 2, p. 35) : l'ensemble stable minimal contenant a se compose de tous les éléments b vérifiant $a \mathfrak{T} b$, c'est-à-dire $ba^{-1} \in S$: c'est donc la classe à droite Sa , et nous avons

$$\mathfrak{T} = \mathcal{C} = \mathcal{R}_S.$$

En outre, d'après (1), l'application inverse f^{-1} associe à chaque élément x de G l'ensemble $f^{-1}(x) = Sx^{-1}$. L'équivalence correspondante, $\mathfrak{T}' = \mathcal{C}'$, décompose G en classes à gauche xS , et nous avons

$$\mathfrak{T}' = \mathcal{C}' = {}_s\mathcal{R}.$$

Par suite, en tenant compte du théorème général établi au chapitre I

(§ 8, th. 1, p. 33), nous voyons que l'ensemble $G/\mathcal{R}_s$ des classes à droite et l'ensemble $G/_s\mathcal{R}$ des classes à gauche par rapport à un sous-groupe S se correspondent biunivoquement :

$$G/\mathcal{R}_s \leftarrow \rightarrow G/_s\mathcal{R}.$$

Comme nous le verrons (section E), le théorème 3 a l'intérêt de pouvoir être étendu à la théorie des demi-groupes.

Remarquons encore que, la règle de simplification étant valable dans G , toute classe à droite Sa et toute classe à gauche aS ont même puissance que S ; cette propriété est particulièrement importante quand G est un groupe fini (voir § 4).

Soient $\mathcal{R}$ et $\mathcal{R}'$ deux équivalences régulières à droite, S et S' les sous-groupes correspondants. On a immédiatement la proposition suivante :

Si $\mathcal{R} \subseteq \mathcal{R}'$, on a $S \subseteq S'$, et réciproquement.

D'autre part, à l'intersection $\mathcal{I} = \mathcal{R} \cap \mathcal{R}'$, qui est également régulière à droite, correspond le sous-groupe $S \cap S'$, car la classe-unité modulo $\mathcal{I}$ est l'intersection des classes-unité modulo $\mathcal{R}$ et modulo $\mathcal{R}'$. De même pour l'intersection d'un ensemble quelconque d'équivalences régulières à droite.

Des deux propositions précédentes résulte qu'au produit transitif $\mathcal{Q} = \mathcal{R} \times \mathcal{R}'$ qui est lui aussi une équivalence régulière à droite, correspond la réunion complète Q des sous-groupes S et S' . En effet, $\mathcal{Q}$ est l'intersection de toutes les équivalences contenant $\mathcal{R}$ et $\mathcal{R}'$, et Q est l'intersection de tous les sous-groupes contenant S et S' ⁽¹⁾. Le treillis des équivalences régulières à droite dans G et le treillis des sous-groupes de G sont donc isomorphes.

THÉOREME 4. — *La condition nécessaire et suffisante pour que les sous-groupes S et S' soient permutables, est que les équivalences régulières à droite correspondantes $\mathcal{R}$ et $\mathcal{R}'$ soient elles-mêmes permutables.*

1° La condition est nécessaire : Soient a , b , x trois éléments du groupe G , tels que l'on ait

$$a \equiv x \ (\mathcal{R}), \quad x \equiv b \ (\mathcal{R}'),$$

(1) La propriété s'étend visiblement à une famille quelconque d'équivalences régulières à droite

c'est-à-dire

$$ax^{-1} = s \in S, \quad xb^{-1} = s' \in S',$$

d'où, puisque S et S' sont permutables,

$$ab^{-1} = ss' = s'_1 s_1, \quad \text{où } s_1 \in S \text{ et } s'_1 \in S'.$$

Il en résulte

$$s'^{-1}_1 a = s_1 b = \gamma,$$

d'où

$$a \equiv \gamma \pmod{\mathcal{R}'}, \quad \gamma \equiv b \pmod{\mathcal{R}},$$

donc $\mathcal{R}$ et $\mathcal{R}'$ sont bien permutables.

2° La condition est *suffisante*. Soient $s \in S$, $s' \in S'$. Nous avons, e désignant l'élément-unité de G ,

$$s \equiv e \pmod{\mathcal{R}}, \quad e \equiv s'^{-1} \pmod{\mathcal{R}'},$$

Puisque $\mathcal{R}$ et $\mathcal{R}'$ sont permutables, il existe un élément $m \in G$ tel que l'on ait

$$s \equiv m \pmod{\mathcal{R}'}, \quad m \equiv s'^{-1} \pmod{\mathcal{R}},$$

c'est-à-dire

$$sm^{-1} = s'_1 \in S', \quad ms' = s_1 \in S,$$

d'où

$$ss' = s'_1 s_1$$

ce qui exprime que S et S' sont permutables.

Exercices. — 1. On considère le groupe symétrique S_3 , ensemble des substitutions sur les chiffres 1, 2, 3, et le sous-groupe $S = \{e, a\}$, où e est la substitution identique et où a désigne la substitution (involutive)

$$a = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}.$$

Former les décompositions en classes à droite et en classes à gauche de S_3 par rapport à S . On remarquera que ces décompositions sont *différentes*.

2. Dans un groupe G , soit A une classe à droite par rapport à un sous-groupe S .

1° Le complexe A^{-1} est classe à gauche par rapport à S .

2° Le complexe $S^* = x^{-1}Sx$, où x désigne un élément quelconque de G , est aussi un sous-groupe de G . Montrer qu'on peut choisir x de manière que A soit classe à gauche par rapport à S^* .

3. La condition nécessaire et suffisante pour qu'un complexe H d'un groupe G soit une classe (à droite ou à gauche par rapport à un sous-groupe quelconque) est que les relations

$$h_1 \in H, \quad h_2 \in H, \quad h_3 \in H$$

entraînent

$$h_1 h_2^{-1} h_3 \in H \quad (1).$$

4. Groupes finis; groupes cycliques. — Soit G un groupe fini, d'ordre N . S'il existe un sous-groupe véritable S de G , S est lui-même fini; soit n son ordre

$$S = \{e = s_1, s_2, \dots, s_n\}.$$

Décomposons G en classes à droite Sa par rapport à S . Chacune de ces classes comprend n éléments $s_i a$ ($i = 1, 2, \dots, n$) qui sont *distincts*, puisque la règle de simplification à droite est valable dans G . Donc,

THÉOREME. — *L'ordre n d'un sous-groupe S d'un groupe fini G d'ordre N , est un diviseur de N , $n \mid N$.*

Le nombre des classes, $\frac{N}{n}$, dans la décomposition à droite ou dans la décomposition à gauche de G par rapport à S , est appelé l'*index* de S dans G , ou l'index de G par rapport à S , et désigné par $G : S$.

Si un sous-groupe G'' est contenu dans un sous-groupe G' ,

$$G \supseteq G' \supseteq G'',$$

on a

$$G : G'' = (G : G')(G' : G''),$$

car l'équivalence $\mathcal{R}''$ correspondant à G'' est contenue dans l'équivalence $\mathcal{R}'$ correspondant à G' et chaque classe $G'a$ de G par rapport à G' est, comme G' , décomposée par $\mathcal{R}''$ en $G' : G''$ classes.

L'ordre n d'un élément x quelconque d'un groupe fini G étant, par définition, l'ordre du sous-groupe cyclique $\langle x \rangle$, divise l'ordre N de $G : n \mid N$.

Considérons un groupe cyclique $G = \langle a \rangle$, fini et d'ordre $N : a^N = e$. Tout sous-groupe G' de G est cyclique (chap. III, § 4, p. 112).

THÉOREME 1. — *L'ordre d'un élément $b = a^n$ du groupe cyclique G est égal au quotient N' de N par le p. g. c. d. $(^2)$ de N et de n ; c'est donc un diviseur de N . Si, en particulier, n divise N , on a $N' = \frac{N}{n}$.*

(¹) Cf. P. DUBREIL, *Contribution à la Théorie des Demi-groupes* (Mémoires de l'Académie des Sciences, t. 63, 1941, chap. I, § 5).

(²) Nous supposons connues les propriétés élémentaires concernant le p. g. c. d. et le p. p. c. m. des nombres naturels, et les nombres premiers. Ces propriétés seront d'ailleurs retrouvées, d'une manière indépendante, dans la théorie des anneaux euclidiens (chap. VI, § 3, p. 318).

Les quotients N' , n' de N et n par leur p. g. c. d. sont premiers entre eux. Pour que l'on ait $(a^n)^m = e$, il faut et il suffit que mn soit multiple de N ,

$$mn = hN \quad \text{ou} \quad mn' = hN',$$

donc que m soit multiple de N' : N' est donc l'ordre du groupe $G' = (a^n)$.

COROLLAIRE. — *Pour que l'élément $b = a^n$ soit un générateur de G , c'est-à-dire pour que l'on ait $N' = N$; il faut et il suffit que n soit premier à N .*

Le nombre des générateurs distincts de G est, par conséquent, égal à l'indicateur ou fonction d'Euler $\varphi(N)$, nombre des entiers naturels premiers à N et ne dépassant pas N [on a, en particulier $\varphi(1) = 1$, nombre de générateurs de (e)].

Si N est un nombre *primaire*, c'est-à-dire une puissance de nombre premier, $N = p^\alpha$, les seuls entiers naturels non premiers à N sont les multiples mp de p ($m = 1, 2, \dots, p^{\alpha-1}, \dots$) parmi lesquels il y a $p^{\alpha-1} - 1$ nombres inférieurs à N . Nous avons donc

$$\varphi(p^\alpha) = p^\alpha - 1 - (p^{\alpha-1} - 1) = p^\alpha \left(1 - \frac{1}{p}\right).$$

Les deux théorèmes suivants, d'ailleurs importants par eux-mêmes, nous conduiront à l'expression de $\varphi(N)$ pour N quelconque.

THÉORÈME 2. — *Si, dans un groupe G , fini ou non, deux éléments a , b sont permutables et ont des ordres finis r et s premiers entre eux, l'ordre t du produit ab est égal à rs .*

Pour tout entier m , on a, puisque a et b sont permutables,

$$(ab)^m = a^m b^m,$$

d'où

$$(ab)^{rs} = e, \quad \text{donc} \quad t \mid rs.$$

On a également

$$(ab)^s = a^s b^s = a^s,$$

et cet élément est un générateur du groupe cyclique (a) puisque s est premier à r ; a est donc une puissance de ab , et, d'après le théorème 1, son ordre r divise t . De même s divise t et, par conséquent, rs divise t : $rs \mid t$. Les deux relations $t \mid rs$ et $rs \mid t$ entraînent $t = rs$.

THÉORÈME 3. — *Si $G = (a)$ est un groupe cyclique d'ordre $N = rs$, où r et s sont premiers entre eux, tout élément de G est, d'une*

manière unique, le produit de deux éléments x_1, x_2 appartenant à des sous-groupes G_1, G_2 d'ordres s et r .

Soient G_1, G_2 les deux sous-groupes cycliques engendrés par $b_1 = a^r$ et $b_2 = a^s$; G_1 est d'ordre s et G_2 d'ordre r . L'intersection $G_1 \cap G_2$ est un groupe dont l'ordre i doit diviser r et s : on a donc $i = 1$, d'où $G_1 \cap G_2 = (e)$. Il en résulte que les $N = rs$ éléments de G de la forme

$$b_1^{\beta_1} b_2^{\beta_2} \quad (\beta_1 = 0, 1, \dots, s-1; \beta_2 = 0, 1, \dots, r-1)$$

sont tous distincts, car l'égalité

$$b_1^{\beta_1} b_2^{\beta_2} = b_1^{\beta'_1} b_2^{\beta'_2}$$

entraîne

$$b_1^{\beta_1 - \beta'_1} b_2^{\beta_2 - \beta'_2} = e, \quad \text{donc} \quad \beta'_1 = \beta_1, \quad \beta'_2 = \beta_2.$$

Par conséquent, l'ensemble $G_1 G_2$ de ces éléments coïncide avec G ⁽¹⁾ et nous avons bien, pour tout $x \in G$,

$$x = x_1 x_2, \quad \text{avec} \quad x_1 = b_1^{\beta_1} \in G_1, \quad x_2 = b_2^{\beta_2} \in G_2.$$

Les éléments x_1 et x_2 sont permutables comme éléments du groupe cyclique G , et leurs ordres s' et r' divisant respectivement s et r , sont premiers entre eux. Par suite, l'ordre de x est $r's'$ et, pour que x soit un générateur de G , il faut et il suffit que x_1 soit un générateur de G_1 et x_2 un générateur de G_2 . Nous avons donc

$$\varphi(rs) = \varphi(r)\varphi(s)$$

dès que r et s sont premiers entre eux.

Si G est un groupe cyclique d'ordre $N = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_h^{\alpha_h}$, où les p_i sont des nombres premiers différents, l'application répétée des résultats précédents montre, d'une part, que tout élément x de G est d'une manière unique le produit de h éléments $x_1, x_2, \dots, x_h$ appartenant à des sous-groupes $G_1, G_2, \dots, G_h$ dont les ordres respectifs sont $p_1^{\alpha_1}, p_2^{\alpha_2}, \dots, p_h^{\alpha_h}$, et, d'autre part, que la fonction d'Euler a pour expression générale

$$\varphi(N) = \varphi(p_1^{\alpha_1} p_2^{\alpha_2} \dots p_h^{\alpha_h}) = \varphi(p_1^{\alpha_1}) \varphi(p_2^{\alpha_2}) \dots \varphi(p_h^{\alpha_h}) = N \prod_{i=1}^h \left(1 - \frac{1}{p_i}\right).$$

Le groupe cyclique d'ordre N est isomorphe au groupe G engendré par une rotation a de $\frac{2\pi}{N}$ autour d'un point O du plan. Soit A_0 un point

(1) Nous reviendrons sur cette propriété lorsque nous aurons introduit la notion de produit direct de deux groupes (t. II).

distinct de O : nous pouvons représenter les différentes rotations de G par les points $A_0, A_1, \dots, A_{N-1}$ en lesquels elles transforment A_0 , et qui sont les sommets d'un polygone régulier convexe de N côtés. Si maintenant nous regardons G comme engendré par l'élément a^n , où n est premier à N , G se trouve représenté par le polygone régulier de N côtés obtenu en joignant les points A_i de n en n . Comme les polygones correspondant aux entiers n et $N - n$ coïncident, le nombre des polygones réguliers distincts de N côtés est égal à $\frac{1}{2} \varphi(N)$. C'est ainsi qu'il y a 2 pentagones, 1 hexagone, 3 heptagones, ..., 2 dodécagones réguliers.

Un groupe G , *fini et d'ordre premier*, n'admet pas de sous-groupes autres que G et le sous-groupe (e) : un tel groupe est, par conséquent, cyclique et abélien ; il est engendré par l'un quelconque des éléments différents de e .

Inversement, tout groupe G qui n'admet aucun sous-groupe véritable et qui ne se réduit pas à l'élément-unité, est cyclique, donc abélien, fini et d'ordre premier. Soit, en effet, a un élément de G distinct de l'élément-unité. Le groupe cyclique (a) est nécessairement égal à G . Si $G = (a)$ était infini, le groupe cyclique (a^2) , distinct de (a) et ne se réduisant pas à (e) , serait un sous-groupe véritable de G , contrairement à l'hypothèse, G est donc fini, et son ordre est nécessairement premier d'après le théorème 1.

Exercices. — 1. Tout groupe fini d'ordre inférieur à 6 est abélien.

2. Si G est un groupe cyclique d'ordre N et si N' est un diviseur de N , G admet un seul sous-groupe d'ordre N' .

3. Établir la formule ⁽¹⁾

$$\sum_{n \mid N} \varphi(n) = N.$$

4. Soit p un nombre premier. Les classes résiduelles modulo p qui sont différentes de zéro : $1, 2, \dots, p-1$, forment un groupe par rapport à la multiplication. En déduire le *théorème de Fermat* :

Pour tout élément x de l'anneau des entiers, on a

$$x^p \equiv x \pmod{p}.$$

⁽¹⁾ Il sera commode d'utiliser l'exercice précédent. On pourra aussi consulter : L. DIRICHLET, *Vorlesungen über Zahlentheorie*, p. 24-26.

§. Groupes intransitifs. Substitutions, cycles, transpositions. —

Soit G un groupe intransitif de transformations d'un ensemble E . Considérons particulièrement un élément a de E , et désignons par H_a le sous-groupe formé par les transformations de G qui laissent a invariant. Appelons éléments G -conjugués de a les éléments qui appartiennent à la même classe de transitivité A que a , par rapport à G , donc les éléments σa où $\sigma \in G$. Nous avons la proposition suivante :

THÉOREME 1. — *Les éléments G -conjugués de a correspondent biunivoquement aux classes à gauche de G par rapport à H_a . Leur nombre, s'il est fini (ce qui a lieu nécessairement quand l'ensemble E lui-même est fini), est égal à l'index de H_a dans G .*

La condition $\sigma a = \tau a$ pour que deux transformations σ et τ de G transforment a en un même élément, s'écrit

$$\sigma^{-1}\tau a = a, \quad \text{c'est-à-dire} \quad \sigma^{-1}\tau \in H_a,$$

d'où

$$\tau \in \sigma H_a,$$

ce qui exprime que σ et τ appartiennent à la même classe à gauche par rapport à H_a . Le théorème en résulte.

Supposons l'ensemble E fini, et soit h le nombre de ses éléments. Une substitution σ opérant dans cet ensemble engendre un groupe cyclique fini Σ , d'ordre m , diviseur de l'ordre $N = h!$ du groupe symétrique.

Appelons *équivalence de transitivité de la substitution* σ et désignons par $\mathfrak{S}_\sigma$ l'équivalence de transitivité du groupe cyclique Σ : nous avons donc

$$x \equiv y \quad (\mathfrak{S}_\sigma)$$

s'il existe un entier n tel que $y = \sigma^n x$, et seulement dans ce cas.

L'équivalence $\mathfrak{S}_\sigma$ décompose l'ensemble E en un certain nombre de classes $A, B, \dots, L$ nommées *systèmes circulaires* associés à la substitution σ .

Considérons l'un de ces systèmes circulaires, A , et soit m_A son ordre, c'est-à-dire le nombre de ses éléments $a_1 = a, a_2, \dots, a_{m_A}$. Si nous désignons par H_a le sous-groupe de Σ qui laisse invariant l'élément a , m_A est, d'après le théorème précédent, égal à l'index de H_a dans Σ . Par conséquent, l'ordre d'un système circulaire A correspondant à la substitution σ divise l'ordre m de cette substitution : $m_A \mid m$.

Pour que le système circulaire A se compose d'un seul élément a , il

faut et il suffit que l'on ait $H_\sigma = \Sigma$, donc que α soit invariant par Σ , ou, ce qui revient au même, par la substitution σ

$$\sigma\alpha = \alpha.$$

Pour déterminer pratiquement le système circulaire A auquel appartient un élément donné α de E , il suffit de former les transformés successifs de α par les puissances de σ

$$\alpha_1 = \sigma^0 \alpha = \alpha, \quad \alpha_2 = \sigma \alpha, \quad \dots, \quad \alpha_{h+1} = \sigma^h \alpha, \quad \dots, \quad \alpha_{m_A} = \sigma^{m_A-1} \alpha.$$

Exemple. — L'équivalence de transitivité de la substitution

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 1 & 3 & 2 \end{pmatrix}$$

décompose l'ensemble $E = \{1, 2, 3, 4, 5\}$ en deux systèmes circulaires : $\{1, 4, 3\}$ et $\{2, 5\}$, d'ordres 3 et 2. Le groupe cyclique Σ engendré par σ est d'ordre 6. Le sous-groupe H_1 laissant 1 invariant se compose de $e = \sigma^0$ et de σ^3 , il est d'ordre 2; le sous-groupe H_2 laissant 2 invariant se compose de e, σ^2, σ^4 ; il est d'ordre 3.

Définition. — Une substitution γ admettant un seul système circulaire A d'ordre μ supérieur à l'unité est appelée *cycle*. Nous avons, d'après cette définition,

$$\gamma x = x \quad \text{pour tout } x \in E - A,$$

tandis que, pour deux éléments a, a' de A , il existe un entier ν (qu'on peut prendre positif ou nul puisque la substitution γ est d'ordre fini) tel que l'on ait

$$a' = \gamma^\nu a.$$

A , comprenant μ éléments distincts, se compose nécessairement des éléments

$$a_1 = a = \gamma^0 a, \quad a_2 = \gamma a, \quad \dots, \quad a_\mu = \gamma^{\mu-1} a$$

deux à deux différents, tandis qu'on a $\gamma^\mu a = a$ et, plus généralement, $\gamma^\mu x = x$ pour tout $x \in A$, donc aussi pour tout $x \in E$: μ est égal à l'ordre m de γ ,

$$\mu = m.$$

Les éléments $a_1, \dots, a_m$ sont *permutés circulairement* par γ ; on représente le cycle γ par la notation

$$\gamma = (a_1, a_2, \dots, a_m).$$

On a

$$(a_1, a_2, \dots, a_m) = (a_2, a_m, \dots, a_1) = \dots$$

On donne le nom de *transpositions* aux cycles d'ordre 2.

Remarque. — Soit τ une substitution quelconque, opérant dans le même ensemble E que γ ; la substitution

$$\gamma' = \tau \gamma \tau^{-1}$$

appelée transformée du cycle γ par τ , est encore un cycle. Posons, en effet, $\tau A = B$. Si $y \in E - B$, on a $\tau^{-1}y = x \in E - A$ d'où $\gamma' y = y$. Si $b, b' \in B$, les éléments $a = \tau^{-1}b$ et $a' = \tau^{-1}b'$ appartiennent à A , d'où $a' = \gamma^v a$, puis $b' = \gamma'^v b$, puisque $\gamma'^v = \tau \gamma^v \tau^{-1}$.

THÉOREME 2. — Toute substitution σ est le produit de cycles $\gamma_A, \gamma_B, \dots, \gamma_L$, deux à deux permutables, correspondant aux différents systèmes circulaires qui lui sont associés

$$\sigma = \gamma_A \gamma_B \dots \gamma_L.$$

L'ordre m de σ est égal au p. p. c. m. μ des ordres $m_A, m_B, \dots, m_L$ de ces différents cycles.

Soit γ_A la substitution définie à partir du système circulaire A par les égalités

$$\begin{aligned} (1) \quad & \gamma_A x = x \quad \text{si } x \in E - A, \\ (1') \quad & \gamma_A a = \sigma a \quad \text{si } a \in A. \end{aligned}$$

Si a et a' appartiennent à A , il existe un entier v tel que l'on ait

$$a' = \sigma^v a,$$

d'où, d'après (1'),

$$(2) \quad a' = \gamma_A^v a.$$

Des relations (1) et (2) résulte que A est un système circulaire pour γ_A , et que γ_A est un cycle d'ordre m_A permutant les éléments de A .

Soient de même $\gamma_B, \dots, \gamma_L$ les cycles définis à partir des systèmes circulaires $B, \dots, L$. Posons

$$\tau = \gamma_A \gamma_B \dots \gamma_L.$$

Un élément $x \in E$ appartient à l'un des systèmes circulaires $A, B, \dots, L$ et à un seul, soit par exemple $x \in D$. Nous avons, d'après (1) et (1'),

$$\tau x = \gamma_D x = \sigma x \quad \text{et, par suite,} \quad \tau = \sigma.$$

D'autre part, A et B étant disjoints, les cycles γ_A, γ_B , par exemple, sont permutables. On a, par conséquent,

$$\sigma^i = \gamma_A^i \gamma_B^i \dots \gamma_L^i.$$

Enfin, les relations

$$m_A \mid m, \quad m_B \mid m, \quad \dots, \quad m_L \mid m$$

entraînent, en désignant par μ le p. p. c. m. des ordres $m_A, m_B, \dots, m_L$ des cycles A, B, ..., L,

$$\mu \mid m.$$

Or, nous avons

$$\sigma^\mu = \gamma_A^\mu \gamma_B^\mu \dots \gamma_L^\mu = e,$$

donc

$$m \mid \mu \quad \text{et, par conséquent,} \quad m = \mu.$$

Considérons maintenant un *groupe de substitutions* G opérant dans l'ensemble E. Nous avons la proposition suivante :

THÉOREME 3. — *L'équivalence de transitivité $\mathfrak{T}$ d'un groupe de substitutions G est le produit (transitif) $\mathfrak{X}$ des équivalences de transitivité des différentes substitutions de G.*

1° On a $\mathfrak{T} \subseteq \mathfrak{X}$. — La relation

$$a' \equiv a \quad (\mathfrak{T}), \quad \text{c'est-à-dire} \quad a' = \sigma a \quad (\sigma \in G)$$

entraîne, en effet,

$$a' \equiv a \quad (\mathfrak{T}_\sigma), \quad \text{donc} \quad a' \equiv a \quad (\mathfrak{X}).$$

2° On a $\mathfrak{X} \subseteq \mathfrak{T}$. — Soit

$$a' \equiv a \quad (\mathfrak{X}).$$

Il existe, dans E, n éléments $a_1 = a, a_2, \dots, a_n = a'$ et, dans G, $n - 1$ substitutions σ_i tels que l'on ait

$$a_i \equiv a_{i+1} \quad (\mathfrak{T}_{\sigma_i}), \quad \text{c'est-à-dire} \quad a_i = \sigma_i^{m_i} a_{i+1} \quad (i = 1, 2, \dots, n - 1; \sigma_i \in G).$$

Si nous posons

$$\sigma = \sigma_1^{m_1} \sigma_2^{m_2} \dots \sigma_{n-1}^{m_{n-1}},$$

nous avons

$$a = \sigma a', \quad \text{avec} \quad \sigma \in G,$$

donc

$$a \equiv a' \quad (\mathfrak{T}) \quad \text{et, par suite,} \quad \mathfrak{X} \subseteq \mathfrak{T}.$$

De la décomposition d'une substitution en cycles, on passe aisément à la décomposition en *produit de transpositions*. En effet, la relation ⁽¹⁾

$$(a_1, a_2, \dots, a_k) = (a_1, a_2)(a_2, a_3) \dots (a_{k-1}, a_k)$$

exprime qu'un cycle d'ordre k est le produit de $k - 1$ transpositions.

⁽¹⁾ Rappelons que le produit $\sigma_m \dots \sigma_2 \sigma_1$ désigne la substitution qui consiste à effectuer d'abord σ_1 , puis σ_2 , ..., et enfin σ_m .

On peut aller plus loin en ordonnant l'ensemble E. Supposons, par exemple, que E soit indexé par l'ensemble des n premiers entiers. L'égalité, facile à vérifier,

$$\begin{aligned}(a_h, a_{h+t}) &= (a_{h+t-1}, a_{h+t})(a_{h+t-2}, a_{h+t-1}) \\ &\dots (a_{h+1}, a_{h+2})(a_h, a_{h+1})(a_{h+1}, a_{h+2}) \\ &\dots (a_{h+t-2}, a_{h+t-1})(a_{h+t-1}, a_{h+t}),\end{aligned}$$

prouve que toute transposition est le produit de transpositions permutant des éléments consécutifs. Nous avons donc finalement la proposition suivante :

Dans un ensemble fini et ordonné E, toute substitution est le produit de transpositions portant sur des éléments consécutifs.

Dans l'ensemble des n premiers entiers, une substitution σ conserve ou change le signe du produit

$$P = \prod_{i < j} (i - j) \quad (i = 1, 2, \dots, n-1; j = 2, 3, \dots, n).$$

Dans le premier cas, σ est dite *paire*; dans le second, *impaire*. Le produit de deux substitutions paires ou de deux substitutions impaires est une substitution paire; le produit d'une substitution paire par une substitution impaire est une substitution impaire.

Toute transposition est impaire, car, si dans le produit P on permute i et j , le facteur $(i - j)$, ainsi que tous les facteurs $(i - k)$ et $(k - j)$ ($k = i + 1, \dots, j - 1$) changent de signe. Au total, P change de signe. Par suite, dans la décomposition d'une substitution en produit de transpositions, la parité du nombre de transpositions est déterminée : toute substitution paire est le produit d'un nombre pair de transpositions. *Les substitutions paires forment un groupe A_n , appelé groupe alterné*, sous-groupe du groupe symétrique S_n , c'est-à-dire du groupe de toutes les substitutions de E.

S_n est d'ordre $n!$ Comme le produit d'une transposition fixe par une substitution impaire est une substitution paire et inversement, il y a autant de substitutions paires que de substitutions impaires : l'ordre du groupe alterné est, par suite, $\frac{1}{2}n!$: son index dans le groupe symétrique est 2.

THÉORÈME 4. — 1° *Le groupe symétrique S_n est engendré par les $n-1$ transpositions $(1, 2), (1, 3), \dots, (1, n)$.*

2° Le groupe alterné A_n est engendré par les $n - 2$ cycles $(1, 2, 3)$, $(1, 2, 4)$, ..., $(1, 2, n)$.

Si i et j sont différents de 1, on a

$$(i, j) = (1, j)(1, i)(1, j).$$

Le groupe engendré par les transpositions $(1, 2)$, $(1, 3)$, ..., $(1, n)$ contient donc toute transposition et coïncide avec le groupe symétrique.

Les cycles

$$(2) \quad (1, 2, i) = (1, i)(1, 2) \quad (i \neq 1, 2)$$

sont des substitutions paires : ils engendrent donc un sous-groupe A'_n du groupe alterné. Inversement, toute substitution $\sigma \in A_n$ est de la forme

$$\sigma = \tau_1 \tau_2 \dots \tau_{2\nu-1} \tau_{2\nu},$$

où les τ_i sont des transpositions. En posant $\alpha = (1, 2)$, nous pouvons écrire

$$\sigma = \tau_1 \alpha \tau_2 \dots \tau_{2\nu-1} \alpha \tau_{2\nu}.$$

Or, on voit, d'après la formule (2), celle qui s'en déduit en prenant les inverses des deux membres et les formules

$$(2') \quad \begin{cases} (2, i)(1, 2) = (i, 2, 1) = (1, 2, i)^{-1}, \\ (1, 2)(i, j) = (i, j)(1, 2) = (1, 2, j)(i, 2, 1)(1, 2, j) \\ \quad = (1, 2, j)(1, 2, i)^{-1}(1, 2, j) \quad (i \text{ et } j \neq 1 \text{ et } 2), \end{cases}$$

que le produit à droite ou à gauche d'une transposition quelconque par α appartient à A'_n . Nous avons donc

$$\sigma \in A'_n \quad \text{et} \quad A'_n = A_n.$$

Exercices. — 1. Décomposer en cycles la substitution

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 6 & 7 & 5 & 4 & 2 & 1 \end{pmatrix}.$$

Cette substitution appartient-elle au groupe alterné A_7 ?

2. A quelle condition le cycle $(1, 2, 3, \dots, m)$ est-il une substitution paire ?

C. — ÉQUIVALENCES RÉGULIÈRES DANS UN GROUPE.

6. **Sous-groupes invariants.** — Considérons une équivalence régulière $\mathcal{R}$ dans un groupe G ; soit S le sous-groupe constitué par la classe-unité. La classe A modulo $\mathcal{R}$ qui contient l'élément a de G vérifie,

d'après les résultats du paragraphe 3 et, puisque $\mathcal{R}$ est régulière aussi bien à droite qu'à gauche, la double égalité

$$A = S a = a S.$$

Le sous-groupe S est donc permutable avec tout élément a de G . Tout sous-groupe ayant cette propriété est appelé *sous-groupe invariant* de G ⁽¹⁾. Nous avons, par conséquent, la proposition suivante :

THÉOREME 1. — *Dans toute décomposition régulière d'un groupe G , la classe-unité S est un sous-groupe invariant de G . Les autres classes sont les complexes $S a = a S$.*

L'équivalence $\mathcal{R}$ étant régulière, l'ensemble-quotient $G/\mathcal{R}$ est un groupoïde homomorphe à G (§ 2, p. 145), donc un groupe (p. 148).

Ce groupe-quotient, appelé aussi *groupe-facteur*, est ordinairement représenté par la notation G/S .

Inversement, donnons-nous un *sous-groupe invariant* S de G . D'après l'égalité

$$S a = a S \quad \text{pour tout } a \in G,$$

l'équivalence régulière à droite associée à S , dans laquelle les classes sont les complexes $S a$ distincts, et l'équivalence régulière à gauche, dans laquelle les classes sont les complexes $a S$, sont confondues, et nous avons par conséquent la proposition suivante :

THÉOREME 2. — *A tout sous-groupe invariant S de G est associée une équivalence régulière $\mathcal{R}$, telle que S soit la classe-unité modulo $\mathcal{R}$ et que les autres classes soient les complexes $S a = a S$ distincts.*

Il en résulte qu'à tout sous-groupe invariant S est associé un *groupe-quotient* $G/\mathcal{R} = G/S$, homomorphe à G .

Les propriétés précédentes expriment que, dans un groupe G , il y a correspondance biunivoque entre les équivalences régulières et les sous-groupes invariants. Ceux-ci peuvent encore être définis comme les sous-groupes pour lesquels la décomposition en classes à droite et la décomposition en classes à gauche coïncident.

La condition

$$(1) \quad a S = S a \quad \text{pour tout } a \in G,$$

⁽¹⁾ Parfois aussi, sous-groupe *distingué*, sous-groupe *normal* (en allemand, Normalteiler).

pour que le sous-groupe S soit invariant, peut encore s'écrire

$$(1') \quad aSa^{-1} = S \quad \text{pour tout } a \in G.$$

Sous cette forme, elle exprime que le *complexe transformé de S par l'élément a* , aSa^{-1} , coïncide avec S quel que soit a . Or, pour qu'il en soit ainsi, il *suffit* que le transformé asa^{-1} de chaque élément s de S appartienne à S , quel que soit $a \in G$, c'est-à-dire que l'on ait

$$aSa^{-1} \subseteq S \quad \text{pour tout } a \in G.$$

Cette dernière condition entraîne, en effet, en remplaçant a par a^{-1}

$$a^{-1}Sa \subseteq S, \quad \text{c'est-à-dire } S \subseteq aSa^{-1},$$

d'où

$$aSa^{-1} = S \quad \text{pour tout } a \in G.$$

Remarque. — L'invariance d'un sous-groupe S n'est pas une propriété intrinsèque de S , mais concerne à la fois ce sous-groupe et le groupe G qui le contient : invariant dans G , S peut très bien ne plus l'être dans un groupe G_1 contenant G . Mais S est invariant dans tout groupe H compris entre G et S .

Exemples. — 1. Tout sous-groupe d'un groupe abélien en est sous-groupe invariant.

2. Dans un groupe G , un sous-groupe H d'index égal à 2 est nécessairement invariant. Si, en effet, nous décomposons G en classes à droite ou en classes à gauche par rapport à H , nous obtenons, dans les deux cas, les classes H et $G - H$ et les deux décompositions coïncident. En particulier, le groupe alterné A_n est sous-groupe invariant du groupe symétrique S_n .

3. Le groupe de Klein V_4 est sous-groupe invariant du groupe symétrique S_4 , ou du groupe alterné A_4 . Montrons que $\alpha \in V_4$ et $\sigma \in S_4$ entraînent $\sigma\alpha\sigma^{-1} \in V_4$, ce qui est évident pour $\alpha = e$. La substitution $\alpha (\neq e)$ est involutive, $\alpha^2 = e$, il en est de même de $\sigma\alpha\sigma^{-1}$. D'autre part, $\sigma\alpha\sigma^{-1}$ ne laisse aucun élément invariant, car $\sigma\alpha\sigma^{-1}x = x$ entraînerait $\alpha(\sigma^{-1}x) = \sigma^{-1}x$, or α ne laisse aucun élément invariant. Par suite, $\sigma\alpha\sigma^{-1}$, permutant le chiffre 1 avec un des chiffres 2, 3, 4, échange également les deux autres chiffres et, par conséquent, appartient à V_4 . Les substitutions de V_4 étant paires, nous avons $V_4 \subseteq A_4$ et V_4 est également sous-groupe invariant de A_4 .

Remarque. — Dans l'ensemble des classes à droite Sa (par exemple) par rapport à un sous-groupe S qui n'est pas invariant, on peut définir une *opération multiforme*, par rapport à laquelle l'ensemble-quotient $G/\mathcal{R}_S$ est ce qu'on appelle un *hypergroupe* ⁽¹⁾.

(1) Cette notion a été introduite par F. MARTY, *Sur une généralisation de la notion de Groupe* (8^e Congrès des Mathématiciens scandinaves, Stockholm, 1934, p. 45-49);

Un *hypergroupe* H est, par définition, un ensemble non vide dans lequel :

1° Est définie une *opération multiforme* : à chaque couple a, b d'éléments de H est associé un *complexe* de H , désigné par ab . A et B étant deux complexes, on pose

$$AB = \bigcup_{a \in A, b \in B} ab.$$

(On écrit aB quand $A = \{a\}$.)

2° Cette opération est *associative* : $a(bc) = (ab)c$ (les ensembles figurant aux deux membres coïncident).

3° Pour tout $a \in H$, on a

$$aH = Ha = H.$$

On remarquera que cette dernière condition rappelle et remplace la propriété d'existence des quotients : elle signifie en effet que, si $b \in H$, il existe x tel que $b \in ax$ et y tel que $b \in ya$.

Cela posé, soit S un sous-groupe (quelconque) d'un groupe G . Le produit d'un élément sa de la classe à droite $Sa = A$, par un élément sb de la classe $Sb = B$ (produit effectué dans G), appartient au complexe $S.aSb$, qui est une *réunion de classes à droite* :

$$S.aSb = \bigcup_{s \in S} S(asb).$$

Sur les groupes et hypergroupes attachés à une fraction rationnelle (*Ann. Éc. Norm. Sup.*, t. 53, 1936, p. 83-123). Elle a été étudiée également, sous le nom de *multigroupe*, par O. ORE, *Structures and Group theory* (*Duke Math. J.*, t. 3, 1937, p. 149-174).

Voir également M. DRESHER-O. ORE, *Theory of multigroups* (*Amer. J. Math.*, t. 60, 1938, p. 705-733); H. S. WALL, *Hypergroups* (*Amer. J. Math.*, t. 59, 1937, p. 77); J. KUNTZMANN, *Opérations multiformes, hypergroupes* (*C. R. Acad. Sc.*, t. 204, 1937, p. 1787) et *Contribution à l'étude des systèmes multiformes* (*Ann. Fac. Sc. Toulouse*, 1939, p. 190), et plus particulièrement l'exposé d'ensemble de M. KRASNER, *Loi de Jordan-Hölder dans les hypergroupes* (*Duke Math. J.*, t. 6, 1940, p. 120-140), qui, dans tous ses travaux, a beaucoup utilisé cette notion.

Le paragraphe III du Mémoire, cité plus haut, de A. CHÂTELET (*Algèbre des relations de congruences*, *Ann. Éc. Norm. Sup.*, t. 64, 1947, p. 339), est consacré aux hypergroupes.

En considérant le cas où deux éléments ne sont pas nécessairement composables R. CROISOT a introduit la notion plus générale d'*hypergroupe partiel* (Cf. *Hypergroupes partiels*, *C. R. Acad. Sc.*, t. 228, 1949, p. 1090; *Algèbres de relations et hypergroupes partiels*, *ibid.*, p. 1181).

En posant $A.B = S a S b$, nous définissons, dans l'ensemble $\mathcal{H}$ des classes à droite, une *multiplication multiforme*.

Puisqu'on a

$$A.B = \{s_1 a s_2 b\}_{s_1 \in S, s_2 \in S}$$

cette multiplication des classes est *associative* :

$$A.(B.C) = \{s_1 a s_2 b s_3 c\}_{s_1, s_2, s_3 \in S} = (A.B).C.$$

Enfin, la condition 3° est vérifiée aussi. Soient A et B deux classes, a un élément de A, b un élément de B. Posons $x = a^{-1}b$, et soit X la classe modulo $\mathcal{R}_S$ qui contient x . Comme $b = ax$, nous avons

$$B = S b = S a e x, \quad \text{où } e \in S,$$

donc

$$B \in A.X.$$

On voit, de même, en appelant Y la classe contenant $y = b a^{-1}$, que

$$B \in Y.A.$$

L'ensemble $\mathcal{H}$ des classes à droite est donc bien un hypergroupe.

Soit Z le *centre* d'un groupe G, c'est-à-dire l'ensemble des éléments z qui sont permutable avec chaque élément de G

$$(2) \quad zx = xz \quad \text{pour tout } x \in G.$$

La relation (2) entraîne

$$xz^{-1} = z^{-1}x \quad \text{pour tout } x \in G,$$

donc $z^{-1} \in Z$; d'autre part, le produit $z_1 z_2$ de deux éléments de Z appartient aussi à Z. Par conséquent, le centre Z est un *sous-groupe* de G, évidemment *abélien*, et *invariant dans* G, puisque l'égalité (2) entraîne

$$Zx = xZ \quad \text{pour tout } x \in G.$$

Tout sous-groupe Z' du centre est également sous-groupe invariant de G. Pour que G soit abélien, il faut et il suffit que l'on ait $Z = G$.

Un groupe non abélien dont tout sous-groupe est invariant est dit *hamiltonien* ⁽¹⁾.

Un groupe G qui n'admet pas de sous-groupes invariants autre que G et $E = \{e\}$ est dit *simple*.

(1) Cf. H. ZASSENHAUS, *Lehrbuch der Gruppentheorie*, I, chap. IV, § 6, p. 123.

THÉOREME. — Pour $n > 4$, le groupe alterné A_n est simple.

Soit N un sous-groupe invariant de A_n . Remarquons d'abord que, si un cycle d'ordre 3 appartient à N , on a $N = A_n$. Soit, en effet, avec des notations convenables,

$$\alpha = (1, 2, 3) \in N.$$

Le transformé de α par la substitution *paire*

$$\pi = (1, 2)(3, k) = \pi^{-1} \quad (k \neq 1, 2, 3)$$

appartient à N

$$\beta = \pi\alpha\pi^{-1} = (2, 1, k) \in N, \quad \text{d'où} \quad \beta^2 = (1, 2, k) \in N,$$

N contient donc tous les cycles de la forme $(1, 2, k)$ ($k = 3, \dots, n$); or, ceux-ci engendrent A_n (§ 5, th. 4, p. 163) : nous avons donc bien $N = A_n$.

Cela posé, soit τ une des substitutions de N , supposé $\neq E$, qui, étant distinctes de l'unité, laissent invariants le plus grand nombre de chiffres : dans la décomposition de τ en cycles, tous les cycles ont le même ordre, car si τ comprenait un cycle d'ordre m et un d'ordre n ($m < n$), τ^m serait une substitution de N distincte de l'unité et laissant au moins m chiffres invariants de plus que τ . Il suffit d'établir que τ est un cycle d'ordre 3. Or τ , étant une substitution paire, ne peut pas être une transposition. Montrons donc qu'il y a contradiction si τ transforme effectivement quatre chiffres au moins, par exemple 1, 2, 3, 4,

La substitution τ est le produit, ou bien de cycles d'ordre 2, par exemple

$$(3) \quad \tau = (1, 2)(3, 4) \dots$$

ou bien de cycles d'un même ordre supérieur à 2, par exemple

$$(4) \quad \tau = (1, 2, 3, \dots) \dots$$

Dans ce second cas, comme τ ne peut pas être égal au cycle $(1, 2, 3, 4)$ qui est une substitution impaire, il y a encore au moins un chiffre, par exemple le chiffre 5, qui figure nécessairement dans la décomposition de τ en cycles. Il en est de même dans le premier cas, sauf si l'on a

$$\tau = (1, 2)(3, 4).$$

Posons $\sigma = (3, 4, 5)$ et $\tau_1 = \sigma\tau\sigma^{-1}$; σ étant paire, nous avons $\tau_1 \in N$ et, dans le premier cas

$$(3') \quad \tau_1 = (1, 2)(4, 5) \dots \neq \tau,$$

dans le second

$$(4') \quad \tau_1 = (1, 2, 4, \dots) \dots \neq \tau,$$

donc

$$\tau^{-1}\tau_1 \neq 1 \quad \text{et} \quad \tau^{-1}\tau_1 \in N.$$

Donc, si τ n'est pas égal à $(1, 2)(3, 4)$, tout chiffre *invariant* par τ , étant supérieur à 5, est invariant par σ , donc aussi par τ_1 et par $\tau^{-1}\tau_1$. Or, $\tau^{-1}\tau_1$ laisse invariant en outre le chiffre 1; nous avons donc dans N une substitution laissant invariant un chiffre de plus que τ , ce qui est absurde. Si enfin $\tau = (1, 2)(3, 4)$, on a

$$\tau^{-1}\tau_1 = (1, 2)(3, 4)(1, 2)(4, 5) = (3, 4, 5) \in N$$

qui, encore, laisse invariant un chiffre de plus que τ ; le théorème est, par conséquent, établi.

L'intersection et le produit de deux équivalences régulières étant des équivalences régulières, *l'intersection et la réunion complète de deux sous-groupes invariants sont des sous-groupes invariants*. D'autre part, un sous-groupe invariant est, d'après (1), permutable avec un complexe quelconque, par conséquent *la réunion complète de deux sous-groupes invariants S_1, S_2 n'est autre que le produit $S_1 S_2 = S_2 S_1$ et celui-ci est un sous-groupe invariant de G* .

Les sous-groupes invariants d'un groupe G forment donc un treillis $\mathfrak{G}$, dans lequel la relation d'inclusion et l'intersection ont la même signification qu'en Théorie des Ensembles; l'union est la réunion complète et le produit. $\mathfrak{G}$ satisfait d'ailleurs aux deux conditions de Moore : a. $G \in \mathfrak{G}$; b. l'intersection I d'une famille $\mathfrak{F}$ de sous-groupes invariants est un sous-groupe invariant ($e \in I \neq \emptyset$), $\mathfrak{G}$ est donc un treillis complet.

L'union ou groupe composé des sous-groupes invariants S de $\mathfrak{F}$ est l'ensemble $\prod_{S \in \mathfrak{F}} S$ des produits d'un nombre fini (variable, quelconque)

d'éléments de G appartenant à des groupes S de la famille $\mathfrak{F}$; $\prod_{S \in \mathfrak{F}} S$ est,

en effet, un groupe contenant chaque $S \in \mathfrak{F}$, et c'est évidemment le plus petit (Cf. chap. III, § 5, th. 3, p. 116). La multiplication des sous-groupes invariants, coïncidant avec l'union du treillis correspondant, est une opération associative, commutative et idempotente.

Le treillis $\mathfrak{G}$ possède encore une propriété remarquable, plus faible

que la distributivité ⁽¹⁾. Remarquons d'abord que, dans tout treillis T , la relation

$$x \subseteq z \quad \text{entraîne} \quad x \cup (y \cap z) \subseteq (x \cup y) \cap z,$$

quel que soit $y \in T$, car on a $y \cap z \subseteq y$, d'où $x \cup (y \cap z) \subseteq x \cup y$; d'autre part, de l'hypothèse $x \subseteq z$ et de $y \cap z \subseteq z$, résulte $x \cup (y \cap z) \subseteq z$; on a donc bien

$$x \cup (y \cap z) \subseteq (x \cup y) \cap z.$$

Cela posé, un treillis est dit *modulaire* si

$$x \subseteq z \quad \text{entraîne} \quad x \cup (y \cap z) = (x \cup y) \cap z.$$

Cette propriété se conserve par dualité; de plus, tout sous-treillis d'un treillis modulaire est modulaire. Il est clair que tout treillis distributif est modulaire. Notons aussi que l'égalité *modulaire*

$$(5) \quad x \cup (y \cap z) = (x \cup y) \cap z \quad (x \subseteq z)$$

est vérifiée d'une façon évidente dans les cas suivants : 1° $x = z$, alors, les deux membres de (5) sont égaux à z ; 2° $z = u$, élément universel de T (s'il existe) : alors les deux membres de (5) sont égaux à $x \cup y$; 3° $x = o$, élément nul de T (s'il existe) : alors, les deux membres de (5) sont égaux à $y \cap z$. Il en résulte que le treillis de cinq éléments défini par le diagramme ci-dessous, est *modulaire*; il n'est *pas distributif*

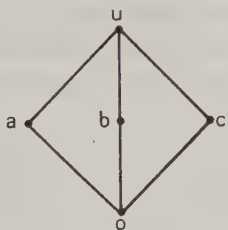


Fig. 8.

car $a \cup (b \cap c) = a \cup o = a$, tandis que $(a \cup b) \cap (a \cup c) = u \cap u = u$.

THÉORÈME 3. — *Tout treillis $\mathfrak{G}$ de sous-groupeïdes d'un groupeïde G , vérifiant les conditions suivantes :*

α. Tout sous-groupeïde $X \in \mathfrak{G}$ est unitaire (chap. II, § 6, p. 92);

⁽¹⁾ R. DEDEKIND, *Über die von drei Moduln erzeugte Dualgruppe*, (*Math. Ann.*, t. 53, 1900, p. 371; *Ges. Werke*, t. 2, p. 236). Les treillis modulaires ont aussi été appelés *structures de Dedekind*.

β. L'union $X \cup Y$ de deux sous-groupoïdes de $\mathfrak{G}$ coïncide avec leur produit

$$X \cup Y = X.Y$$

est un treillis modulaire.

Soient X, Y, Z trois sous-groupoïdes, éléments de $\mathfrak{G}$; nous supposons $X \subseteq Z$; pour prouver l'égalité modulaire (5), il suffit d'établir la relation

$$(X \cup Y) \cap Z \subseteq X \cup (Y \cap Z).$$

Soit donc $a \in (X \cup Y) \cap Z$. Nous avons, en tenant compte de β,

$$a = xy = z, \quad \text{où } x \in X, \ y \in Y, \ z \in Z.$$

Or, puisque X est contenu dans Z , x appartient à Z , qui, d'après α, est unitaire : il en résulte

$$y \in Z, \quad \text{d'où } y \in Y \cap Z$$

et

$$a = xy \in X.(Y \cap Z) = X \cup (Y \cap Z),$$

ce qu'il fallait démontrer.

COROLLAIRE (Dedekind). — *Le treillis des sous-groupes invariants d'un groupe G est modulaire; en particulier, le treillis des sous-groupes d'un groupe abélien est modulaire* (1).

THÉORÈME 4. — *Soit G' un sous-groupe d'un groupe G . Si G'' est un sous-groupe invariant de G' et si S désigne un sous-groupe quelconque de G , $G'' \cap S$ est un sous-groupe invariant de $G' \cap S$.*

(1) Dans le même ordre d'idées, mentionnons un théorème dû à O. ORE (*Structures and Group theory*, II, *Duke Math. J.*, t. 4, 1938, p. 247) : *pour que le treillis des sous-groupes d'un groupe G soit distributif, il faut et il suffit que G soit un groupe cyclique généralisé, c'est-à-dire que deux éléments quelconques a, b de G soient toujours puissances d'un élément c de G (dépendant, en général, de a et b). Voir aussi G. BIRKHOFF *Lattice theory*, chap. VI, § 9, p. 96 où l'on trouvera ce théorème avec sa démonstration.*

Considérons alors un groupe abélien qui n'est pas cyclique généralisé, par exemple le produit direct P d'un nombre fini (≥ 2) de groupes cycliques infinis $(a), (b), \dots, (l)$, c'est-à-dire l'ensemble des produits formels $x = a^\alpha b^\beta \dots l^\lambda$ pour lesquels l'égalité n'a lieu que si les exposants correspondants (qui sont des entiers ≥ 0) coïncident, $a, b, \dots, l$ étant de plus permutables. D'après le théorème de Ore que nous venons de citer, le treillis des sous-groupes de P n'est pas distributif : nous avons ainsi un exemple de groupe dont les sous-groupes invariants forment un *treillis modulaire*, mais non distributif.

On trouvera dans *Lattice theory* (exerc. 1, p. 98) des exemples de groupes (non abéliens) dont les sous-groupes forment un treillis non modulaire.

Le transformé xrx^{-1} d'un élément $r \in G' \cap S$ par un élément $x \in G' \cap S$ appartient, en effet, à G'' et à S .

THÉOREME 5. — Soit G'' un sous-groupe invariant d'un groupe G' , lui-même sous-groupe d'un groupe G . Si S est un sous-groupe de G permutable avec chaque élément de G' :

$$xS = Sx \quad \text{pour tout } x \in G',$$

SG'' est un sous-groupe invariant de SG' .

S est permutable avec G' et G'' , donc les complexes SG' , SG'' sont des sous-groupes de G . De plus, SG'' est sous-groupe invariant de SG' , car on a, quel que soit $x = sg' \in SG'$,

$$xSG''x^{-1} = sg'SG''g'^{-1}s^{-1} = sSg'G''g'^{-1}s^{-1} = sSG''s^{-1}.$$

Or,

$$sS = S \quad \text{et} \quad G's^{-1} \subseteq G'S = SG'',$$

d'où

$$xSG''x^{-1} \subseteq SG'' \quad \text{pour tout } x \in SG'$$

et SG'' est, par conséquent, invariant dans SG' .

Exercices. — 1. Si, dans un groupe G , H est le sous-groupe engendré par les éléments c d'un complexe C , il faut et il suffit, pour que H soit invariant, que l'on ait

$$aca^{-1} \in H \quad \text{pour tout } a \in G \text{ et tout } c \in C.$$

En particulier, il suffit que l'on ait

$$aca^{-1} \in C \quad \text{pour tout } a \in G \text{ et tout } c \in C.$$

2. Dans un groupe G , on appelle *commutateur* (ou *commutant*) de deux éléments a , b l'élément $c = aba^{-1}b^{-1}$.

1° Quel est le commutateur de xax^{-1} et de xbx^{-1} ?

2° Montrer que le groupe commutateur G' ou premier dérivé de G , c'est-à-dire le groupe engendré par les commutateurs, est sous-groupe invariant de G ;

3° Le groupe quotient G/G' est abélien;

4° Tout sous-groupe invariant H de G tel que G/H soit abélien contient G' .

5° Si N est un sous-groupe invariant de G , son premier dérivé N' , groupe engendré par les commutateurs d'éléments de N , est aussi sous-groupe invariant de G ⁽¹⁾.

(1) T. SZELE utilise cette propriété pour démontrer le théorème suivant : Si un groupe G possède un sous-groupe parfait, il admet aussi un sous-groupe invariant qui est parfait (et peut d'ailleurs coïncider avec G). Un groupe parfait est un groupe G comprenant plus d'un élément et coïncidant avec son dérivé : $G = G'$, cf. C. R. Acad. Sc., t. 230, 1950.

3. Le groupe des translations T est sous-groupe invariant du groupe des déplacements G . Étudier le groupe-quotient G/T .

4. Soit H le sous-groupe du groupe symétrique S_4 qui laisse invariant un certain élément, par exemple 4. On a, en désignant par V_4 le groupe de Klein,

$$G = H.V_4 \quad \text{et} \quad S_4/V_4 \simeq S_3.$$

5. On considère le groupe de substitutions G de l'ensemble $E = \{1, 2, 3, 4, 5\}$ qui est engendré par les transpositions

$$\alpha = (1, 2), \quad \beta = (1, 3), \quad \gamma = (4, 5).$$

Déterminer son centre Z .

6. Soit G un groupe multiplicatif. H étant un sous-groupe de G , on désignera par $\mathcal{R}_H$ l'équivalence régulière à droite correspondante, définie par

$$x \equiv x_1 \ (\mathcal{R}_H) \quad \text{si et seulement si} \quad x_1 x^{-1} \in H,$$

par ${}_H\mathcal{R}$ l'équivalence régulière à gauche, définie par

$$x \equiv x_2 \ ({}_H\mathcal{R}) \quad \text{si et seulement si} \quad x^{-1} x_2 \in H.$$

1° A deux sous-groupes S, T de G , on associe la relation binaire $\mathcal{B}$ définie dans G par

$$x \mathcal{B} y \quad \text{si et seulement si} \quad y = sxt, \quad \text{où} \quad s \in S, \quad t \in T.$$

Montrer que $\mathcal{B}$ est une relation d'équivalence.

2° Montrer que $\mathcal{B}$ contient les équivalences $\mathcal{R}_S$ et ${}_T\mathcal{R}$, et est la plus fine équivalence ayant cette propriété. Quels que soient les sous-groupes S, T de G , $\mathcal{R}_S$ et ${}_T\mathcal{R}$ sont permutables.

3° Montrer que, si S est sous-groupe invariant de G , $\mathcal{B}$ est régulière à gauche, et décompose G en classes à gauche par rapport à un certain sous-groupe que l'on précisera. Que peut-on dire si T est un sous-groupe invariant, si S et T le sont tous les deux ?

7. Théorème d'homomorphisme (cas des groupes). — Soient G un groupe, $\bar{G}$ un groupoïde homomorphe à G : $\bar{G}$ est également un groupe, comme nous l'avons vu au paragraphe 2. L'équivalence d'homomorphisme $\mathcal{R}$, définie dans G par

$$x \equiv x' \ (\mathcal{R}) \quad \text{si} \quad \bar{x} = \bar{x}'$$

étant régulière, la classe-unité S , ensemble des éléments de G qui ont pour image l'élément unité $\bar{e}$ de $\bar{G}$, est un sous-groupe invariant de G appelé *noyau* de l'homomorphisme, et l'on a, d'après le théorème général du paragraphe 2 (p. 147), l'isomorphisme

$$G/S \simeq \bar{G}$$

entre $\bar{G}$ et le groupe-quotient $G/S = G/\mathcal{R}$.

Telle est la forme que prend le *théorème d'homomorphisme dans le cas des groupes*. Ce théorème montre que la recherche des groupes homomorphes à G et celle des sous-groupes invariants de G sont des problèmes équivalents. Il entraîne aussi que, si G est un groupe fini d'ordre N , tout groupe $\bar{G}$ homomorphe à G a pour ordre un diviseur de N , égal au quotient de N par l'ordre de S , c'est-à-dire à l'index $G:S$ de S dans G .

Exemple. — Si, à tout vecteur $\vec{V}$ de l'espace, nous faisons correspondre sa projection orthogonale $\vec{V}_1$ sur un plan P , le groupe G_1 des vecteurs du plan P par rapport à l'addition géométrique, est homomorphe au groupe G des vecteurs de l'espace. Le sous-groupe (invariant) S des vecteurs auxquels correspond dans G_1 le vecteur nul est l'ensemble des vecteurs perpendiculaires à P .

Remarque. — Lorsqu'un homomorphisme $G \sim \bar{G}$ applique un groupe G sur un sous-groupe invariant $\bar{G}$ d'un groupe G_1 (ce qu'on écrit $G \rightarrow G_1$) on appelle *conoyau* le groupe quotient $G_1/\bar{G}$.

Indiquons une application intéressante du théorème d'homomorphisme aux groupes abéliens finis.

THÉORÈME. — *Si G est un groupe abélien fini d'ordre N et si p est un diviseur premier de N , il existe dans G un élément d'ordre p .*

Soient $a_1, a_2, \dots, a_N$ les éléments de G , $d_1, d_2, \dots, d_N$ leurs ordres respectifs.

Considérons le groupe abélien H engendré par N éléments $x_1, x_2, \dots, x_N$ avec les seules relations fondamentales

$$x_i^{d_i} = e \quad (i = 1, 2, \dots, N),$$

e étant l'élément-unité de H ⁽¹⁾. La correspondance

$$x_1^{m_1} x_2^{m_2} \dots x_N^{m_N} \rightarrow a_1^{m_1} a_2^{m_2} \dots a_N^{m_N}$$

(1) Une réalisation du groupe H peut être obtenue de la manière suivante. Considérons l'ensemble des systèmes

$$S = (m_1, m_2, \dots, m_N) = (m_i)$$

de N entiers m_i vérifiant les inégalités $0 \leq m_i < d_i$, avec, pour ces systèmes, la loi de composition

$$(m_i)(n_i) = (r_i),$$

où r_i est le reste (≥ 0) de la division de $m_i + n_i$ par d_i . Si l'on pose

$$x_1 = (1, 0, \dots, 0), \quad x_2 = (0, 1, \dots, 0), \quad \dots, \quad x_N = (0, 0, \dots, 1), \\ e = (0, 0, \dots, 0),$$

les relations fondamentales sont bien vérifiées et l'on a

$$S = (m_1, m_2, \dots, m_N) = x_1^{m_1} x_2^{m_2} \dots x_N^{m_N}.$$

est un homomorphisme

$$H \sim G.$$

Donc, l'ordre N de G divise l'ordre $d_1 d_2 \dots d_N$ de H . Un diviseur premier p de N divise donc au moins un des d_i , soit par exemple d_1 , et l'élément $a = a_1^{\frac{d_1}{p}}$ est bien d'ordre p .

Exercices. — 1. Le groupe symétrique S_3 est homomorphe au groupe G de l'exercice 5, paragraphe 6. Déterminer le sous-groupe invariant S de G tel que

$$G/S \simeq S_3.$$

2. Dans l'espace à trois dimensions, le groupe R des rotations autour d'un point O est homomorphe au groupe G des déplacements. Quel est le sous-groupe invariant S tel que

$$G/S \simeq R?$$

3. On considère l'anneau des entiers, C , comme un groupe *additif*. Quels sont les groupes homomorphes à C ?

8. Automorphismes intérieurs. — Étant donné un élément a d'un groupe G , considérons l'application α de G en lui-même définie par

$$(1) \quad \alpha x = axa^{-1}.$$

A chaque élément a du groupe G correspond une telle application. La règle de simplification étant valable dans G , α est une application *biunivoque* de G sur lui-même. D'autre part, cette application est *régulière* pour l'opération de G , car on a

$$\alpha(xy) = axya^{-1} = axa^{-1}aya^{-1} = (\alpha x)(\alpha y),$$

α est donc un *automorphisme* du groupe G (c'est-à-dire un isomorphisme de G avec lui-même).

Les automorphismes définis par la relation (1) sont appelés *automorphismes intérieurs* du groupe G . Les autres automorphismes, s'il en existe, sont par définition les automorphismes *extérieurs*.

THÉORÈME. — *Les automorphismes intérieurs forment un groupe homomorphe à G .*

Considérons l'application

$$(2) \quad a \rightarrow \alpha$$

du groupe G sur l'ensemble Γ des automorphismes intérieurs, définie

par la relation (1). Au produit ba correspond l'automorphisme φ défini par

$$\varphi x = ba.x.(ba)^{-1} = baxa^{-1}b^{-1} = \beta(axa^{-1}) = \beta(\alpha x) = \beta\alpha x,$$

c'est-à-dire le *produit*, au sens de la composition des transformations, des automorphismes α et β correspondant à a et b . L'application (2) de G sur Γ est donc un *homomorphisme* : l'ensemble Γ des automorphismes intérieurs, étant homomorphe au groupe G , est lui-même un groupe.

Du théorème précédent résulte, d'après le théorème d'homomorphisme, que le groupe Γ des automorphismes intérieurs est *isomorphe* au groupe-quotient de G par l'un de ses sous-groupes invariants. Celui-ci est l'ensemble des éléments m de G auxquels correspond, dans Γ , l'automorphisme unité ε

$$mxm^{-1} = x, \quad \text{c'est-à-dire} \quad mx = xm \quad \text{pour tout} \quad x \in G.$$

L'ensemble de ces éléments m est donc le *centre* Z de G , et le groupe Γ des automorphismes intérieurs d'un groupe G est isomorphe au groupe-quotient du centre

$$\Gamma \simeq G/Z.$$

Étudions maintenant le groupe Γ des automorphismes intérieurs, en tant que groupe de transformations opérant dans G . L'élément

$$\alpha x = axa^{-1}$$

est appelé *transformé de x par a* , ou encore *élément Γ -conjugué*, plus brièvement *conjugué*, de x . De même, le complexe

$$\alpha H = aHa^{-1}$$

est appelé *transformé de H par a* , ou *complexe Γ -conjugué* du complexe H .

Les éléments invariants par Γ étant ceux du centre, qui comprend au moins l'élément-unité e , le groupe Γ est *intransitif*. Son équivalence de transivité, $\mathfrak{G}$, est définie par $x \equiv y(\mathfrak{G})$ s'il existe $a \in G$ tel que $y = axa^{-1}$. Les classes de G modulo $\mathfrak{G}$ sont appelées *classes d'éléments conjugués*. La classe modulo $\mathfrak{G}$ qui contient un élément du centre, se réduit à cet élément.

Soit X la classe contenant un élément quelconque x . Si nous écrivons que les transformés de x par a et b coïncident,

$$(3) \quad axa^{-1} = bxb^{-1},$$

nous définissons entre a et b une relation réflexive, symétrique et transitive, qui est par conséquent une *équivalence* $\mathcal{E}$ dans G . De plus, cette équivalence est *régulière à gauche*, car (3) entraîne, en désignant par r un élément quelconque de G

$$ra.x.a^{-1}r^{-1} = rb.x.b^{-1}r^{-1}, \quad \text{c'est-à-dire} \quad ra \equiv rb(\mathcal{E}).$$

Les différents conjugués de x correspondent donc biunivoquement aux classes modulo $\mathcal{E}$, c'est-à-dire aux classes à gauche de G par rapport au sous-groupe N_x , classe-unité modulo $\mathcal{E}$. Or, les éléments n de la classe-unité sont ceux pour lesquels on a

$$n x n^{-1} = e x e^{-1} = x, \quad \text{c'est-à-dire} \quad n x = x n,$$

et le sous-groupe N_x est, par conséquent, l'ensemble des éléments de G qui sont permutables avec x . On l'appelle le *normalisateur* de x . Nous avons ainsi établi la proposition suivante (qu'on peut aussi rattacher au théorème 1 du § 5) :

THÉOREME. — *Les différents conjugués d'un élément x correspondent biunivoquement aux classes à gauche de G par rapport au normalisateur N_x . Si la classe X est finie, son ordre ξ est égal à l'index de N_x dans G . Si G lui-même est fini et d'ordre ν , ξ divise ν .*

En supposant G fini, désignons par ζ l'ordre de son centre Z , par $\xi_1, \dots, \xi_k$ les ordres des classes $X_1, \dots, X_k$ qui comprennent *plus d'un élément*, nous avons

$$(4) \quad \nu = \zeta + \xi_1 + \xi_2 + \dots + \xi_k.$$

On donne à cette relation le nom d'*équation des classes*. Nous en indiquerons l'application suivante (1) :

Si G est un groupe d'ordre p^n , où p est un nombre premier, son centre Z ne se réduit pas à l'élément-unité. L'égalité $Z = (e)$

(1) On démontre aussi, à partir de cette équation, le *théorème de Frobenius* : G étant un groupe fini d'ordre N et C une classe d'éléments conjugués d'ordre h , le nombre des solutions x de $x^n \in C$ est un multiple du p. g. c. d. de hn et de N .

En particulier, si n divise N , le nombre des solutions de $x^n = e$, où e désigne l'élément-unité de G , est un multiple de n . Pour la démonstration, voir FROBENIUS (*Über einen Fundamentalsatz der Gruppentheorie*, Berlin, Sitzungsber., 1903, p. 987; 1907, p. 483), ainsi que A. SPEISER (*Theorie der Gruppen von endlicher Ordnung*, Berlin, Springer, 1927, p. 44) et H. ZASSENHAUS (*Lehrbuch der Gruppentheorie*, t. 1, Leipzig-Berlin, 1937, p. 26).

Le théorème de Frobenius a été généralisé par DUBUQUE (*Rec. Math. Moscou*, t. 5, (47), p. 189).

entraînant $\zeta = 1$, serait en effet en contradiction avec l'équation (4), où ν est égal à p^n et où les ξ_i sont des diviseurs de ν différents de l'unité, donc des multiples de p .

Plus généralement, le *normalisateur* N_C d'un complexe C est l'ensemble des éléments de G qui sont permutable avec C . On voit, comme plus haut, que les différents conjugués de C correspondent biunivoquement aux classes à gauche de G par rapport à N_C . Si leur nombre est fini, c'est l'index de N_C dans G .

Si le complexe considéré est un sous-groupe S , les complexes conjugués aSa^{-1} , transformés de S par des automorphismes intérieurs sont des sous-groupes de G , appelés *groupes conjugués* de S . Pour qu'un sous-groupe soit invariant dans G , il faut et il suffit qu'il coïncide avec tous ses conjugués, ou encore que son normalisateur soit le groupe G lui-même.

Le normalisateur N_S d'un sous-groupe S est le plus grand sous-groupe contenant S comme sous-groupe invariant. En effet, il résulte d'abord de la définition de N_S que S est sous-groupe de N_S , et invariant dans N_S . D'autre part, si H est un sous-groupe dont S est sous-groupe invariant, on a, pour tout $h \in H$,

$$hSh^{-1} = S, \quad \text{donc } h \in N_S \text{ et } H \subseteq N_S.$$

Exercices. — 1. Quels sont les automorphismes du groupe cyclique d'ordre 3 ?

2. L'ensemble de tous les automorphismes d'un groupe G est un groupe intransitif Γ_0 . Le groupe Γ des automorphismes intérieurs est un sous-groupe invariant de Γ_0 .

3. Soit x un élément d'un groupe G . Le sous-groupe cyclique (x) est sous-groupe invariant du normalisateur N_x de x .

4. Quel est l'ordre du centre d'un groupe non abélien d'ordre p^3 , p désignant un nombre premier ?

5. Si H est un sous-groupe d'un groupe G , l'intersection I et la réunion complète R des conjugués de H sont des sous-groupes invariants de G .

D. — ÉQUIVALENCES RÉGULIÈRES DANS UN ANNEAU.

9. *Classification des anneaux.* — Nous avons défini plus haut (chap. III, § 10, p. 138) un *anneau* A comme un domaine où existent deux opérations, une *addition* et une *multiplication*, avec les propriétés suivantes :

A est un groupe abélien par rapport à l'addition;
A est un demi-groupe par rapport à la multiplication ⁽¹⁾;
La multiplication est distributive par rapport à l'addition.

L'anneau A est dit *commutatif* si sa multiplication est commutative, ce qu'on ne suppose pas nécessairement ⁽²⁾. La *formule du binôme*

$$(x + a)^n = x^n + C_n^1 x^{n-1} a + \dots + C_n^k x^{n-k} a^k + \dots + a^n$$

est valable dans tout anneau commutatif. Les *coefficients du binôme* C_n^k , désignés souvent aussi par la notation $\binom{n}{k}$ ont pour valeur ⁽³⁾

$$C_n^k = \binom{n}{k} = \frac{n(n-1)\dots(n-k+1)}{k!} = \frac{n!}{k!(n-k)!}.$$

Dans tout anneau A , la *multiplication est distributive, non seulement par rapport à l'addition, mais aussi par rapport à la soustraction*, ce qui entraîne qu'un produit est nul dès qu'un facteur l'est (chap. III, § 10, p. 139)

$$0 \cdot x = x \cdot 0 = 0 \quad \text{pour tout } x \in A.$$

Dans l'anneau des entiers $\mathbb{C}$ et dans ses sous-anneaux (tels que l'anneau des entiers pairs ou celui des multiples d'un nombre donné m), cette condition *suffisante* pour qu'un produit soit nul est également *nécessaire* : le produit de deux entiers différents de zéro est différent de zéro. Mais il n'en est pas ainsi dans tous les anneaux. Nous avons en effet, dans l'anneau $\mathbb{C}/(4)$ des classes résiduelles modulo 4 (cf. § 1, p. 143 et § 2, p. 148), l'égalité ⁽⁴⁾

$$2 \times 2 = 0, \quad \text{avec } 2 \neq 0.$$

Cette remarque conduit aux notions suivantes :

⁽¹⁾ En d'autres termes, la multiplication est *associative*.

⁽²⁾ Les anneaux non commutatifs les plus importants sont les *systèmes hypercomplexes* et les *anneaux de matrices*.

⁽³⁾ Démonstration immédiate par récurrence sur n , au moyen de la formule intermédiaire

$$C_n^k = C_{n-1}^k + C_{n-1}^{k-1}.$$

On peut remarquer aussi que C_n^k est le nombre de combinaisons, sans répétitions, de n lettres k à k (on pourra se reporter à un traité de mathématiques spéciales ou de mathématiques générales).

⁽⁴⁾ On voit qu'un anneau-quotient σ/α , défini par une équivalence régulière α , peut posséder des propriétés algébriques nettement différentes de celles de l'anneau σ , auquel il est homomorphe.

Dans un anneau A , un élément a tel qu'il existe un élément *non nul* a_1 , vérifiant la relation

$$aa_1 = 0 \quad (a_1 \neq 0),$$

est appelé *diviseur de zéro à gauche*. De même, a est *diviseur de zéro à droite* s'il existe au moins un élément *non nul* a_2 tel que

$$a_2a = 0 \quad (a_2 \neq 0).$$

Dans un anneau commutatif, ces deux notions coïncident.

Le produit ra , où r est un élément quelconque de A , est diviseur de zéro à gauche en même temps que a . L'ensemble des diviseurs de zéro à gauche et à droite est multiplicativement permis.

L'élément zéro est un diviseur de zéro. Un diviseur de zéro *non nul* est dit *véritable* diviseur de zéro, ou diviseur de zéro, sans plus, si aucune confusion n'est à craindre.

Un élément d'un anneau A est *nilpotent* si l'une de ses puissances est nulle

$$a^h = 0.$$

Tout élément nilpotent est diviseur de zéro. Par exemple, l'élément **2** dans l'anneau $C/(4)$ est nilpotent. L'élément **2** dans l'anneau $C/(6)$ est un diviseur de zéro, mais n'est pas nilpotent.

Pour qu'un anneau A ne possède pas de véritables diviseurs de zéro, il faut et il suffit que l'ensemble $A^* = A - \{0\}$ soit fermé par rapport à la multiplication; il en est ainsi dans le cas d'un corps (chap. III, § 10, p. 140) : un corps n'a pas de diviseurs de zéro (véritables). D'une façon générale, quand un anneau A n'a pas de véritables diviseurs de zéro, A^* est un *semi-groupe multiplicatif*, car la relation

$$a \cdot x = b \cdot x \quad (a, b, x \neq 0)$$

entraîne

$$(a - b) \cdot x = 0, \quad \text{donc} \quad a - b = 0,$$

et la règle de simplification à droite (par exemple) est valable dans A^* par rapport à la multiplication.

On donne le nom de *domaine d'intégrité* à tout anneau commutatif sans véritables diviseurs de zéro. L'anneau des entiers C est un domaine d'intégrité, tandis que $C/(4)$ n'en est pas un. Cherchons à quelle condition l'anneau des classes résiduelles $C/(m)$ est un domaine d'intégrité.

Il faut que m soit premier, car, dans le cas contraire, la relation $ab = m$, où a et b sont distincts de 1 et de m , entraîne pour les

classes **a** et **b** correspondantes

$$ab = 0, \quad \text{avec } a \text{ et } b \neq 0,$$

Cette condition est également *suffisante*, car si $m = p$, où p est premier, et si **a** est une classe différente de zéro, tout nombre de cette classe est premier à p et son produit par un autre nombre b n'est multiple de p que si b est multiple de p : les relations

$$ab = 0, \quad a \neq 0$$

entraînent donc

$$b = 0.$$

L'ensemble des éléments *non nuls* du domaine d'intégrité $C/(p)$ est donc, par rapport à la multiplication, un *semi-groupe fini* et, par conséquent, un *groupe* (chap. III, § 2, p. 106) : $C/(p)$ est donc un *corps* de p éléments (*champ de Galois*). Le même raisonnement montre que *tout domaine d'intégrité fini est un corps*. L'anneau des entiers C est un exemple simple de domaine d'intégrité infini qui n'est pas un corps.

Considérons, dans un anneau quelconque A , le groupe cyclique *additif* engendré par un élément x . Si ce groupe est fini quel que soit $x \in A$, et si son ordre α_x divise un entier positif M *indépendant* de x , cet ordre α_x n'a, quand x décrit A , qu'un nombre fini de valeurs possibles $\alpha_1, \alpha_2, \dots$, diviseurs de M ; le p. p. c. m. N de ces valeurs $\alpha_1, \alpha_2, \dots$ est le *plus petit entier positif* tel que l'on ait

$$Nx = 0 \quad \text{pour tout } x \in A,$$

et la relation

$$nx = 0 \quad \text{pour tout } x \in A,$$

où n est un nombre entier ($n \in C$) a lieu si n est multiple de N et *seulement* dans ce cas : on dit alors que l'anneau A est de *caractéristique non nulle* N .

Dans le cas contraire, 0 est le seul entier n tel que

$$nx = 0 \quad \text{pour tout } x \in A,$$

on dit que A est un anneau de *caractéristique nulle*.

Le cas où l'anneau A admet un *élément-unité* e (élément-unité à gauche, par exemple, si l'anneau A n'est pas commutatif) est particulièrement simple. On a, en effet, pour tout entier positif n ,

$$nx = x + \dots + x = (e + \dots + e)x = ne.x,$$

de sorte que l'expression nx peut être regardée comme le *produit de deux éléments de l'anneau A*, *ne et x*. Pour abrégé, l'élément ne sera, à partir de maintenant, désigné par n , mais, lorsqu'il y aura lieu de préciser que n n'est pas un nombre naturel ordinaire, nous écrirons $n \in A$.

Dans ces conditions, pour que l'on ait

$$nx = 0 \quad \text{pour tout } x \in A$$

(donc en particulier pour $x = e$), il faut et il suffit que

$$n = 0 \quad (n = ne \in A).$$

Par suite, *pour qu'un anneau A possédant un élément-unité (à gauche par exemple) e soit de caractéristique non nulle, il faut et il suffit que le groupe cyclique additif (e) soit fini, et la caractéristique de A est égale à l'ordre de ce groupe.*

Un anneau A sans véritables diviseurs de zéro a une caractéristique égale soit à zéro, soit à un nombre premier p.

Si, en effet, la caractéristique était nn' ($n, n' \neq 0, 1$), il existerait dans l'anneau A des éléments a, b tels que l'on ait

$$na \neq 0, \quad n'b \neq 0;$$

on aurait alors

$$na.n'b = nn'.ab = 0,$$

contrairement à l'hypothèse qu'il n'existe pas de diviseurs de zéro.

En particulier un domaine d'intégrité, un *corps* (commutatif ou gauche), sont de caractéristique *nulle ou de caractéristique p (p premier)*.

Dans un anneau A sans véritables diviseurs de zéro, si l'on a une relation de la forme

$$na = 0 \quad (n \in \mathbb{C}, a \in A),$$

avec $a \neq 0$, l'entier n est multiple de la caractéristique, donc nul si A est de caractéristique nulle, multiple de p si A est de caractéristique p. On a, en effet, pour tout $x \in A$,

$$0 = na.x = n.ax = a.nx, \quad \text{d'où} \quad nx = 0,$$

et n est multiple de la caractéristique.

Exemples. — L'anneau des entiers C et ses sous-anneaux sont de caractéristique nulle.

L'anneau $\mathbb{C}/(m)$ des classes résiduelles modulo m a la caractéristique m ; si m est premier, $m = p$, cet anneau est un *corps de caractéristique p*.

Des règles de calcul remarquables se présentent dans les *anneaux commutatifs de caractéristique p* ($p \neq 0$), en particulier dans les *corps commutatifs de caractéristique p* . Dans un tel domaine, les coefficients

$$C_p^k = \frac{p(p-1)\dots(p-k+1)}{k!} \quad (k = 1, \dots, p-1),$$

dans le développement de $(x + a)^p$ sont tous multiples de p , puisque, $2, \dots, k$ étant premiers à p , leur produit est aussi premier à p , donc divise $(p-1)\dots(p-k+1)$. Nous avons donc

$$C_p^k x^{p-k} a^k = 0,$$

d'où

$$(1) \quad (x + a)^p = x^p + a^p$$

et, en remplaçant x par $x - a$,

$$(1') \quad (x - a)^p = x^p - a^p.$$

Ces formules entraînent, de proche en proche,

$$(2) \quad (a_1 + a_2 + \dots + a_m)^p = a_1^p + a_2^p + \dots + a_m^p,$$

$$(3) \quad (x + a)^{p^f} = x^{p^f} + a^{p^f},$$

$$(3') \quad (x - a)^{p^f} = x^{p^f} - a^{p^f}.$$

En supposant que l'anneau considéré A ait un élément-unité e , et en prenant dans (2)

$$a_1 = a_2 = \dots = a_m = e,$$

nous obtenons

$$m^p = m \quad (m \in A).$$

Cette relation est valable en particulier dans le *corps des classes résiduelles* $C/(p)$: il en résulte qu'on a, pour tout nombre naturel x ,

$$x^p \equiv x \pmod{p},$$

propriété connue sous le nom de *théorème de Fermat* (cf. § 4, exerc. 4, p. 158).

Exercices. — 1. Dans un anneau avec élément-unité, un élément qui a un inverse à gauche n'est pas diviseur de zéro à gauche. Dans un *domaine d'intégrité*, si l'on a une égalité de la forme

$$a = e a,$$

où a est un élément particulier *non nul*, e est élément-unité.

2. Combien y a-t-il de diviseurs de zéro dans l'anneau des classes résiduelles modulo m , $\mathbb{C}/(m)$?

3. On considère un nombre naturel $m = p_1^{\alpha_1} \dots p_r^{\alpha_r}$, où les p_i sont des nombres premiers différents. Combien l'anneau $\mathbb{C}/(m)$ admet-il de diviseurs de zéro nilpotents?

Quels sont les nombres m tels que :

1° Zéro soit le seul diviseur de zéro nilpotent ?

2° Tout diviseur de zéro soit nilpotent ?

10. Notion d'idéal. — Soit A un anneau que nous ne supposons pas nécessairement commutatif. Considérons dans A une équivalence $\mathcal{R}$ que nous supposons

Régulière par rapport à l'addition;

Régulière à droite par rapport à la multiplication.

Soit $\mathfrak{m}$ la classe-zéro modulo $\mathcal{R}$, c'est-à-dire la classe qui contient l'élément-zéro de A . Cette classe $\mathfrak{m}$ possède les propriétés suivantes :

1. $\mathfrak{m}$ est un sous-groupe abélien par rapport à l'addition, ou sous-module, de A : en d'autres termes, les relations $a \in \mathfrak{m}$, $b \in \mathfrak{m}$ entraînent $a + b \in \mathfrak{m}$.

1 bis. La relation $x \equiv y (\mathcal{R})$ équivaut à $x - y \in \mathfrak{m}$, et les classes modulo $\mathcal{R}$ sont les complexes $x + \mathfrak{m}$ distincts.

En effet, si l'on considère l'anneau A comme un groupe additif, la classe-zéro $\mathfrak{m}$ joue le rôle de classe-unité, et les propriétés précédentes sont celles qui ont été établies au chapitre IV, (§ 3 et 6), la notation multiplicative étant remplacée ici par la notation additive.

2. Au point de vue multiplicatif, $\mathfrak{m}$ est un complexe permis à droite, c'est-à-dire que la relation $a \in \mathfrak{m}$ entraîne $ax \in \mathfrak{m}$ quel que soit $x \in A$.

En effet, la relation $a \in \mathfrak{m}$ équivaut à

$$a \equiv 0 (\mathcal{R}),$$

d'où, puisque $\mathcal{R}$ est régulière à droite

$$ax \equiv 0 (\mathcal{R}), \quad \text{c'est-à-dire} \quad ax \in \mathfrak{m}.$$

Alors que la propriété 1 bis caractérise l'équivalence $\mathcal{R}$ à partir de la classe-zéro $\mathfrak{m}$, les propriétés 1 et 2 concernent uniquement cette classe en tant que sous-ensemble de l'anneau A .

Définition. — On donne le nom d'*idéal à droite* dans l'anneau A à tout sous-groupe additif de A qui est multiplicativement permis à droite dans A . Pratiquement, pour qu'un sous-ensemble non vide $\mathfrak{m}$ de A soit un idéal à droite dans A , il faut et il suffit que $a \in \mathfrak{m}$, $b \in \mathfrak{m}$ entraînent $a - b \in \mathfrak{m}$ et que $a \in \mathfrak{m}$ entraîne $ax \in \mathfrak{m}$ pour tout $x \in A$.

Par rapport à l'équivalence $\mathcal{R}$ considéré ci-dessus, la classe-zéro $\mathfrak{m}$ est donc un idéal à droite.

Donnons-nous inversement un idéal à droite $\mathfrak{m}$ dans l'anneau A : $\mathfrak{m}$ est sous-groupe additif de A , donc l'équivalence $\mathcal{R}$ définie par la propriété 1 bis est régulière par rapport à l'addition ; $\mathfrak{m}$ est d'ailleurs la classe-zéro modulo $\mathcal{R}$. Enfin, $\mathcal{R}$ est régulière à droite par rapport à la multiplication, car la relation

$$a \equiv b \ (\mathcal{R}), \quad \text{c'est-à-dire} \quad a - b \in \mathfrak{m}$$

entraîne, puisque $\mathfrak{m}$ est idéal à droite,

$$(a - b)x \in \mathfrak{m}, \quad \text{c'est-à-dire} \quad ax \equiv bx \ (\mathcal{R})$$

quel que soit $x \in A$.

Il y a donc, dans tout anneau A , correspondance biunivoque entre les équivalences régulières par rapport à l'addition, régulières à droite par rapport à la multiplication, et les idéaux à droite.

On définit d'une manière analogue les idéaux à gauche dans A comme sous-groupes additifs de A , multiplicativement permis à gauche. Les idéaux à gauche correspondent biunivoquement aux équivalences régulières par rapport à l'addition et régulières à gauche par rapport à la multiplication.

On donne le nom d'*idéal bilatère* à tout sous-ensemble qui est à la fois idéal à droite et idéal à gauche : les idéaux bilatères correspondent biunivoquement aux équivalences régulières par rapport à l'addition et à la multiplication.

Dans un anneau commutatif, les trois notions d'idéal à droite, d'idéal à gauche et d'idéal bilatère coïncident ; tout sous-module multiplicativement permis est appelé *idéal*.

Soient $\mathfrak{m}$ un idéal bilatère dans un anneau A (non commutatif) et $\mathcal{R}$ l'équivalence régulière correspondante. Les classes modulo $\mathcal{R}$ sont appelées *classes résiduelles* modulo $\mathfrak{m}$. La relation $x \equiv y (\mathcal{R})$ s'écrit ordinairement

$$x \equiv y \ (\mathfrak{m})$$

et s'énonce : « x congru à y modulo $\mathfrak{m}$ » ⁽¹⁾. L'ensemble-quotient $A/\mathcal{R}$ est homomorphe à A (chap. IV, § 2, p. 146 et 148); c'est donc un anneau, appelé *anneau des classes résiduelles modulo $\mathfrak{m}$* et désigné ordinairement par la notation $A/\mathfrak{m}$.

Inversement, si un anneau $\bar{A}$ est homomorphe à A , l'équivalence d'homomorphisme $\mathcal{R}$ est *régulière* par rapport à l'addition et à la multiplication et, par conséquent, l'ensemble $\mathfrak{m}$ des éléments de A qui ont pour image l'élément-zéro de $\bar{A}$, c'est-à-dire la classe-zéro modulo $\mathcal{R}$, est un idéal bilatère ⁽²⁾. On a (chap. IV, § 2, p. 147)

$$\bar{A} \simeq A/\mathcal{R} = A/\mathfrak{m},$$

ce qui constitue le *théorème d'homomorphisme pour les anneaux*.

Si un anneau $\bar{A}$ est homomorphe à un anneau A , $A \sim \bar{A}$, l'ensemble des éléments de A qui ont pour image l'élément-zéro de $\bar{A}$ est un idéal bilatère $\mathfrak{m}$ et on a l'isomorphisme d'anneaux

$$\bar{A} \simeq A/\mathfrak{m}.$$

L'*égalité* est, dans tout anneau A , une équivalence régulière : l'idéal correspondant, qui se compose du seul élément 0, est appelé *idéal-zéro* et désigné par (0). A l'*équivalence absolue* correspond l'anneau A lui-même, qui est appelé *idéal-unité*, et désigné par (1) lorsque A admet un élément-unité 1. Quand il en est ainsi, pour qu'un idéal $\mathfrak{m}$ coïncide avec A , il faut et il suffit que l'on ait

$$1 \in \mathfrak{m}.$$

THÉORÈME. — *Dans un corps K , il n'existe pas d'autres idéaux que l'idéal-zéro et l'idéal-unité.*

(1) En particulier, la relation $x \in \mathfrak{m}$ s'écrit souvent sous la forme $x \equiv 0 \pmod{\mathfrak{m}}$.

(2) Ce fait peut aussi se vérifier directement. L'homomorphisme considéré $A \sim \bar{A}$ est une application $a \rightarrow \bar{a}$ de A sur $\bar{A}$, telle que l'on ait

$$\overline{a+b} = \bar{a} + \bar{b} \quad \text{et} \quad \overline{ab} = \bar{a}\bar{b}.$$

Donc, si deux éléments a, b de A ont pour image 0 dans $\bar{A}$, nous avons

$$\overline{a \pm b} = 0.$$

et, pour tout $x \in A$

$$\overline{ax} = 0 \bar{x} = 0, \quad \overline{xa} = \bar{x} 0 = 0,$$

ce qui prouve que l'ensemble $\mathfrak{m}$ est un idéal bilatère dans A . D'ailleurs, d'après le théorème d'homomorphisme pour les groupes, $\mathfrak{m}$ est un sous-groupe additif de A ; c'est, de plus, un sous-ensemble multiplicativement permis (§ 2, th. 3, p. 149).

Soit $\mathfrak{m}$ un idéal de K . Si $\mathfrak{m}$ est différent de (0) , il existe au moins un élément a non nul de K appartenant à $\mathfrak{m}$. Or, la relation $a \in \mathfrak{m}$ entraîne

$$a^{-1}a = aa^{-1} = 1 \in \mathfrak{m}, \quad \text{donc } \mathfrak{m} = K.$$

Tout idéal $\mathfrak{m}$ (d'un seul côté ou bilatère) dans un anneau A est sous-anneau de A . La réciproque n'est évidemment pas vraie : un sous-anneau est multiplicativement *fermé*, tandis qu'un idéal est multiplicativement *permis*, condition plus forte ⁽¹⁾.

Exemple. — Dans l'anneau C des entiers, les congruences arithmétiques sont régulières : la classe-zéro modulo m , ensemble des multiples km de m (k entier relatif arbitraire) est donc un idéal, que l'on désigne par (m) .

Exercices. — 1. Dans un anneau A , commutatif ou non, on considère un élément a . L'ensemble $\mathfrak{a}$ des éléments $x \in A$ tels que l'on ait

$$ax = 0,$$

est un idéal à droite.

2. Dans un anneau *commutatif* A , l'ensemble des éléments nilpotents est un idéal. Plus généralement, l'ensemble des éléments de A dont une puissance (positive) appartient à un idéal donné $\mathfrak{a}$, est un idéal $\mathfrak{r}$, contenant $\mathfrak{a}$, et appelé *radical* de $\mathfrak{a}$.

11. Idéaux d'un anneau; opérations fondamentales. — L'ensemble $\mathcal{J}_g$ des idéaux à gauche d'un anneau R (que nous ne supposons pas commutatif), l'ensemble $\mathcal{J}_d$ des idéaux à droite, l'ensemble $\mathcal{J}$ des idéaux bilatères, vérifient chacun les *conditions de Moore* : par exemple, *a.* $R \in \mathcal{J}_g$; *b.* Toute intersection d'idéaux à gauche est un idéal à gauche : en effet, cette intersection, non vide puisqu'elle contient l'élément-zéro de R , est d'une part un sous-groupe additif de R , d'autre part un ensemble multiplicativement permis à gauche dans R .

Il en résulte que $\mathcal{J}_g$, $\mathcal{J}_d$ et $\mathcal{J}$, ordonnés partiellement par la relation d'inclusion, sont des *treillis complets*, contenus dans le treillis $\mathcal{S}$ des sous-groupes additifs de R ; comme on l'a vu, $\mathcal{S}$ est un treillis complet et modulaire. Or, le plus petit sous-groupe additif $\mathfrak{a} = \sum_{\mathfrak{m} \in \mathcal{F}} \mathfrak{m}$ contenant tous les idéaux d'une famille $\mathcal{F}$ (non vide) d'idéaux à gauche, est déjà un idéal à gauche. En effet, tout élément a de $\mathfrak{a}$ est

⁽¹⁾ Nous pouvons d'ailleurs donner, en anticipant un peu, l'exemple suivant. L'ensemble C des entiers relatifs est un sous-anneau du corps Γ des nombres rationnels; il n'est pas un idéal dans Γ .

une somme finie

$$a = m_1 + \dots + m_\lambda$$

d'éléments m_i d'idéaux $\mathfrak{m}_i \in \mathcal{F}$ (cf. chap. III, § 5, th. 3, p. 116) et nous avons, pour tout $r \in R$,

$$ra = rm_1 + \dots + rm_\lambda, \quad \text{où } rm_i \in \mathfrak{m}_i,$$

donc

$$ra \in \mathfrak{a}$$

L'union dans $\mathcal{J}_g$ (et, de même, dans $\mathcal{J}_d$ ou dans $\mathcal{J}$) coïncide, par conséquent, avec la somme, ou réunion complète, des idéaux en tant que sous-groupes additifs de R : $\mathcal{J}_g$, $\mathcal{J}_d$ et $\mathcal{J}$ sont des sous-treillis de $\mathcal{S}$ et, par conséquent, des treillis modulaires.

En particulier, le plus petit idéal à gauche contenant deux idéaux à gauche $\mathfrak{m}_1$, $\mathfrak{m}_2$ est l'idéal-somme $\mathfrak{m}_1 + \mathfrak{m}_2$, ensemble des éléments de la forme $m_1 + m_2$, où $m_i \in \mathfrak{m}_i$; il est bilatère si $\mathfrak{m}_1$ et $\mathfrak{m}_2$ le sont.

La relation d'inclusion $\subseteq$, et les deux opérations fondamentales, intersection $\cap$ et addition $+$, ont une signification arithmétique qui est l'origine d'une autre terminologie. Dans l'anneau C des entiers, pour que l'idéal (m) , ensemble des multiples de m , soit contenu dans l'idéal (m') , $(m) \subseteq (m')$, il faut et il suffit que m soit un multiple de m' : $m \equiv 0(m')$. Pour cette raison, on énonce encore la relation d'inclusion, pour deux idéaux (de $\mathcal{J}_g$, ou de $\mathcal{J}_d$, ou de $\mathcal{J}$), $\mathfrak{m} \subseteq \mathfrak{m}'$, en disant que $\mathfrak{m}$ est un multiple de $\mathfrak{m}'$, $\mathfrak{m}'$ un diviseur de $\mathfrak{m}$, et l'on écrit

$$\mathfrak{m} \equiv 0 \quad (\mathfrak{m}').$$

Toujours dans l'anneau C , l'intersection des deux idéaux (a) , (b) est l'ensemble des multiples communs de a et de b , donc est l'idéal (m) , m désignant le p. p. c. m. des nombres a , b ; leur somme $(a) + (b)$, ensemble des nombres $ra + sb$, où r , s sont des entiers arbitraires, est l'idéal (d) , où d est le p. g. c. d. de a et b ⁽¹⁾. Aussi donne-t-on encore le nom de *plus petit commun multiple* à une *intersection* d'idéaux, et écrit-on $[\mathfrak{a}_1, \mathfrak{a}_2, \dots, \mathfrak{a}_n]$ pour $\mathfrak{a}_1 \cap \mathfrak{a}_2 \cap \dots \cap \mathfrak{a}_n$; de même, la *somme* est appelée *plus grand commun diviseur* et l'on écrit $(\mathfrak{a}_1, \mathfrak{a}_2, \dots, \mathfrak{a}_n)$ pour $\mathfrak{a}_1 + \mathfrak{a}_2 + \dots + \mathfrak{a}_n$.

En associant à chaque *complexe* $K \subseteq R$ le plus petit idéal à gauche $\bar{K}$ le contenant, intersection de tous les idéaux à gauche contenant K ,

(1) On sait, d'après l'algorithme d'Euclide, que d est de la forme $ra + sb$. Cette propriété bien connue sera rattachée plus loin (chap. VI, § 3, p. 316) à des théorèmes généraux.

nous définissons, dans R , une *fermeture* puisque $\mathcal{J}_g$ vérifie les conditions de Moore : cet idéal $\bar{K}$ est, par définition, l'*idéal à gauche engendré par le complexe* K .

Tout idéal à gauche $\mathfrak{m}$ contenant un élément a contient

$$a + a = 2a, \quad 3a, \quad \dots$$

et

$$a - a = 0, \quad 0 - a = -a, \quad -2a, \quad \dots,$$

donc na , où n est un entier relatif quelconque. D'autre part, $\mathfrak{m}$ contient aussi tous les produits ra , où r est un élément arbitraire de R . Par conséquent, la relation $a \in \mathfrak{m}$ entraîne

$$na + ra \in \mathfrak{m} \quad \text{pour tout } n \in \mathbb{C} \text{ et tout } r \in R.$$

Or, ces éléments $na + ra$ ($n \in \mathbb{C}$, $r \in R$), appelés *multiples à gauche de a dans R* , forment un *idéal à gauche dans R* , car nous avons

$$(na + ra) - (n'a + r'a) = (n - n')a + (r - r')a,$$

avec

$$n - n' \in \mathbb{C}, \quad r - r' \in R$$

et

$$r'(na + ra) = nr'.a + r'.r.a = r_1a,$$

avec

$$r_1 = nr' + r'r \in R.$$

Cet idéal est donc l'*idéal à gauche engendré par a* : un tel idéal à gauche, engendré par un complexe réduit à un seul élément, est dit *principal à gauche* et désigné par $\langle a \rangle$. La relation $a \in \mathfrak{m}$, où $\mathfrak{m}$ est un idéal à gauche, équivaut à $\langle a \rangle \subseteq \mathfrak{m}$.

Si l'anneau R possède un élément-unité e , l'élément na peut être regardé comme le produit de deux éléments de R :

$$na = ne.a = sa, \quad \text{où } s = ne \in R;$$

alors, tous les multiples de a sont de la forme ra , où r décrit R , et l'idéal principal à gauche coïncide avec le complexe-produit : $\langle a \rangle = Ra$. Il n'en est plus de même dans un anneau sans élément-unité : Ra est encore un idéal à gauche, on a $Ra \subseteq \langle a \rangle$, mais en général Ra ne contient pas a et l'inclusion est stricte.

Dans l'anneau R des entiers relatifs *pairs*, par exemple, l'élément

$$6 = 2 + 2 + 2 = 3.2$$

et, de même, les éléments $(2p + 1)2$, appartiennent à l'idéal principal

(bilatère) (2), mais ne sont pas le produit de deux éléments de l'anneau, donc n'appartiennent pas à l'idéal $R.2$.

Plus généralement, l'ensemble α des sommes

$$\sum_{i=1}^h (n_i a_i + r_i a_i), \quad n_i \in C, \quad r_i \in R,$$

c'est-à-dire des sommes de multiples à gauche d'éléments fixes $a_1, \dots, a_h$, est l'*idéal à gauche* engendré par l'ensemble de ces éléments. Inversement, on dit que l'ensemble $\{a_1, \dots, a_h\}$ est une *base* de cet idéal à gauche, et l'on écrit

$$\alpha = (a_1, \dots, a_h);$$

α est la somme des idéaux principaux à gauche $\langle a_i \rangle$. On dit qu'un idéal à gauche $\mathfrak{m}$ admet une base finie s'il est susceptible de ce mode de génération.

Si deux idéaux à gauche ont des bases finies

$$\alpha = (a_1, \dots, a_h) = \sum_{i=1}^h \langle a_i \rangle, \quad \mathfrak{b} = (b_1, \dots, b_k) = \sum_{j=1}^k \langle b_j \rangle,$$

l'idéal à gauche $\alpha + \mathfrak{b}$, somme des idéaux principaux $\langle a_i \rangle, \langle b_j \rangle$, a, lui aussi, une base finie :

$$\alpha + \mathfrak{b} = \sum_{i=1}^h \langle a_i \rangle + \sum_{j=1}^k \langle b_j \rangle = (a_1, \dots, a_h, b_1, \dots, b_k).$$

On peut aussi établir cette propriété en remarquant que l'idéal $\alpha + \mathfrak{b}$ est le groupe composé des groupes additifs α et $\mathfrak{b}$, et en appliquant le théorème 2 du chapitre III (§ 5, p. 115).

Il n'est pas nécessaire d'énoncer les propriétés symétriques des précédentes; si un *idéal à droite* α admet une base finie $\{a_1, \dots, a_h\}$, on écrit

$$\alpha = \{a_1, \dots, a_h\}.$$

L'*idéal bilatère principal* (a) engendré par un élément a , c'est-à-dire le plus petit idéal bilatère contenant a , est visiblement l'idéal engendré par les *multiples bilatères*

$$na + ra + ar' + r_1 ar_2 \quad (n \in C, r, r', r_1, r_2 \in R).$$

Dans un *anneau commutatif*, ces multiples sont tous de la forme

$na + ra$; si, en outre, l'anneau possède un *élément-unité*, tout multiple de a est de la forme ra et l'on a

$$(a) = Ra.$$

Dans un anneau non commutatif avec *élément-unité*, tout multiple de a est de la forme r_1ar_2 , et l'idéal bilatère principal (a) est engendré par le complexe RaR .

Un idéal bilatère, en particulier un idéal dans un anneau commutatif, admet une base finie,

$$\mathfrak{a} = (a_1, \dots, a_h),$$

s'il est engendré par un ensemble fini $\{a_1, \dots, a_h\}$, appelé *base* de l'idéal.

On remarquera qu'un même idéal peut admettre des bases différentes. On a, par exemple, dans l'anneau C des entiers :

$$\begin{aligned} (1) &= (-1) = (3, 4) = (2, 5), \\ (2) &= (6, 8). \end{aligned}$$

Les modes de génération précédents fournissent des procédés simples, souvent employés, pour définir ou pour construire des idéaux dans un anneau donné. Ils ont aussi un grand intérêt théorique, comme le montrent les notions suivantes.

Un anneau à idéaux principaux (ou anneau principal) est un anneau commutatif où tout idéal est principal. Plus généralement, un anneau commutatif dans lequel tout idéal admet une base finie, est appelé *noethérien*⁽¹⁾. On dit aussi qu'un tel anneau vérifie l'*axiome de la base finie*. Tout anneau fini est noethérien; tout corps est un anneau noethérien.

THÉORÈME. — *L'anneau C des entiers est un anneau à idéaux principaux, donc noethérien.*

L'anneau C est, en effet, un *groupe cyclique additif*, d'ordre infini, engendré par 1. Tout idéal $\mathfrak{m}$, dans C , est un sous-groupe additif de C ,

⁽¹⁾ Du nom de la mathématicienne Emmy Noether, à qui est due l'étude de ces anneaux et la théorie axiomatique des idéaux : cf. *Idealtheorie in Ringbereichen*, *Math. Ann.*, t. 83, 1921, p. 24-66, et *Abstrakter Aufbau der Idealtheorie in algebraischen Zahl und Funktionenkörpern*, *Math. Ann.* t. 96, 1926, p. 26-64. Nous rencontrons, comme application d'un théorème dû à Hilbert, deux types importants d'anneaux noethériens au chap. VI, § 5, p. 331.

donc un *groupe cyclique* (chap. III, § 4, p. 112) et nous avons ⁽¹⁾

$$\mathfrak{m} = (m).$$

Lorsqu'un anneau R est sous-anneau d'un anneau R' , il existe entre les idéaux de R et ceux de R' une correspondance remarquable étudiée par Grell ⁽²⁾. Soit $\mathfrak{m}$ un idéal à gauche, par exemple, dans l'anneau R : associons-lui l'idéal $f\mathfrak{m}$ qu'il engendre dans R' ; $f\mathfrak{m}$ est appelé *extension* de $\mathfrak{m}$. À un idéal à gauche, $\mathfrak{m}'$, de l'anneau R' , associons, dans R , l'ensemble $\varphi\mathfrak{m}' = \mathfrak{m}' \cap R$ qui est évidemment un idéal à gauche de R , appelé *contraction* de $\mathfrak{m}'$.

Chacune des applications uniformes f, φ est *isotone* (propriétés 1^a, 1^a'a, p. 121). De plus, on a les propriétés.

$$(2a) \quad \mathfrak{m} \subseteq \varphi f\mathfrak{m} = f\mathfrak{m} \cap R$$

et

$$(2'a) \quad \mathfrak{m}' \supseteq f\varphi\mathfrak{m}' = f(\mathfrak{m}' \cap R),$$

puisque $f(\mathfrak{m}' \cap R)$ est le plus petit idéal à gauche de l'anneau R' contenant le complexe $\mathfrak{m}' \cap R (\subseteq \mathfrak{m}')$. La correspondance entre le treillis complet $\mathcal{J}_g$ des idéaux à gauche de R et le treillis complet $\mathcal{J}'_g$ des idéaux à gauche de R' , définie par les deux applications uniformes f, φ , est donc une *correspondance de Galois inversée* (chap. III, § 6). Les éléments fermés, c'est-à-dire les idéaux de R qui sont *contractions* et les idéaux de R' qui sont *extensions* forment des treillis complets $\mathfrak{C}, \mathfrak{C}'$, et se correspondent biunivoquement par les applications f et $\varphi (= f^{-1})$; enfin, cette application biunivoque et isotone de $\mathfrak{C}$ sur $\mathfrak{C}'$ est un *isomorphisme pour les opérations de ces treillis*, c'est-à-dire pour l'*intersection* et l'*addition des idéaux* (cf. chap. III, § 6, p. 123).

(¹) On peut encore exprimer ce résultat en disant que, dans l'anneau C des entiers de signe quelconque, les congruences arithmétiques sont les seules équivalences régulières par rapport à l'addition (donc les seules régulières à la fois par rapport à l'addition et à la multiplication). Mais il existe de nombreuses *équivalences régulières seulement par rapport à la multiplication*, par exemple :

1^o $x \equiv y (\omega_p)$ si les décompositions de x et y en facteurs premiers contiennent le nombre premier p avec le même exposant [on a 1 = 3 et 2 $\not\equiv$ 4 (ω_2)];

2^o Dans $C - \{0\}$ ou dans N , $x \equiv y (\varepsilon)$ si xy est un carré parfait.

(²) H. GRELL, *Beziehungen zwischen den Idealen verschiedener Ringe* (Math. Ann., t. 97, 1927, p. 490-523). Voir aussi W. KRULL, *Idealtheorie* (Ergebn. der Math., IV, t. 3, 1935, § 7). Nous étudions ici cette correspondance comme *correspondance de Galois inversée*; l'interprétation au moyen des fonctions multiformes, vue plus haut pour les correspondances de Galois générales (ordinaires ou inversées), a été indiquée par : M. L. DUBREIL-JACOTIN, *Quelques propriétés des applications multiformes* (C. R. Acad. Sc., t. 230, 1950, p. 806-808). Les auteurs précédents considèrent le cas d'*anneaux commutatifs avec élément-unité*.

Dans un anneau R que nous ne supposons pas nécessairement commutatif, considérons un idéal à gauche α , un complexe quelconque C et l'ensemble M des produits ac , où $a \in \alpha$, $c \in C$. Le groupe additif $\bar{M}$ engendré par M est un idéal à gauche. En effet, puisque α contient $-a$ en même temps que a , $\bar{M}$ est l'ensemble des sommes finies

$$s = \alpha_1 c_1 + \dots + \alpha_\lambda c_\lambda \quad (\alpha_i \in \alpha, c_i \in C)$$

(cf. chap. III, § 3, p. 110) et cet ensemble est multiplicativement permis à gauche dans R , puisque nous avons, pour tout $r \in R$,

$$rs = r\alpha_1 c_1 + \dots + r\alpha_\lambda c_\lambda, \quad \text{où } r\alpha_i \in \alpha,$$

donc rs appartient à $\bar{M}$ en même temps que s . L'idéal à gauche $\bar{m} = \bar{M}$ est appelé idéal-produit de l'idéal α par le complexe C , et désigné par αC ; quand C se compose d'un seul élément, $C = \{c\}$, on emploie la notation simplifiée αc (dans ce cas, d'ailleurs, l'idéal-produit coïncide avec le complexe-produit M).

Le complexe C est souvent un idéal à gauche b ; on a alors

$$\alpha b \subseteq b.$$

Si α est un idéal bilatère, on a aussi

$$\alpha b \subseteq \alpha,$$

d'où

$$(1) \quad \alpha b \subseteq \alpha \cap b.$$

La multiplication des idéaux à gauche est associative :

$$\alpha_1(\alpha_2 \alpha_3) = (\alpha_1 \alpha_2) \alpha_3.$$

On peut donc parler du produit d'un nombre quelconque d'idéaux à gauche et, en particulier, des puissances (entières et positives) m^α d'un tel idéal m .

Nous n'énoncerons pas les définitions et propriétés symétriques des précédentes, mais nous remarquerons que le produit αb d'un idéal à gauche α par un idéal à droite b est un idéal bilatère; si, de plus, α et b admettent des bases finies,

$$\alpha = \{\alpha_1, \dots, \alpha_h\}, \quad b = \{b_1, \dots, b_k\},$$

l'idéal bilatère αb admet la base finie

$$\alpha = \{\alpha_1 b_1, \dots, \alpha_i b_j, \dots, \alpha_h b_k\}.$$

Cette règle et la formule (1) sont valables en particulier s'il s'agit d'idéaux bilatères ou d'idéaux d'un anneau commutatif.

Remarque. — Dans un anneau R possédant un élément-unité e , l'idéal à gauche $\bar{C}$ engendré par un complexe C n'est autre que l'idéal-produit RC , dans lequel R est considéré comme idéal à gauche. Nous avons, en effet,

$$C = eC \subseteq RC, \quad \text{d'où} \quad \bar{C} \subseteq RC.$$

Comme, d'autre part, $\bar{C}$ contient nécessairement RC , nous avons l'égalité

$$\bar{C} = RC.$$

Dans le treillis $\mathcal{J}_g$ des idéaux à gauche, par exemple, la multiplication respecte la relation d'inclusion

$$m_1 \subseteq m_2 \quad \text{entraîne} \quad am_1 \subseteq am_2 \quad \text{et} \quad m_1 b \subseteq m_2 b,$$

quels que soient $a, b, m_1, m_2 \in \mathcal{J}_g$. Soit $\mathcal{F}$ une famille d'idéaux m ; la relation

$$m \subseteq \sum_{m \in \mathcal{F}} m$$

entraîne, quel que soit l'idéal $a \in \mathcal{J}_g$,

$$am \subseteq a \left(\sum_{m \in \mathcal{F}} m \right), \quad \text{d'où} \quad \sum_{m \in \mathcal{F}} am \subseteq a \left(\sum_{m \in \mathcal{F}} m \right).$$

Inversement, l'idéal $a \left(\sum_{m \in \mathcal{F}} m \right)$ est le groupe additif engendré par les produits ax , où

$$a \in a, \quad x \in \sum_{m \in \mathcal{F}} m,$$

ce qui entraîne

$$x = m_1 + \dots + m_\lambda, \quad \text{où} \quad m_i \in m_i \quad \text{et} \quad m_i \in \mathcal{F},$$

d'où

$$ax = am_1 + \dots + am_\lambda \in \sum_{m \in \mathcal{F}} am \quad \text{et} \quad a \left(\sum_{m \in \mathcal{F}} m \right) \subseteq \sum_{m \in \mathcal{F}} am;$$

nous avons finalement l'égalité

$$(2) \quad a \left(\sum_{m \in \mathcal{F}} m \right) = \sum_{m \in \mathcal{F}} am \quad (a \in \mathcal{J}_g, \mathcal{F} \subseteq \mathcal{J}_g),$$

formule de distributivité à gauche de la multiplication par rapport à

l'addition. On établit de même la *formule de distributivité à droite* :

$$(3) \quad \left(\sum_{m \in \mathcal{F}} m \right) a = \sum_{m \in \mathcal{F}} ma \quad (a \in \mathcal{I}_g, \mathcal{F} \subseteq \mathcal{I}_g).$$

On a, en particulier,

$$(2') \quad a(m + m') = am + am',$$

$$(3') \quad (m + m')a = ma + m'a.$$

En résumé, $\mathcal{I}_g$ est un treillis dans lequel existe, à côté de l'intersection et de l'union confondue ici avec l'addition, une troisième opération, la *multiplication*; celle-ci, d'après (2') et (3'), est *distributive par rapport à l'union* : un treillis de cette nature est appelé *treillis multiplicatif* ⁽¹⁾.

Notons qu'ici la multiplication, d'après (2) et (3), est distributive non seulement par rapport aux unions finies, mais par rapport à toute union : on dit qu'il y a *distributivité générale* de la multiplication par rapport à l'union. De plus, la multiplication est ici *associative*, ce que l'on peut exprimer en disant que $\mathcal{I}_g$ est un *demi-groupe réticulé* (c'est-à-dire demi-groupe multiplicatif et en même temps un treillis, avec distributivité).

On a, visiblement, les mêmes propriétés pour le treillis $\mathcal{I}_d$ des idéaux à droite, et le treillis $\mathcal{I}$ des idéaux bilatères. Si l'anneau R est commutatif, la multiplication dans $\mathcal{I} = \mathcal{I}_g = \mathcal{I}_d$ est, en outre, commutative.

Les relations

$$m_1 \cap m_2 \subseteq m_1, \quad m_1 \cap m_2 \subseteq m_2$$

entraînent

$$a(m_1 \cap m_2) \subseteq am_1 \cap am_2,$$

mais on n'a pas nécessairement l'égalité : nous en verrons plus loin un exemple (chap. VI, § 5, exerc. 5, p. 343).

Exercices. — 1. Soient a et b deux idéaux dans un anneau commutatif R . Si $a \subseteq b$, on a $a \cap b = a$, $a + b = b$, et réciproquement. D'autre part, la relation $a \subseteq b$ entraîne, m désignant un idéal quelconque de R : $m \cap a \subseteq m \cap b$, $m + a \subseteq m + b$; montrer, par des exemples pris dans l'anneau des entiers $\mathbb{C}$, que les réciproques ne sont pas valables.

(1) Pour l'étude de cette notion et de quelques autres, plus faibles ou plus fortes, voir G. BIRKHOFF, *Lattice theory*, chap. XIII : *Lattice ordered semi-groups* et chap. XIV : *Lattice ordered groups*; M. L. DUBREIL-JACOTIN, L. LESIEUR et R. CROISOT, *Leçons sur la Théorie des Treillis*, 2^e partie, chap. I et II (*Groupeïdes ordonnés, demi-groupes demi-réticulés ou gerbiers, groupes réticulés*, etc.).

2. Établir, pour deux idéaux $\mathfrak{a}$, $\mathfrak{b}$ d'un anneau commutatif, la relation

$$(\mathfrak{a}, \mathfrak{b}) [\mathfrak{a}, \mathfrak{b}] = (\mathfrak{a} + \mathfrak{b}) (\mathfrak{a} \cap \mathfrak{b}) \subseteq \mathfrak{a}\mathfrak{b}.$$

3. Soit e l'élément-unité d'un groupe G , fini ou infini.

1° L'ensemble des entiers relatifs m tels que l'on ait

$$x^m = e \quad \text{pour tout } x \in G$$

est un idéal $\mathfrak{a} = (a)$ dans l'anneau des entiers $\mathbb{C}$. Pour que l'on ait $a \neq 0$, il faut et il suffit que les ordres des différents éléments de G soient tous finis et ne prennent qu'un nombre fini de valeurs distinctes : cette condition étant remplie, a est le p. p. c. m. des ordres des éléments de G . L'entier a est, par définition, l'exposant du groupe G . Rattacher à cette notion celle de caractéristique d'un anneau.

2° G étant un groupe d'exposant $a > 0$, soit p un diviseur premier de a . Si a est divisible par p^α , mais non par $p^{\alpha+1}$, il existe dans G , pour tout entier β tel que $1 \leq \beta \leq \alpha$, un élément d'ordre p^β . En déduire que, dans un groupe abélien Γ d'exposant $a > 0$, tout diviseur de l'exposant, en particulier l'exposant lui-même, est l'ordre d'un élément. Dans un groupe abélien Γ , l'exposant (> 0) est le maximum de l'ordre des éléments; s'il est égal à l'ordre du groupe (supposé fini), le groupe est cyclique.

3° L'exposant d'un groupe abélien fini Γ d'ordre N est multiple de tout diviseur premier p de N . Si l'ordre d'un groupe abélien fini Γ est le produit de nombres premiers distincts, Γ est cyclique.

4. Soit R' un corps commutatif, R un anneau contenu dans R' , donc un domaine d'intégrité. Étudier la correspondance de Grell entre les idéaux de R et ceux de R' . Quels sont les idéaux fermés de R ?

12. Idéaux sans diviseurs, idéaux premiers, idéaux primaires. — Considérons un idéal $\mathfrak{m}$ dans un anneau commutatif R . Nous nous proposons d'étudier les propriétés de l'anneau des classes résiduelles $R/\mathfrak{m}$ et notamment de chercher à quelles conditions $R/\mathfrak{m}$ est un corps ou un domaine d'intégrité.

On désigne sous le nom d'*idéal sans diviseurs* (en allemand, teilerlos) un idéal $\mathfrak{m}$ n'admettant pas d'autres diviseurs que lui-même et l'idéal-unité R . Un tel idéal est encore appelé *maximal*.

THÉORÈME 1. — *Pour que l'anneau des classes résiduelles $R/\mathfrak{m}$ soit un corps, il faut que l'idéal $\mathfrak{m}$ soit sans diviseurs. Si l'anneau R possède un élément-unité, cette condition nécessaire est aussi suffisante.*

Désignons par X la classe modulo $\mathfrak{m}$ qui contient un élément x de R . Supposons que $R/\mathfrak{m}$ soit un corps : si A est une classe différente de la classe-zéro $\mathfrak{m}$ et B une classe quelconque, il existe une classe C vérifiant

la relation

$$(1) \quad AC = B.$$

Par conséquent, si a est un élément de R n'appartenant pas à $\mathfrak{m}$, et b un élément quelconque, il existe au moins un élément $c \in C$ tel que l'on ait

$$(1') \quad ac \equiv b \pmod{\mathfrak{m}}.$$

Cela étant, soit $\mathfrak{m}'$ un diviseur véritable de $\mathfrak{m}$. Il existe au moins un élément $a \in \mathfrak{m}'$ qui n'appartient pas à $\mathfrak{m}$ et, en appliquant ce qui précède, nous obtenons

$$b \equiv ac \pmod{\mathfrak{m}}.$$

d'où *a fortiori*, puisque $\mathfrak{m} \subseteq \mathfrak{m}'$, $b \equiv ac \pmod{\mathfrak{m}'}$.

Or $ac \equiv 0 \pmod{\mathfrak{m}'}$, d'où $b \equiv 0 \pmod{\mathfrak{m}'}$ quel que soit $b \in R$; il en résulte $\mathfrak{m}' = R$ et $\mathfrak{m}$ est sans diviseurs.

Réciproquement, montrons, en supposant que R possède un élément-unité, que, si $\mathfrak{m}$ est sans diviseurs, $R/\mathfrak{m}$ est un corps et, à cet effet, que l'équation (1), où les classes A et B sont données ($A \neq \mathfrak{m}$) admet au moins une solution C .

Soit a un élément de la classe A : a n'appartient pas à $\mathfrak{m}$. Nous avons donc

$$\mathfrak{m} + (a) = R,$$

puisque l'idéal figurant au premier membre est un véritable diviseur de $\mathfrak{m}$, d'où, pour tout élément b de R

$$b = m + x \quad \text{où } x \in (a) \text{ et } m \equiv 0 \pmod{\mathfrak{m}}.$$

Comme R admet un élément-unité, nous avons $x = ca$, où $c \in R$, d'où, en revenant aux classes correspondantes

$$B = CA,$$

ce qu'il fallait démontrer.

Tout idéal $\mathfrak{p}$ de l'anneau R tel que l'anneau des classes résiduelles $R/\mathfrak{p}$ soit un *domaine d'intégrité* est, par définition, un *idéal premier*. Pour que $\mathfrak{p}$ soit premier, il faut et il suffit, en désignant par $O (= \mathfrak{p})$ l'élément-zéro de $R/\mathfrak{p}$, par A, B les classes modulo $\mathfrak{p}$ qui contiennent deux éléments a, b de R , que les relations

$$AB = O, \quad A \neq O, \quad B \neq O$$

soient *incompatibles*, donc, en revenant aux éléments de R , que les

relations

$$ab \in \mathfrak{p}, \quad a \notin \mathfrak{p}, \quad b \notin \mathfrak{p}$$

soient incompatibles ⁽¹⁾.

Par conséquent, *pour qu'un idéal $\mathfrak{p}$ soit premier, il faut et il suffit que les relations*

$$(2) \quad ab \in \mathfrak{p}, \quad a \notin \mathfrak{p}$$

entraînent

$$(3) \quad b \in \mathfrak{p}.$$

On peut, dans cette condition, remplacer les éléments par des idéaux et le signe $\in$ par le signe $\subseteq$: *pour qu'un idéal $\mathfrak{p}$ soit premier, il faut et il suffit que les relations*

$$(2') \quad ab \subseteq \mathfrak{p}, \quad a \not\subseteq \mathfrak{p}$$

entraînent

$$(3') \quad b \subseteq \mathfrak{p}.$$

Si, en effet, $(2')$ entraîne $(3')$, et si deux éléments a, b de R vérifient les relations (2) , les idéaux principaux $\mathfrak{a} = (a)$, $\mathfrak{b} = (b)$ vérifient les relations $(2')$; on a donc $(3')$, d'où $b \in \mathfrak{p}$, donc $\mathfrak{p}$ est premier.

Inversement, supposons $\mathfrak{p}$ premier, et soient $\mathfrak{a}$ et $\mathfrak{b}$ deux idéaux vérifiant les relations $(2')$. Il existe au moins un élément $a \in \mathfrak{a}$ n'appartenant pas à $\mathfrak{p}$; on a, d'autre part, pour tout $b \in \mathfrak{b}$

$$ab \in \mathfrak{ab} \subseteq \mathfrak{p}.$$

Les relations (2) sont donc vérifiées. Comme $\mathfrak{p}$ est premier, on a la relation (3) , d'où

$$b \subseteq \mathfrak{p},$$

c'est-à-dire $(3')$.

L'idéal-unité est premier. Pour que, dans un anneau R , l'idéal (0) soit premier, il faut et il suffit que R soit un domaine d'intégrité.

D'après le théorème 1, *tout idéal sans diviseurs dans un anneau R possédant un élément-unité, est premier* (puisque tout corps est un domaine d'intégrité).

Si $\mathfrak{p}$ est un idéal premier dans un anneau R et si, en outre, le domaine d'intégrité $R/\mathfrak{p}$ est fini, ce domaine est un corps et, par suite, $\mathfrak{p}$ est un idéal sans diviseurs. Ce cas se présente dans l'anneau des entiers $\mathbb{C}$,

⁽¹⁾ Ou, ce qui revient au même, que l'ensemble $R - \mathfrak{p}$ soit multiplicativement fermé.

dans lequel tout idéal $\mathfrak{m}$ est principal, $\mathfrak{m} = (m)$ et où, par conséquent, $C/(m)$ est fini dès que $m \neq 0$; il y a donc, dans C , identité entre les idéaux premiers *non nuls* et les idéaux sans diviseurs; pour que l'idéal $\mathfrak{p} = (p)$ soit premier ($p \neq 0$), il faut et il suffit que p soit un nombre premier.

Quant à l'idéal (0) , il est premier dans C , mais n'est pas sans diviseurs.

On donne le nom d'*idéal primaire*, dans un anneau commutatif R , à tout idéal $\mathfrak{q}$ tel que, dans l'anneau $R/\mathfrak{q}$ des classes résiduelles, tout diviseur de zéro soit nilpotent. Pour que $\mathfrak{q}$ soit primaire, il faut et il suffit que les relations (dans $R/\mathfrak{q}$)

$$AB = 0, \quad A \neq 0, \quad B^n \neq 0 \quad \text{pour tout entier naturel } n$$

soient *incompatibles*, donc, en revenant à l'anneau R , que les relations

$$ab \in \mathfrak{q}, \quad a \notin \mathfrak{q}$$

entraînent :

Il existe un nombre naturel h tel que $(^1) b^h \in \mathfrak{q}$.

Tout idéal premier est primaire.

Exemple. — Dans l'anneau C des entiers, tout idéal de la forme $\mathfrak{q} = (p^\alpha)$ où p est un nombre premier et α un nombre naturel, est primaire (*cf.* exerc. 3, p. 185).

Pour établir une propriété importante des idéaux primaires, nous aurons besoin de la remarque suivante. Considérons un idéal $\mathfrak{m}$ quelconque dans un anneau R , et h éléments $a_1, a_2, \dots, a_h$ de R vérifiant des relations de la forme

$$a_i^{\sigma_i} \in \mathfrak{m},$$

où les σ_i sont des nombres naturels. *En posant*

$$\mathfrak{a} = (a_1, a_2, \dots, a_h),$$

on a la relation

$$\mathfrak{a}^\alpha \subseteq \mathfrak{m},$$

dès que le nombre naturel α est assez grand.

(¹) On peut encore mettre cette condition sous la forme équivalente

$$ab \in \mathfrak{q} \quad \text{et} \quad \text{aucune puissance de } b \text{ n'appartient à } \mathfrak{q}$$

entraînent

$$a \in \mathfrak{q}.$$

Un élément x de $\mathfrak{a}^x$ est, en effet, la somme d'un nombre fini de termes de la forme

$$\pi = (n_1 a_{i_1} + r_1 a_{i_1}) \dots (n_\alpha a_{i_\alpha} + r_\alpha a_{i_\alpha}),$$

où les n_k sont des entiers relatifs, les r_k des éléments de R , les a_{i_k} certains des éléments $a_1, a_2, \dots, a_h$. Si l'on a

$$(4) \quad \alpha \geq \sigma_1 + \sigma_2 + \dots + \sigma_h - (h - 1),$$

il existe au moins un indice μ , parmi les nombres $1, 2, \dots, h$, tel que a_μ figure dans π un nombre de fois supérieur ou égal à σ_μ : π appartient alors à l'idéal $(a_\mu^{\sigma_\mu})$, donc à $\mathfrak{m}$. Par conséquent, l'inégalité (4) entraîne $\mathfrak{a}^\alpha \subseteq \mathfrak{m}$.

En particulier, les relations $a^\sigma \in \mathfrak{m}$, $b^\tau \in \mathfrak{m}$ entraînent

$$(a \pm b)^{\sigma+\tau-1} \in (a, b)^{\sigma+\tau-1} \subseteq \mathfrak{m}.$$

Cela posé, la propriété que nous avons en vue est la suivante.

THÉOREME 2. — *L'ensemble $\mathfrak{p}$ des éléments de l'anneau R dont une puissance appartient à un idéal primaire $\mathfrak{q}$, est un idéal premier, diviseur de $\mathfrak{q}$, appelé idéal premier associé à $\mathfrak{q}$. [Cet idéal est, d'après sa définition, le radical de $\mathfrak{q}$ (cf. exerc. 2, p. 188). On dit aussi que $\mathfrak{q}$ est un idéal primaire appartenant à $\mathfrak{p}$].*

Les relations

$$x \in \mathfrak{p}, \quad y \in \mathfrak{p}, \quad \text{c'est-à-dire} \quad x^\sigma \in \mathfrak{q}, \quad y^\tau \in \mathfrak{q}$$

entraînent

$$(x \pm y)^{\sigma+\tau-1} \in \mathfrak{q}, \quad \text{c'est-à-dire} \quad x \pm y \in \mathfrak{p}$$

et, quel que soit $r \in R$,

$$(rx)^\sigma \in \mathfrak{q}, \quad \text{donc} \quad rx \in \mathfrak{p}.$$

L'ensemble $\mathfrak{p}$ est donc un idéal.

Les relations

$$ab \in \mathfrak{p}, \quad a \notin \mathfrak{p}$$

entraînent

$$(ab)^\sigma = a^\sigma b^\sigma \in \mathfrak{q} \quad \text{et} \quad a^\sigma \notin \mathfrak{q},$$

d'où, $\mathfrak{q}$ étant primaire,

$$(b^\sigma)^h \in \mathfrak{q}, \quad \text{donc} \quad b \in \mathfrak{p}$$

et, par conséquent, $\mathfrak{p}$ est premier. On a évidemment $\mathfrak{q} \subseteq \mathfrak{p}$.

D'après les définitions, on a immédiatement la proposition suivante :

Les relations $ab \in \mathfrak{q}$ et $a \notin \mathfrak{q}$ entraînent $b \in \mathfrak{p}$. On en déduit que si deux idéaux $\mathfrak{a}$, $\mathfrak{b}$ vérifient $\mathfrak{ab} \subseteq \mathfrak{q}$ et $\mathfrak{a} \not\subseteq \mathfrak{q}$, on a $\mathfrak{b} \subseteq \mathfrak{p}$. En effet, soient b un élément quelconque de $\mathfrak{b}$, a un élément appartenant à $\mathfrak{a}$ mais non à $\mathfrak{q}$: le produit ab appartient à $\mathfrak{ab}$, donc à $\mathfrak{q}$; puisque a n'appartient pas à $\mathfrak{q}$, il en résulte $b \in \mathfrak{p}$.

Si l'idéal premier $\mathfrak{p}$ associé à $\mathfrak{q}$ admet une base finie,

$$\mathfrak{p} = (p_1, p_2, \dots, p_n),$$

ce qui a toujours lieu quand l'anneau R est noethérien, les relations

$$p_i^{\sigma_i} \subseteq \mathfrak{q}$$

entraînent

$$\mathfrak{p}^\alpha \subseteq \mathfrak{q},$$

dès que le nombre naturel α dépasse une certaine valeur. La plus petite valeur ρ de α pour laquelle cette relation est vérifiée est appelée *exposant* de l'idéal $\mathfrak{q}$.

L'idéal premier $\mathfrak{p}$ associé à $\mathfrak{q}$ est le *seul idéal premier* qui vérifie une relation de la forme

$$\mathfrak{p}^\rho \subseteq \mathfrak{q} \subseteq \mathfrak{p}.$$

Si l'on a, en effet,

$$\mathfrak{p}_1^\sigma \subseteq \mathfrak{q} \subseteq \mathfrak{p}_1,$$

où $\mathfrak{p}_1$ est un idéal premier, les relations

$$\mathfrak{p}_1^\sigma \subseteq \mathfrak{p} \quad \text{et} \quad \mathfrak{p}^\rho \subseteq \mathfrak{p}_1$$

entraînent

$$\mathfrak{p}_1 \subseteq \mathfrak{p} \quad \text{et} \quad \mathfrak{p} \subseteq \mathfrak{p}_1,$$

donc

$$\mathfrak{p} = \mathfrak{p}_1.$$

Si un anneau R possède un élément-unité 1, on a

$$R\rho = R = (1) \quad \text{quel que soit } \rho.$$

Il n'existe donc pas d'autre idéal primaire appartenant à R que l'idéal unité R .

Dans tout anneau commutatif R , un idéal $\mathfrak{q}$ tel que les relations

$$\mathfrak{ab} \subseteq \mathfrak{q}, \quad \mathfrak{a} \not\subseteq \mathfrak{q},$$

où $\mathfrak{a}$ et $\mathfrak{b}$ sont deux idéaux, entraînent :

$$\text{Il existe un nombre naturel } \beta \text{ tel que } \mathfrak{b}^\beta \subseteq \mathfrak{q}$$

est *primaire*. Si l'on a, en effet,

$$ab \in \mathfrak{q}, \quad a \notin \mathfrak{q},$$

on obtient, en considérant les idéaux principaux $\mathfrak{a} = (a)$, $\mathfrak{b} = (b)$,

$$b^\beta \in \mathfrak{b}^\beta \subseteq \mathfrak{q}.$$

Inversement, considérons un idéal *primaire* $\mathfrak{q}$ et deux idéaux $\mathfrak{a}$ et $\mathfrak{b}$ vérifiant les relations

$$\mathfrak{ab} \subseteq \mathfrak{q}, \quad \mathfrak{a} \not\subseteq \mathfrak{q}$$

et supposons, en outre, que l'idéal $\mathfrak{b}$ admette une base finie

$$\mathfrak{b} = (b_1, b_2, \dots, b_n).$$

Il existe au moins un élément a de $\mathfrak{a}$ n'appartenant pas à $\mathfrak{q}$ et nous avons

$$ab_i \in \mathfrak{ab} \subseteq \mathfrak{q}, \quad a \notin \mathfrak{q},$$

d'où

$$b_i^{\beta_i} \in \mathfrak{q}$$

et, par suite,

$$\mathfrak{b}^\beta \subseteq \mathfrak{q},$$

dès que β est assez grand.

Nous indiquerons encore deux résultats souvent utiles.
Soient $\mathfrak{p}$ et $\mathfrak{q}$ deux idéaux ayant les propriétés suivantes :

- 1° $\mathfrak{q} \subseteq \mathfrak{p}$;
- 2° Si $b \in \mathfrak{p}$, il existe un entier positif β tel que $b^\beta \in \mathfrak{q}$;
- 3° $ab \in \mathfrak{q}$, $a \notin \mathfrak{q}$ entraînent $b \in \mathfrak{p}$.

L'idéal $\mathfrak{q}$ est primaire et $\mathfrak{p}$ est l'idéal premier associé à $\mathfrak{q}$.

Soit, en effet,

$$ab \in \mathfrak{q}, \quad a \notin \mathfrak{q}.$$

On a, d'après 3° et 2°,

$$b^\beta \in \mathfrak{q}$$

et, par suite, $\mathfrak{q}$ est primaire. D'autre part, d'après 2°, tout élément de $\mathfrak{p}$ a une puissance contenue dans $\mathfrak{q}$. Inversement, considérons un élément x dont une puissance appartient à $\mathfrak{q}$, et soit m le plus petit entier positif tel que l'on ait

$$x^m \in \mathfrak{q}.$$

Si $m = 1$, nous avons, d'après 1°,

$$x \in \mathfrak{p}.$$

Si m est supérieur à 1, nous avons

$$x^{m-1} \cdot x \in \mathfrak{q}, \quad \text{avec} \quad x^{m-1} \notin \mathfrak{q},$$

d'où, d'après 3°,

$$x \in \mathfrak{p}.$$

L'idéal $\mathfrak{p}$ est donc l'ensemble des éléments de l'anneau dont une puissance appartient à $\mathfrak{q}$, c'est-à-dire l'idéal premier associé à $\mathfrak{q}$.

Supposons maintenant que l'anneau R ait un *élément-unité*, que deux idéaux $\mathfrak{p}$ et $\mathfrak{q}$ de R possèdent les *propriétés* 1° et 2° et qu'en outre :

4° $\mathfrak{p}$ soit un idéal sans diviseurs ($\mathfrak{p} \neq R$).

L'idéal $\mathfrak{q}$ est primaire et $\mathfrak{p}$ est l'idéal premier associé à $\mathfrak{q}$.

Soit, en effet,

$$ab \in \mathfrak{q} \quad \text{et} \quad a^n \notin \mathfrak{q} \quad \text{quel que soit } n.$$

Nous avons, d'après 2°,

$$a \notin \mathfrak{p}, \quad \text{donc} \quad (\mathfrak{p}, a) = R,$$

d'où

$$1 = p + ra, \quad \text{avec} \quad p \in \mathfrak{p}, \quad \text{donc} \quad p^\sigma \in \mathfrak{q}.$$

L'égalité précédente entraîne

$$b = pb + rab, \quad \text{d'où} \quad b \equiv pb \pmod{\mathfrak{q}}$$

et, en multipliant cette congruence par les puissances de p ,

$$b \equiv pb \equiv p^2 b \equiv \dots \equiv p^\sigma b \equiv 0 \pmod{\mathfrak{q}}.$$

L'idéal $\mathfrak{q}$ est donc bien primaire.

On a de plus, d'après 1° et 4°,

$$\mathfrak{q} \neq R,$$

donc l'idéal premier $\bar{\mathfrak{p}}$ associé à $\mathfrak{q}$ est aussi différent de R . D'autre part,

$$x \in \mathfrak{p} \quad \text{entraîne} \quad x^n \in \mathfrak{q} \subseteq \bar{\mathfrak{p}},$$

d'où $x \in \bar{\mathfrak{p}}$. On a donc

$$\mathfrak{p} \subseteq \bar{\mathfrak{p}} \subset R \quad \text{et, par suite,} \quad \mathfrak{p} = \bar{\mathfrak{p}}.$$

Remarque. — Les résultats précédents subsistent si l'on remplace la condition 2° par la condition (plus forte ou équivalente)

$$(2') \quad \mathfrak{p}^2 \subseteq \mathfrak{q}.$$

L'intérêt de la notion d'idéal primaire vient surtout du théorème suivant, dû à E. Noether ⁽¹⁾, et qui généralise le théorème de décomposition d'un nombre en produit de puissances de facteurs premiers.

THÉORÈME DE DÉCOMPOSITION. — *Dans un anneau noethérien, chaque idéal est l'intersection d'un nombre fini d'idéaux primaires* ⁽²⁾.

Exercices. — 1. Dans l'anneau des entiers pairs, l'idéal principal (4) n'est pas premier, mais il est sans diviseurs. (L'hypothèse concernant l'existence d'un élément-unité est donc essentielle dans la seconde partie du théorème 1).

2. Dans l'anneau des entiers C , on considère un nombre premier p et l'idéal primaire $\mathfrak{q} = (p^\alpha)$. Quel est l'idéal premier $\mathfrak{p}$ associé à $\mathfrak{q}$? Quel est l'exposant de $\mathfrak{q}$?

3. Dans l'anneau des entiers C , tout idéal primaire est de la forme (p^α) , où p est un nombre premier, α un nombre naturel ⁽³⁾.

13. Condition maximale. Base finie. Axiome des chaînes de diviseurs. — Soit $\mathcal{I}$ le treillis des idéaux d'un anneau commutatif R ; nous nous proposons de montrer que *l'axiome de la base finie, pour l'anneau R , est équivalent à la condition maximale pour l'ensemble partiellement ordonné $\mathcal{I}$, donc aussi, moyennant l'axiome du choix, à la condition de chaîne ascendante dans $\mathcal{I}$* (chap. I, § 11, p. 50).

La condition maximale dans $\mathcal{I}$ signifie que, dans tout ensemble $\mathcal{E}$ non vide d'idéaux, il y a au moins un idéal $\mathfrak{m}$ maximal dans $\mathcal{E}$, c'est-à-dire qui n'est contenu dans aucun autre idéal $\mathfrak{m}' \in \mathcal{E}$; il est commode d'exprimer cette propriété en disant que *l'anneau R vérifie la condition maximale* ⁽⁴⁾; le mode de raisonnement par induction correspon-

⁽¹⁾ E. NOETHER, *Idealtheorie in Ringbereichen* (*Math. Ann.*, t. 83, 1921, p. 24-66). Dans le cas particulier des anneaux de polynômes (à coefficients dans un corps), le théorème a été établi par E. LASKER, *Zur theorie der Moduln und Ideale* (*Math. Ann.*, t. 60, 1905, p. 20-116); ces anneaux sont noethériens d'après un théorème dû à Hilbert (voir chap. VI, § 5, p. 331).

⁽²⁾ Voir § 14, p. 212.

⁽³⁾ Cf. Exerc. 3, § 9 p. 185. Il y a identité, dans l'anneau des entiers C , entre les idéaux primaires et les puissances d'idéaux premiers. Nous rencontrerons plus loin (Chap. VI, § 5, p. 342) des anneaux où il existe des idéaux primaires qui ne sont pas puissances d'idéaux premiers, et des puissances d'idéaux premiers qui ne sont pas primaires.

⁽⁴⁾ En remplaçant les mots « maximal » et « qui n'est contenu » par les mots « minimal » et « qui ne contient », on obtient l'énoncé de l'axiome symétrique, la *condition minimale*. Un anneau commutatif, ayant un élément-unité et vérifiant la condition minimale, est appelé *anneau d'Artin*. On démontre que *tout anneau d'Artin est noethérien*, [voir P. SAMUEL, *La notion de multiplicité en Algèbre et en Géométrie algébrique* (*J. de math. pures et appl.*, t. 30, 1951, p. 159); *Thèse*, Paris, 1949, chap. I, § 1]. Ce théorème se rattache d'une part à la théorie des anneaux non commutatifs

dant (p. 51), prend le nom de *principe d'induction sur les diviseurs* : pour montrer que tous les idéaux de R ont une certaine propriété P , il suffit d'établir que, si un idéal α n'avait pas cette propriété, il existerait un diviseur véritable α' de α , $\alpha' \supset \alpha$, ne l'ayant pas non plus (ce qui exige en particulier que l'anneau R , idéal maximum, ait cette propriété).

Dire que $\mathcal{J}$ vérifie la *condition de chaîne ascendante* signifie que toute suite monotone croissante d'idéaux de R

$$\alpha_1 \subset \alpha_2 \subset \dots$$

est nécessairement finie, ou, ce qui revient au même, que dans toute suite monotone non décroissante

$$\alpha_1 \subseteq \alpha_2 \subseteq \dots$$

tous les idéaux sont égaux à partir d'un certain rang. On exprime commodément cette condition en disant que *l'anneau R vérifie l'axiome des chaînes de diviseurs* (en allemand, *Teilerkettensatz*, ou *O-Satz*).

Indiquons d'abord les propositions qui ne font intervenir ni l'axiome du choix, ni aucun principe équivalent.

THÉOREME 1. — *Pour un anneau R la condition maximale entraîne l'axiome de la base finie.*

Soit α un idéal de R ; l'ensemble $\mathcal{E}$ des idéaux contenus dans α et ayant une base finie, n'est pas vide, puisqu'il comprend tout idéal engendré par une partie finie de α . Il existe dans $\mathcal{E}$ au moins un *élément maximal* $\mathfrak{m} = (m_1, \dots, m_r) \subseteq \alpha$. Si $\mathfrak{m}$ était différent de α , il y aurait au moins un élément x de α n'appartenant pas à $\mathfrak{m}$; l'idéal $\mathfrak{m}' = (m_1, \dots, m_r, x)$, véritable diviseur de $\mathfrak{m}$, ferait encore partie de l'ensemble $\mathcal{E}$, ce qui est contradictoire. Nous avons donc

$$\alpha = \mathfrak{m} = (m_1, \dots, m_r).$$

LEMME 1. — *Soit $\mathcal{C}$ une chaîne d'idéaux d'un anneau R . La réunion $\mathfrak{m} = \bigcup_{\alpha \in \mathcal{C}} \alpha$ (au sens de la théorie des ensembles) est un idéal; l'ensemble partiellement ordonné $\mathcal{J}$ de tous les idéaux de R est inductif.*

[cf. N. JACOBSON, *The Theory of Rings* (Math. Surv., t. II, chap. IV)], d'autre part, à celle des treillis multiplicatifs [cf. L. LESIEUR, *Conditions suffisantes pour que, dans un treillis multiplicatif complet, la condition de chaîne descendante entraîne la condition de chaîne ascendante* (C. R. Acad. Sc., t. 234, 1952, p. 1017)].

Soit

$$m \in \mathfrak{m} = \bigcup_{\alpha \in \mathcal{C}} \alpha;$$

nous avons $m \in \alpha$ pour au moins un idéal $\alpha \in \mathcal{C}$; il en résulte $rm \in \alpha$ quel que soit $r \in R$, donc $rm \in \mathfrak{m}$. Soit, en outre, $m' \in \mathfrak{m}$, donc $m' \in \alpha'$ pour au moins un idéal $\alpha' \in \mathcal{C}$. $\mathcal{C}$ étant une chaîne, l'un des idéaux α , α' contient l'autre et comprend à la fois m et m' , donc $m - m'$, d'où $m - m' \in \mathfrak{m}$; donc, $\mathfrak{m}$ est un idéal, qui est borne supérieure de $\mathcal{C}$ dans $\mathcal{J}$, puisqu'il l'est, d'après sa définition, dans $\mathcal{T}(R)$. Étant donné que toute chaîne $\mathcal{C}$ extraite de $\mathcal{J}$ possède, dans $\mathcal{J}$, une borne supérieure, $\mathcal{J}$ est un ensemble inductif.

Dans le cas d'un anneau noethérien, on a une proposition plus forte.

THEOREME 2. — *Si un anneau R vérifie l'axiome de la base finie, toute chaîne d'idéaux $\mathcal{C}$ contient un idéal maximum, tout ensemble non vide d'idéaux, $\mathcal{S}$, est inductif, et l'anneau R vérifie l'axiome des chaînes de diviseurs.*

Soit $\mathcal{C}$ une chaîne d'idéaux; l'idéal $\mathfrak{m} = \bigcup_{\alpha \in \mathcal{C}} \alpha$, borne supérieure de $\mathcal{C}$ dans $\mathcal{J}$ d'après le lemme 1, a ici une base finie :

$$\mathfrak{m} = (m_1, \dots, m_r).$$

On a, pour chaque indice i , $m_i \in \alpha_i$, $\alpha_i \in \mathcal{C}$; or, l'un des idéaux $\alpha_1, \dots, \alpha_r$ contient tous les autres : cet idéal, α^* , comprend donc tous les générateurs m_i de $\mathfrak{m}$, d'où $\mathfrak{m} \subseteq \alpha^*$, alors que, d'après la définition de $\mathfrak{m}$, nous avons $\alpha^* \subseteq \mathfrak{m}$, d'où $\mathfrak{m} = \alpha^* \in \mathcal{C}$; la borne supérieure $\mathfrak{m}$ de $\mathcal{C}$, appartenant à $\mathcal{C}$, en est élément maximum.

En appliquant ce qui précède à une chaîne $\mathcal{C}$ extraite d'un ensemble non vide, $\mathcal{S}$, d'idéaux, nous voyons que $\mathcal{S}$ est inductif.

Une suite monotone non décroissante d'idéaux

$$\alpha_1 \subseteq \alpha_2 \subseteq \dots \subseteq \alpha_n \subseteq \dots$$

contient en particulier, un idéal maximum, ce qui exige que les idéaux α_i coïncident à partir d'un certain rang : l'anneau R vérifie l'axiome des chaînes de diviseurs.

Indiquons encore une conséquence du lemme 1.

LEMME 2. — *Dans un anneau commutatif R avec élément-unité e , l'ensemble $\mathcal{J}'$ des idéaux distincts de R est inductif.*

Considérons une chaîne $\mathcal{C}$ extraite de $\mathcal{J}'$ et l'idéal $\mathfrak{m} = \bigcup_{\alpha \in \mathcal{C}} \alpha$ borne supérieure de $\mathcal{C}$ dans $\mathcal{J}$. L'égalité $\mathfrak{m} = R$ entraînerait $e \in \mathfrak{m}$, donc $e \in \alpha$ pour au moins un α de $\mathcal{C}$, d'où $\alpha = R$, ce qui est impossible, puisque

$$\alpha \in \mathcal{C} \subseteq \mathcal{J}' = \mathcal{J} - \{R\}.$$

Nous avons donc $\mathfrak{m} \subset R$, *strictement*, c'est-à-dire $\mathfrak{m} \in \mathcal{J}'$: $\mathcal{J}'$ est inductif.

Dans ce qui précède, nous avons obtenu, entre les trois axiomes considérés : condition maximale (CM), axiome de la base finie (BF), axiome des chaînes de diviseurs (CD), les implications

$$CM \Rightarrow BF \Rightarrow CD.$$

Pour établir leur *équivalence*, il suffit de montrer que $CD \Rightarrow CM$: la démonstration, qui est d'ailleurs immédiate, mais fait intervenir l'*axiome du choix*, a été donnée plus haut (chap. I, § 11, p. 50) quand nous avons vu, d'une façon générale que *la condition de chaîne ascendante entraîne la condition maximale*. En définitive, *les anneaux noethériens sont caractérisés par l'un quelconque des trois axiomes CM, BF, CD*.

Le *principe de Zorn* permet de voir directement que *l'axiome de la base finie entraîne la condition maximale*. Ce principe s'énonce ici : *dans tout ensemble inductif $\mathcal{E}$ d'idéaux existe au moins un idéal maximal dans $\mathcal{E}$* . Or, d'après le théorème 2, tout ensemble $\mathcal{E} \neq \emptyset$ d'idéaux d'un anneau R vérifiant l'*axiome de la base finie*, est inductif : la condition maximale en résulte.

En utilisant encore le principe de Zorn et en tenant compte du lemme 2, on obtient le théorème suivant.

THÉORÈME 3. — *Dans un anneau commutatif R qui possède un élément-unité e (mais n'est pas supposé noethérien), tout idéal $\mathfrak{m} \neq R$ est contenu dans un idéal maximal $\mathfrak{p} \neq R$, c'est-à-dire dans un idéal sans diviseurs et, par conséquent, premier (§ 12, p. 199).*

Exercice. — Soit $\bar{R}$ un anneau homomorphe à un anneau R . L'ensemble de toutes les images inverses, dans R , des éléments d'un idéal $\bar{\mathfrak{a}}$ de $\bar{R}$, est un idéal $\mathfrak{a}$. Si R est noethérien, $\bar{R}$ l'est aussi ⁽¹⁾.

⁽¹⁾ Voir t. II. Notons aussi qu'un anneau noethérien peut avoir des sous-anneaux ou des sur-anneaux qui ne sont pas noethériens (cf. chap. VI, § 5, p. 337).

14. **Décomposition en facteurs dans un demi-groupe abélien avec élément-unité** ⁽¹⁾. — Soit D un *demi-groupe abélien* par rapport à une opération O , possédant un *élément neutre* e . Associons à l'opération O la relation binaire $\mathcal{S}$ définie dans D par

$$a\mathcal{S}b \quad (a, b \in D) \quad \text{si l'on a} \quad a = bOr, \quad r \in D.$$

La relation $\mathcal{S}$ est un *préordre*, appelé *préordre de décomposition* (relatif à l'opération O). En effet, $\mathcal{S}$ est *réflexive*, puisqu'on a : $a = aOe$; d'autre part, les relations

$$a = bOr, \quad b = cOs \quad \text{entraînent} \quad a = cO(sOr),$$

donc $\mathcal{S}$ est *transitive*.

Pour que $\mathcal{S}$ soit un *ordre partiel*, il faut et il suffit que $\mathcal{S}$ soit *propre*, donc que $a\mathcal{S}b$ et $b\mathcal{S}a$, c'est-à-dire

$$a = bOr \quad \text{et} \quad b = aOr', \quad \text{entraînent} \quad a = b,$$

donc que le demi-groupe D soit un *holoïde* ⁽²⁾. Lorsqu'il en est ainsi, l'élément-neutre e est élément maximum (ce qu'on exprime encore en disant que le demi-groupe partiellement ordonné D est *entier*).

Si $\mathcal{S}$ est un *ordre total*, l'holoïde D est dit *linéaire*.

Dans le cas général où $\mathcal{S}$ est seulement un *préordre*, la relation

$$\mathcal{R} = \mathcal{S} \cap \mathcal{S}^{-1}$$

est, comme nous l'avons vu (chap. I, § 5, th. 3, p. 23) une *équivalence*, que nous appellerons *équivalence de décomposition*. $\mathcal{R}$ respecte $\mathcal{S}$ et, dans l'ensemble-quotient $\bar{D} = D/\mathcal{R}$, l'image $\bar{\mathcal{S}}$ de $\mathcal{S}$ est un *ordre partiel* que nous noterons également $\subseteq$. Rappelons que l'on a, dans $\bar{D}$, $\bar{a}\bar{\mathcal{S}}\bar{b}$ dès qu'il existe une image inverse a de $\bar{a}$ et une image inverse b de $\bar{b}$ vérifiant $a\mathcal{S}b$, et alors des images inverses *quelconques* de $\bar{a}$ et $\bar{b}$ ont la même propriété (*ibid.*, th. 2, p. 22). Deux éléments de D équivalents modulo $\mathcal{R}$ sont dits *associés*.

La relation d'équivalence $\mathcal{R}$ est régulière par rapport à l'opéra-

(1) La décomposition en facteurs donne lieu à une étude différente, d'ailleurs plus complexe, lorsqu'on part d'un groupoïde avec élément-unité dans lequel existe *a priori* une relation d'ordre partiel, en particulier d'un demi-groupe demi-réticulé ou gerbier. Voir M. L. DUBREIL-JACOTIN, *Quelques propriétés arithmétiques dans un demi-groupe demi-réticulé entier* (C. R. Acad. Sc., t. 232, 1551, p. 1174); M. L. DUBREIL-JACOTIN, L. LESIEUR et R. CROISOT, *Leçons sur la Théorie des Treillis*, 2^e partie, chap. V.

(2) Cf. chap. II, § 5, p. 81, où l'on trouvera les indications bibliographiques concernant cette notion introduite par F. Klein-Barmen.

tion O . Soit, en effet, $a = b(\mathcal{R})$, c'est-à-dire $a = bOr$ et $b = aOs$; nous avons

$$aOx = (bOx)Or, \quad bOx = (aOx)Os, \quad \text{d'où} \quad aOx \equiv bOx \quad (\mathcal{R}).$$

On peut donc définir, à partir de O , une opération $\bar{O}$ dans l'ensemble quotient $\bar{D} = D/\mathcal{R}$ qui en fait un groupoïde *homomorphe* à D , donc un *demi-groupe abélien avec élément neutre $\bar{e}$* .

Montrons que l'image $\bar{\mathcal{S}}$ de $\mathcal{S}$ est la relation définie dans $\bar{D}$ à partir de $\bar{O}$ comme $\mathcal{S}$ dans D , à partir de O . Soit $\bar{a}\bar{\mathcal{S}}\bar{b}$; si a, b sont, dans D , des images inverses de $\bar{a}, \bar{b}$, nous avons $a\mathcal{S}b$, c'est-à-dire

$$a = bOr, \quad \text{d'où} \quad \bar{a} = \bar{b}\bar{O}\bar{r}.$$

Inversement, $\bar{a} = \bar{b}\bar{O}\bar{r}$ entraîne, pour des images inverses quelconques a, b, r , $a \equiv bOr \quad (\mathcal{R})$, d'où, en particulier, $a\mathcal{S}(bOr)$, c'est-à-dire

$$a = (bOr)Or' = bO(rOr'),$$

donc $a\mathcal{S}b$ et, par conséquent, $\bar{a}\bar{\mathcal{S}}\bar{b}$.

Puisque $\bar{\mathcal{S}}$ est un ordre partiel, le demi-groupe $\bar{D}$ est un *holoïde*.

Nous appellerons *décomposition* de a , dans D , toute relation de la forme

$$(1) \quad a \equiv bOc \quad (\mathcal{R}),$$

b et c seront appelés *facteurs de décomposition* de a ; la décomposition (1) est *effective* si aucun des facteurs de décomposition b, c n'est congru à a modulo $\mathcal{R}$; dans le cas contraire, la décomposition est dite *banale*. Tout élément a admet au moins la décomposition banale $a = aOe$; un élément i n'admettant aucune décomposition effective est dit *irréductible*. Ces notions s'appliquent, en particulier, au cas d'un *holoïde*: alors, l'équivalence $\mathcal{R}$ est l'égalité.

A la décomposition (1) de a dans D correspond, dans l'*holoïde* $\bar{D}$, la décomposition

$$(2) \quad \bar{a} = \bar{b}\bar{O}\bar{c}$$

et, inversement, (2) entraîne (1) pour des images inverses quelconques a, b, c de $\bar{a}, \bar{b}, \bar{c}$; les décompositions correspondantes (1) et (2) sont *effectives en même temps*, puisque les relations $a \equiv b(\mathcal{R})$ et $\bar{a} = \bar{b}$ ont lieu en même temps. Il en résulte que l'image $\bar{i}$ d'un élément i , irréductible, de D , est un élément irréductible de $\bar{D}$; de même, toute

image inverse i d'un élément $\bar{i}$ irréductible de $\bar{D}$, est un élément irréductible de D .

THÉORÈME 1. — 1° Si l'ensemble $\bar{D}$ partiellement ordonné par $\bar{\mathcal{S}}$ (que nous noterons $\subseteq$) vérifie la condition maximale (ou, ce qui revient au même, la condition de chaîne ascendante), tout élément $\bar{a}$ de $\bar{D}$ admet une représentation au moyen d'un nombre fini d'éléments irréductibles

$$(3) \quad \bar{a} = \bar{i}_1 \bar{O} \dots \bar{O} \bar{i}_n \quad (n \geq 1).$$

2° Dans D , tout élément a admet la représentation correspondante

$$(4) \quad a \equiv i_1 O \dots O i_n \quad (\mathcal{R}).$$

Tout élément irréductible $\bar{i}$ de $\bar{D}$, en particulier l'élément neutre $\bar{e}$ (élément maximum), vérifie l'équation (3) avec $n = 1$. Si donc un élément $\bar{a}$ n'admettait aucune représentation finie de la forme (3), il serait décomposable

$$\bar{a} = \bar{x} \bar{O} \bar{y} \quad (\bar{a} \subset \bar{x}, \bar{a} \subset \bar{y}),$$

et l'un au moins des éléments $\bar{x}$, $\bar{y}$ devrait, à son tour, n'admettre aucune représentation finie de la forme (3) : la première partie du théorème en résulte immédiatement, en appliquant la condition maximale sous la forme du principe d'induction associé (chap I, § 11, p. 51).

La représentation (4) résulte de (3).

Étudions quelques cas particuliers importants.

A. L'opération O de D est idempotente. — Remplaçons le signe O par le signe $\cap$; l'opération $\cap$ de D étant associative, commutative et idempotente, D est un $\cap$ -demi-treillis (chap. II, § 6, remarque p. 97) dans lequel la relation d'ordre $\subseteq$ est définie par

$$x \subseteq y \quad \text{si} \quad x = x \cap y;$$

e est donc élément maximum; de plus, $x \subseteq y$ entraîne $x \mathcal{S} y$; inversement, si l'on a $x \mathcal{S} y$, c'est-à-dire $x = y \cap r$, on en déduit

$$x \cap y = (y \cap r) \cap y = (y \cap y) \cap r = y \cap r = x,$$

c'est-à-dire $x \subseteq y$: $\mathcal{S}$ coïncide donc avec la relation d'ordre partiel du demi-treillis D , D est un holoïde par rapport à l'opération $\cap$, et $\mathcal{R}$ est l'égalité. Réciproquement, il est clair que tout $\cap$ -demi-treillis avec élément maximum, est un holoïde par rapport à l'opération $\cap$.

Le théorème général prend la forme suivante (facile d'ailleurs à établir directement).

THÉORÈME 2. — *Dans un $\cap$ -demi-treillis D vérifiant la condition maximale ⁽¹⁾ tout élément est l'intersection d'un nombre fini d'éléments irréductibles.*

Ce théorème s'applique en particulier à un treillis, et le théorème dual est évidemment valable.

Dans un anneau, un idéal irréductible se définit comme un idéal qui n'est pas l'intersection de deux diviseurs véritables : en considérant l'ensemble $\mathcal{I}$ des idéaux d'un anneau commutatif R comme un $\cap$ -demi-treillis, nous obtenons la première partie du théorème suivant.

THÉORÈME 3 (théorème de décomposition dans les anneaux noëthériens). — *Dans un anneau noëthérien R , tout idéal est*

- 1° *L'intersection d'un nombre fini d'idéaux irréductibles;*
- 2° *L'intersection d'un nombre fini d'idéaux primaires.*

Pour établir la deuxième partie, il suffit d'appliquer le lemme suivant.

LEMME. — *Dans un anneau noëthérien R , tout idéal irréductible est primaire.*

Démontrons la propriété équivalente : *si un idéal $\mathfrak{m}$ de R n'est pas primaire, il est réductible.*

L'idéal $\mathfrak{m}$ n'étant pas primaire, il existe deux éléments a, b de R vérifiant

$$ab \in \mathfrak{m}, \quad a \notin \mathfrak{m}, \quad b^h \notin \mathfrak{m},$$

quel que soit l'entier naturel h . Soit $\mathfrak{m}_h$ l'ensemble des éléments x de R vérifiant $xb^h \in \mathfrak{m}$; $\mathfrak{m}_h$ est visiblement un idéal, et nous avons

$$a \in \mathfrak{m}_1, \quad \text{donc} \quad \mathfrak{m} \subset \mathfrak{m}_1 \text{ (strictement),}$$

$$\mathfrak{m}_h \subseteq \mathfrak{m}_{h+1} \quad \text{quel que soit } h,$$

d'où, puisque R est noëthérien,

$$\mathfrak{m}_n = \mathfrak{m}_{n+1} = \dots$$

pour un certain entier n .

⁽¹⁾ Il n'est pas nécessaire ici de supposer l'existence d'un élément neutre pour l'opération $\cap$, c'est-à-dire d'un *élément maximum* dans D . La réflexivité de $\mathcal{S}$ résulte ici de l'idempotence de l'opération $\cap$.

L'idéal $\mathfrak{c} = \mathfrak{m} + \mathbf{R}b^n$ est un véritable diviseur de $\mathfrak{m}$, puisqu'on a

$$b^{n+1} \in \mathbf{R}b^n \subseteq \mathfrak{c} \quad \text{et} \quad b^{n+1} \notin \mathfrak{m};$$

les relations $\mathfrak{m} \subset \mathfrak{c}$ et $\mathfrak{m} \subset \mathfrak{m}_1$ entraînent $\mathfrak{m} \subseteq \mathfrak{m}_1 \cap \mathfrak{c}$: établissons l'égalité $\mathfrak{m} = \mathfrak{m}_1 \cap \mathfrak{c}$, et nous aurons bien une décomposition effective de $\mathfrak{m}$.

Soit c un élément de $\mathfrak{m}_1 \cap \mathfrak{c}$: nous avons

$$cb \in \mathfrak{m} \quad \text{et} \quad c = m + rb^n, \quad \text{avec} \quad m \in \mathfrak{m},$$

d'où

$$cb - rb^{n+1} \in \mathfrak{m} \quad \text{et, par conséquent,} \quad rb^{n+1} \in \mathfrak{m},$$

c'est-à-dire $r \in \mathfrak{m}_{n+1} = \mathfrak{m}_n$, donc $rb^n \in \mathfrak{m}$ et enfin $c \in \mathfrak{m}$. Nous avons, par conséquent, $\mathfrak{m}_1 \cap \mathfrak{c} \subseteq \mathfrak{m}$, d'où l'égalité, et le lemme est établi.

Dans un anneau commutatif quelconque, tout idéal premier $\mathfrak{p}$ est irréductible, car la relation $\mathfrak{p} = \mathfrak{a} \cap \mathfrak{b}$, avec $\mathfrak{p} \subset \mathfrak{a}$, entraîne

$$\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{a} \cap \mathfrak{b} = \mathfrak{p} \subseteq \mathfrak{b},$$

d'où, puisque $\mathfrak{p}$ est premier et $\mathfrak{a} \not\subseteq \mathfrak{p}$, $\mathfrak{b} \subseteq \mathfrak{p}$ et, par conséquent, $\mathfrak{p} = \mathfrak{b}$: la décomposition ne peut être que banale.

Lorsqu'on utilise, dans un anneau noëthérien, la représentation d'un idéal $\mathfrak{m}$ comme intersection d'idéaux premiers

$$(5) \quad \mathfrak{m} = \mathfrak{q}_1 \cap \mathfrak{q}_2 \cap \dots \cap \mathfrak{q}_\lambda,$$

il est avantageux de tenir compte de la propriété suivante :

THÉOREME 4. — *L'intersection*

$$\mathfrak{a} = \mathfrak{q}_1 \cap \dots \cap \mathfrak{q}_\alpha$$

d'idéaux premiers appartenant au même idéal premier $\mathfrak{p}$, est primaire et appartient à $\mathfrak{p}$.

1° Nous avons

$$\mathfrak{a} \subseteq \mathfrak{q}_1 \subseteq \mathfrak{p}.$$

2° Si $b \in \mathfrak{p}$, il existe un entier β_i tel que $b^{\beta_i} \in \mathfrak{q}_i$ ($i = 1, \dots, \alpha$); si $\beta = \text{Max} \{ \beta_1, \dots, \beta_\alpha \}$, nous avons $b^\beta \in \mathfrak{a}$.

3° Supposons que l'on ait $ab \in \mathfrak{a}$, $b \notin \mathfrak{p}$; on a $ab \in \mathfrak{q}_i$ donc $a \in \mathfrak{q}_i$, d'où $a \in \mathfrak{a}$.

D'après les trois propriétés précédentes, $\mathfrak{a}$ est primaire et appartient à l'idéal premier $\mathfrak{p}$ (§ 12, p. 203).

Le théorème 4 permet de remplacer par un seul idéal primaire, dans

la représentation (5), tous les idéaux primaires appartenant à un même idéal premier. Remarquons, d'autre part, que si $\mathfrak{q}_1$, par exemple, contient l'intersection $\mathfrak{q}_2 \cap \dots \cap \mathfrak{q}_\lambda$, on peut le supprimer sans altérer le second membre ($\mathfrak{q}_1$ est dit alors *superflu*). En appliquant autant que possible ces deux procédés, on aboutit à une *représentation normée*, ne comprenant aucun idéal superflu, et dans laquelle deux idéaux primaires $\mathfrak{q}_i, \mathfrak{q}_j$ appartiennent toujours à des idéaux premiers différents : $\mathfrak{p}_i \neq \mathfrak{p}_j$. Les idéaux primaires $\mathfrak{q}_i$ figurant dans une telle représentation normée sont appelés *composants primaires* de $\mathfrak{m}$, les idéaux premiers $\mathfrak{p}_i$ correspondants sont les *idéaux premiers essentiels* de $\mathfrak{m}$. Nous n'étudierons pas ici les questions d'unicité.

Remarque. — Un idéal $\mathfrak{m}$ qui admet une représentation normée comprenant plus d'un composant

$$\mathfrak{m} = \mathfrak{q}_1 \cap \mathfrak{q}_2 \cap \dots \cap \mathfrak{q}_r, \quad r \geq 2,$$

n'est pas primaire.

Soit en effet $\mathfrak{p}_i$ l'idéal premier associé à $\mathfrak{q}_i$; nous avons $\mathfrak{p}_i \neq \mathfrak{p}_j$ pour $i \neq j$; parmi les idéaux $\mathfrak{p}_1, \dots, \mathfrak{p}_r$, il y en a au moins un qui ne contient aucun des autres : supposons par exemple que $\mathfrak{p}_1$ ait cette propriété et soit

$$a_i \in \mathfrak{p}_i, \quad a_i \notin \mathfrak{p}_1 \quad (i = 2, \dots, r)$$

nous avons $a_i^{\alpha_i} \in \mathfrak{q}_i$ pour un entier α_i convenable.

Aucun des idéaux $\mathfrak{q}_2, \dots, \mathfrak{q}_r$ n'étant superflu, nous avons $\mathfrak{m} \subset \mathfrak{q}_1$ (strictement), soit donc q_1 un élément de $\mathfrak{q}_1$ n'appartenant pas à $\mathfrak{m}$. En posant $\alpha = \text{Max}(\alpha_i)$, nous avons

$$q_1(a_2 \dots a_r)^\alpha \in \mathfrak{m}, \quad q_1 \notin \mathfrak{m}.$$

Si $\mathfrak{m}$ était primaire, il en résulterait

$$(a_2 \dots a_r)^{\lambda \alpha} \in \mathfrak{m} \subseteq \mathfrak{q}_1 \subseteq \mathfrak{p}_1,$$

d'où

$$a_i \in \mathfrak{p}_1 \quad \text{pour au moins une valeur de } i,$$

ce qui est contradictoire.

La démonstration précédente est valable même si l'anneau considéré n'est pas noëthérien.

B. Soit D un demi-groupe *multiplicatif*, abélien, avec élément unité e . Tout élément x de la forme $x = ra$ est appelé *multiple* de a , a est un *diviseur* de x ; on dit aussi que a *divise* x et l'on écrit $a \mid x$; si a ne divise pas y , on écrit $a \nmid y$. La relation $\mid$ n'est autre que l'inverse $\mathcal{S}^{-1}$ de la relation $\mathcal{S}$ considérée plus haut : c'est donc aussi une relation de préordre. La recherche des diviseurs d'un élément x donné revient à déterminer les décompositions de x en produits d'éléments de D .

Les relations $a|x$, $x\mathcal{S}a$ signifient que x appartient à l'idéal principal $Da=(a)$ engendré par a ($a \in D$ a puisque D possède un élément-unité) ou encore que l'idéal (x) est contenu dans l'idéal (a) . La congruence $x \equiv y(\mathcal{R})$, c'est-à-dire $x|y$ et $y|x$, signifie donc que les idéaux principaux (x) et (y) sont confondus.

Considérons les éléments inversibles ou unités de D : si ε est une unité, son inverse ε^{-1} en est une aussi; comme le produit de deux unités est encore une unité, les unités forment un groupe E ($e \in E \subseteq D$).

La relation $\mathbf{P}$ définie par

$$x\mathbf{P}y \quad \text{si et seulement si} \quad y = \varepsilon x, \quad \text{où} \quad \varepsilon \in E$$

est réflexive, symétrique ($x = \varepsilon^{-1}y$) et transitive : c'est une relation d'équivalence, d'ailleurs régulière vis-à-vis de la multiplication. Nous avons $\mathbf{P} \subseteq \mathcal{S}$ et, par conséquent, $\mathbf{P} \subseteq \mathcal{R}$.

Supposons maintenant l'équivalence $\mathcal{R}$ simplifiable, ce qui a lieu si $\bar{D}$ est un semi-groupe, et seulement dans ce cas (§ 1, p. 144). Une congruence

$$(6) \quad a \equiv xy \quad (\mathcal{R})$$

entraîne

$$(6') \quad a = (xy)z = xy', \quad \text{avec} \quad y' = yz,$$

d'où

$$xy \equiv xy' \quad (\mathcal{R})$$

et, par conséquent,

$$y \equiv y' \quad (\mathcal{R}).$$

On peut donc transformer la congruence (6) en une égalité (6') à condition de remplacer y par un élément y' associé à y et convenablement choisi.

On voit alors, de proche en proche, que, si $\bar{D}$ vérifie la condition maximale, la représentation (3) dans $\bar{D}$ fournit, dans D , une représentation

$$(4') \quad a = i'_1 \dots i'_n$$

sous forme d'égalité, dans laquelle $i'_1, \dots, i'_n$ sont des images inverses convenablement choisies de $\bar{i}_1, \dots, \bar{i}_n$. D'une façon plus précise, on peut prendre par exemple pour $\bar{i}'_1, \dots, \bar{i}'_{n-1}$ des images inverses quelconques de $\bar{i}_1, \dots, \bar{i}_{n-1}$; i'_n doit être alors une image inverse convenable de $\bar{i}_n$.

B'. Le cas précédent se présente toutes les fois que D lui-même est un semi-groupe. En effet, la congruence $ax \equiv bx(\mathcal{R})$ signifie

$$ax = bx.r = br.x, \quad bx = ax.s = as.x,$$

d'où, puisque D est un semi-groupe, $a = br$, $b = as$, c'est-à-dire $a \equiv b(\mathcal{R})$: $\mathcal{R}$ est bien simplifiable. Si $\bar{D}$ vérifie la condition maximale, tout élément de D est le produit d'un nombre fini d'éléments irréductibles.

De plus, quand D est un semi-groupe, les équivalences $\mathcal{R}$ et $\mathbf{P}$ coïncident. Soit, en effet, $x \equiv y(\mathcal{R})$, c'est-à-dire

$$x = yr, \quad y = xs, \quad (r, s \in D).$$

Il en résulte

$$xrs = x = xe, \quad \text{d'où} \quad rs = e;$$

r et s sont des unités et nous avons bien $x \equiv y(\mathbf{P})$.

L'équivalence $\mathcal{R}$, ici, définit donc une décomposition du semi-groupe abélien D en classes par rapport à son sous-groupe E tout à fait analogue à la décomposition d'un groupe abélien par rapport à un sous-groupe.

Les classes sont formées des éléments qui engendrent un même idéal principal. Le semi-groupe multiplicatif Π des idéaux principaux est isomorphe au semi-groupe quotient $\bar{D} = D/\mathcal{R}$; Π est un holoïde ⁽¹⁾.

La décomposition (4'), valable pour tout élément a de D si $\bar{D}$ (ou Π) vérifie la condition maximale, peut s'écrire

$$(4'') \quad a = \varepsilon i_1 \dots i_n,$$

(1) Dans le semi-groupe abélien D , un élément irréductible a est un élément n'admettant pas d'autre décomposition que $\bar{a} = \bar{a}\bar{e}$.

D'une façon générale, dans un groupoïde Γ ayant un élément-unité τ , une décomposition $\alpha = \beta\gamma$ est dite triviale si

(1) ou bien $\beta = \gamma = \alpha$ (α est alors idempotent);

(2) ou bien $\beta = \alpha\tau_1, \gamma = \tau_2$ (ou $\beta = \tau_1, \gamma = \tau_2\alpha$),

τ_1, τ_2 étant inverses l'un de l'autre $\tau_1\tau_2 = \tau$; un élément α est dit *indécomposable* si toute décomposition de α est triviale (cf. M. L. DUBREIL-JACOTIN, L. LESIEUR et R. CROISOT, *Leçons sur les Treillis...*, page 218).

Ici, le semi-groupe $\bar{D}$ n'a pas d'autre élément idempotent que $\bar{e}$; de plus, $\bar{D}$ ne contient aucun élément inversible autre que $\bar{e}$. Il en résulte que, dans $\bar{D}$, les deux notions d'élément irréductible et d'élément indécomposable se confondent.

Dans le semi-groupe D , un élément irréductible est un élément a n'admettant que des décompositions de la forme $a = a_1b_1$, où par exemple $a_1 \equiv a(\mathcal{R})$, c'est-à-dire ici $a_1 = a\varepsilon_1$, ε_1 étant une unité : $\varepsilon_1\varepsilon_2 = e$; il en résulte $a = a\varepsilon_1\varepsilon_2 = a\varepsilon_1b_1$, d'où $b_1 = \varepsilon_2$. Puisque D n'admet pas d'élément idempotent autre que e , les deux notions d'élément irréductible et d'élément indécomposable se confondent encore dans D .

où $i_1, \dots, i_n$ sont des images inverses quelconques de $\bar{i}_1, \dots, \bar{i}_n$ ou encore des générateurs quelconques des idéaux principaux correspondants; ε désigne une unité convenable.

Un élément p de D qui n'est pas une unité est dit *premier* s'il est irréductible ⁽¹⁾, *premier au sens strict* si

$$p \mid ab \text{ et } p \nmid a \text{ entraînent } p \mid b,$$

ce qui équivaut à

$$ab \in (p) \text{ et } a \notin (p) \text{ entraînent } b \in (p),$$

de sorte qu'un élément est *premier au sens strict* si l'idéal qu'il engendre est *premier et seulement dans ce cas* ⁽²⁾.

Tout élément associé à un élément premier (ou premier au sens strict) est premier (ou premier au sens strict).

THÉOREME 5. — *Tout élément p premier au sens strict est premier.*

Soit, en effet, $p = xy$ une décomposition de p . Nous avons $p \mid xy$: p divise donc au moins l'un des facteurs x, y , par exemple $p \mid x$. Comme $x \mid p$, p et x sont associés, y est une unité et la décomposition $p = xy$ est banale.

THÉOREME 6. — *Si $\bar{D}(=D/\mathcal{R})$, ou, ce qui revient au même, si le demi-groupe Π des idéaux principaux vérifie la condition maximale, tout élément a de D qui n'est pas une unité est le produit d'un nombre fini d'éléments premiers (distincts ou non).*

Si $a \notin E$, on a

$$(7) \quad a = p_1 p_2 \dots p_n \quad (n \geq 1, p_i \text{ premiers}).$$

Ce théorème résulte immédiatement de la décomposition (4").

Il importe de remarquer qu'on a, pour l'unicité de la décomposition (7), un théorème qui est valable indépendamment de la condition maximale, mais qui nécessite l'existence d'une décomposition en produit d'éléments premiers au sens strict.

⁽¹⁾ Quand les éléments de D sont des polynomes, on dit encore *irréductible* au lieu de *premier*.

⁽²⁾ La terminologie que nous employons est celle de H. HASSE, *Höhere Algebra*, t. 2, p. 11 et de B. L. VAN DER WAERDEN, *Moderne Algebra*, t. 1, p. 63; W. KRULL (*Idealtheorie*, p. 11) appelle *premier* un élément p tel que l'idéal principal (p) soit premier, c'est-à-dire un élément premier au sens strict dans notre terminologie.

THÉOREME 7. — *Si un élément a du semi-groupe abélien D est un produit d'éléments premiers au sens strict*

$$(7) \quad a = p_1 p_2 \dots p_r$$

et si

$$(7') \quad a = q_1 q_2 \dots q_s$$

est une décomposition de a en produit d'éléments premiers, on a

$$r = s$$

et, en permutant éventuellement les indices, q_i et p_i sont associés ⁽¹⁾ (les q_i sont donc premiers au sens strict).

Si $r = 1$, on a aussi $s = 1$, car p_1 est irréductible et les q_i ne sont pas des unités.

Supposons $r > 1$ et le théorème vrai quand la décomposition (7) comprend moins de r facteurs; l'élément premier au sens strict p_1 , divisant le produit $q_1 \dots q_s$, divise au moins un facteur du second membre, q_1 par exemple : comme q_1 est premier, p_1 et q_1 sont associés : $q_1 = p_1 \varepsilon$, $\varepsilon \in E$. Simplifions par p_1 : comme $p_2 \notin E$, nous avons $s \geq 2$; en remplaçant q_2 par $q'_2 = q_2 \varepsilon$, nous avons deux décompositions de même forme que (7) et (7'), mais qui comprennent $r - 1$ et $s - 1$ facteurs. La proposition en résulte.

Ce qui précède s'applique, en particulier, au semi-groupe multiplicatif $D = \mathfrak{o}^*$ formé par les éléments *non nuls* d'un domaine d'intégrité $\mathfrak{o}$, ayant un élément-unité e . Si, par exemple, $\mathfrak{o}$ est l'anneau C des entiers, nous avons $e = 1$, il y a dans $\mathfrak{o}^*$ deux unités, 1 et -1 ; on a

$$x \equiv y \quad (\mathcal{R}) \quad \text{si} \quad |x| = |y|,$$

$\overline{D}$ n'est autre que l'ensemble N des nombres naturels; $a \subset b$, dans $\overline{D}$, signifie : b divise a , les éléments indécomposables de $\overline{D}$ sont les nombres premiers. La condition maximale est remplie (toute suite de nombres naturels dans laquelle chaque nombre est un véritable diviseur du précédent, est finie) et la représentation (3) est la représentation usuelle en produit de facteurs premiers. Nous reprendrons ces propriétés, sous une forme plus générale, au chapitre VI.

(1) On exprimera ces deux propriétés en disant que la décomposition (7) est *unique*.

Exercice 2. — 1° Dans un ensemble E partiellement ordonné (par $\subseteq$), on considère une opération O , associative et commutative ⁽¹⁾, telle que le préordre de décomposition correspondant $\mathcal{S}$ implique la relation d'ordre ($a\mathcal{S}b \Rightarrow a \subseteq b$). Montrer que D est un holoïde par rapport à O .

2° L'ensemble $\mathcal{J}$ des idéaux d'un anneau commutatif R ⁽¹⁾ est un holoïde par rapport à la multiplication. Montrer que tout idéal premier est indécomposable (en général, la réciproque n'est pas vraie, voir chap. VI, § 5, ex. 4, p. 342).

(1) On suppose que E (ou R) possède un élément-unité.

CHAPITRE V.

DEMI-GROUPES. CORPS.

A. — DEMI-GROUPES ABÉLIENS. PROBLÈMES D'IMMERSION COMMUTATIFS.

1. **Groupes homomorphes à un demi-groupe abélien.** — Le premier problème fondamental qui se présente dans l'étude des corps consiste à *construire un corps K , minimal, contenant un domaine d'intégrité donné D* : en prenant pour D l'anneau des entiers, on obtiendra comme corps K le *corps des nombres rationnels*. Ce problème d'immersion se rattache à un autre, plus simple : *plonger un semi-groupe abélien dans un groupe abélien*, qui est lié lui-même à la *recherche des groupes homomorphes à un demi-groupe abélien donné*, problème intéressant en lui-même et admettant de nombreuses applications.

Nous allons étudier ces problèmes, dans l'ordre inverse, pour aller du plus simple au plus complexe (section A). Nous nous occuperons ensuite de leurs généralisations dans le *cas non commutatif* (section B); on rencontre ici des difficultés notables dont la solution exige l'emploi de nouvelles méthodes qui, cependant, comme dans le cas abélien, reposent sur la considération de certaines équivalences régulières. Par cette étude des *équivalences remarquables d'un demi-groupe*, les sections A et B sont un prolongement du chapitre précédent.

La section C est consacrée à l'étude de certains corps, les *corps ordonnés*, dont le corps des nombres rationnels est l'exemple le plus élémentaire. L'analyse des propriétés de ces corps nous conduira à la méthode de *complétion* qui permet, notamment, de construire le *corps des nombres réels* à partir du corps des nombres rationnels.

Le lecteur qui désire avancer rapidement dans l'étude des corps peut passer directement de la première section à la troisième.

Considérons un *demi-groupe abélien* D et supposons qu'il existe un homomorphisme appliquant D sur un *groupe* $\overline{G}$, qui sera, lui aussi,

abélien :

$$(1) \quad D \sim \bar{G}.$$

Désignons par $\bar{x}$ l'image, dans $\bar{G}$, d'un élément x de D , dans cet homomorphisme, par $\mathbf{P}$ l'équivalence d'homomorphisme :

$$x \equiv y (\mathbf{P}) \Leftrightarrow \bar{x} = \bar{y}.$$

Étudions les classes $A, \dots$ modulo $\mathbf{P}$ et, en particulier, la *classe-unité* U , c'est-à-dire l'ensemble des éléments $u_1, u_2, \dots$ de D qui ont pour image l'élément-unité $\bar{u}$ du groupe $\bar{G}$.

1° *Toute classe H modulo $\mathbf{P}$ est un complexe net* ⁽¹⁾. — Soit a un élément quelconque de D ; désignons par $\bar{a}$ son image dans $\bar{G}$, par $\bar{h}$ celle des éléments de la classe H . Posons

$$\bar{x} = \bar{a}^{-1} \bar{h}$$

et soit x une image inverse quelconque de $\bar{x}$, dans D . Le produit ax a pour image

$$\overline{ax} = \bar{a} \bar{x} = \bar{h}, \quad \text{donc} \quad ax \in H.$$

On a d'ailleurs $H : a = X$, classe des éléments de D ayant pour image $\bar{x}$.

2° *La classe-unité U est un sous-demi-groupe unitaire* ⁽²⁾. — Si u_1 et u_2 appartiennent à U , donc $\bar{u}_1 = \bar{u}_2 = \bar{u}$, on a

$$\overline{u_1 u_2} = \bar{u}_1 \bar{u}_2 = \bar{u}^2 = \bar{u}, \quad \text{donc} \quad u_1 u_2 \in U.$$

Si l'on a

$$u_1 \in U \quad \text{et} \quad u_1 x \in U,$$

il s'ensuit

$$\overline{u_1 x} = \bar{u}_1 \bar{x} = \bar{u} \bar{x} = \bar{x} = \bar{u}, \quad \text{donc} \quad x \in U.$$

3° *Pour que l'on ait $a_1 \equiv a_2 (\mathbf{P})$, il faut et il suffit qu'il existe deux éléments u_1 et u_2 de U vérifiant l'égalité*

$$(2) \quad u_1 a_1 = u_2 a_2.$$

Supposons $a_1 \equiv a_2 (\mathbf{P})$; considérons l'inverse $\bar{b}$, dans le groupe $\bar{G}$, de

(1) C'est-à-dire tel que, pour tout $a \in D$, la relation $ax \in H$ ait au moins une solution x dans D (chap. II, § 6, p. 92). D étant *abélien*, l'ensemble des solutions x sera appelé *quotient* de H par a et désigné par $H : a$.

(2) Cf. Chap. IV, § 2, th. 2; nous rappelons dans le texte la démonstration.

l'élément $\bar{a}_1 = \bar{a}_2$, et une image inverse b , dans D , de $\bar{b}$. Nous avons

$$\overline{ba_i} = \bar{b} \bar{a_i} = \bar{u} \quad (i = 1, 2),$$

donc

$$ba_1 = u_2 \in U, \quad ba_2 = u_1 \in U,$$

d'où, puisque D est un demi-groupe abélien,

$$u_1 a_1 = u_2 a_2 (= ba_1 a_2).$$

Inversement, *quels que soient* $a \in D$ *et* $u \in U$, *on a*

$$au \equiv a \quad (\mathbf{P}),$$

puisque $\overline{au} = \bar{a} \bar{u} = \bar{a}$. L'égalité (2) entraîne donc la congruence $a_1 \equiv a_2 \quad (\mathbf{P})$, et nous pouvons, en résumé, énoncer le théorème suivant :

THÉOREME 1. — *S'il existe un groupe $\bar{G}$ homomorphe au demi-groupe abélien D , chaque classe modulo l'équivalence d'homomorphisme $\mathbf{P}$ est un complexe net; la classe unité U est un sous-demi-groupe net et unitaire; l'équivalence $\mathbf{P}$ est caractérisée, à partir de U , de la façon suivante : pour que l'on ait*

$$a_1 \equiv a_2 \quad (\mathbf{P}),$$

il faut et il suffit qu'il existe deux éléments u_1, u_2 de U vérifiant l'égalité

$$(2) \quad a_1 u_1 = a_2 u_2.$$

La réciproque est le théorème suivant :

THÉOREME 2. — *S'il existe un sous-demi-groupe net, S , de D , la relation Σ définie par*

$$a_1 \equiv a_2 \quad (\Sigma)$$

s'il existe

$$s_1, s_2 \in S \quad \text{tels que l'on ait} \quad s_1 a_1 = s_2 a_2$$

est une équivalence régulière et l'ensemble quotient D/Σ est un groupe $\bar{G}$. La classe-unité U contient S et pour qu'on ait l'égalité $U = S$, il est, non seulement nécessaire, mais suffisant, que S soit unitaire. L'équivalence $\mathbf{P}$ définie par U comme Σ l'est par S , coïncide avec Σ .

Σ est évidemment une relation réflexive et symétrique; c'est aussi une relation transitive, car si l'on a également $a_2 \equiv a_3 \quad (\Sigma)$, c'est-à-dire

$$s'_2 a_2 = s'_3 a_3, \quad \text{où} \quad s'_2, s'_3 \in S,$$

il en résulte

$$s'_2 s_1 . a_1 = s'_2 s_2 a_2 = s_2 s'_3 . a_3, \quad \text{d'où} \quad a_1 \equiv a_3 \ (\Sigma),$$

puisque $s'_2 s_1$ et $s_2 s'_3$ appartiennent à S.

Cette *équivalence* Σ est *régulière*, puisque $a_1 \equiv a_2 (\Sigma)$ c'est-à-dire $s_1 a_1 = s_2 a_2$ entraîne, quel que soit $x \in D$,

$$s_1 . a_1 x = s_2 . a_2 x, \quad \text{d'où} \quad a_1 x \equiv a_2 x \ (\Sigma).$$

Soient s, s' deux éléments de S : nous avons

$$ss' = s's, \quad \text{donc} \quad s \equiv s' \ (\Sigma);$$

S est contenu dans une classe U, modulo Σ .

Considérons un élément a quelconque de D et la classe A, modulo Σ , à laquelle il appartient : nous avons, quels que soient $s, s_1 \in S$,

$$s_1 . sa' = s_1 s . a, \quad \text{donc} \quad sa \equiv a \ (\Sigma),$$

ce qui entraîne, pour les classes correspondantes, $UA = A$: U est *élément-unité* dans le demi-groupe quotient D/Σ .

Puisque S est net, il existe un élément x de D vérifiant $ax \in S$, ce qui entraîne, pour les classes, $AX = U$. Tout élément A de D/Σ a donc un inverse : D/Σ est un groupe $\overline{G}$ homomorphe à D. D'après le théorème 1, U est sous-demi-groupe-unitaire de D ; il faut donc, pour qu'on ait l'égalité $S = U$, que S soit unitaire.

C'est aussi *suffisant*. Remarquons, en effet, que, si $u \in U$, on a

$$u \equiv s \ (\Sigma), \quad \text{où} \quad s \in S, \quad \text{donc} \quad s_1 u = s_2 s \in S,$$

c'est-à-dire

$$(3) \quad s_1 u = s'_1, \quad \text{où} \quad s_1, s'_1 \in S.$$

Inversement, un élément u vérifiant (3) appartient à U puisqu'on a

$$s'_1 = s_1 u \equiv u (\Sigma)$$

U est donc l'ensemble des éléments u vérifiant (3). Or, si S est unitaire, (3) entraîne $u \in S$, d'où $U = S$.

D'après le théorème 1, $\mathbf{P}$ est l'équivalence d'homomorphisme ; elle coïncide donc avec Σ . Σ et $\mathbf{P}$ sont appelées *équivalences réversibles* associées respectivement à S et à U.

D'après les théorèmes 1 et 2, il existe une correspondance biunivoque entre les groupes $\overline{G}$ homomorphes à un demi-groupe abélien D

et les sous-demi-groupes nets et unitaires U de D ; U est la classe-unité dans l'homomorphisme $D \sim \bar{G}$. De plus, tout sous-demi-groupe net S de D fournit un groupe $\bar{G}$ homomorphe à D ; P et Σ désignant les équivalences précédemment définies, on a l'isomorphisme

$$\bar{G} \simeq D/P = D/\Sigma$$

(théorème d'homomorphisme).

Exemples ⁽¹⁾. — 1. Prenons pour D le demi-groupe additif des entiers naturels, pour S le sous-demi-groupe des multiples km d'un nombre fixe m , pour lesquels k est au moins égal à un entier fixe k_0 . S est net : si $a \in D$, il existe bien $x \in D$ tel que

$$a + x = km, \quad \text{avec } k \geq k_0.$$

L'équivalence Σ définie par

$$a_1 \equiv a_2 \quad (\Sigma) \quad \text{si} \quad a_1 + k_1 m = a_2 + k_2 m \quad (k_1, k_2 \geq k_0)$$

n'est autre que la congruence arithmétique modulo m ; U est l'ensemble de tous les multiples de m : c'est bien un sous-demi-groupe net et unitaire. Le groupe $\bar{G}$, homomorphe à D , est le groupe additif $C/(m)$ des classes résiduelles modulo m .

2. Si D est un groupe (abélien), tout sous-groupe S est net et unitaire ⁽²⁾; l'équivalence Σ correspondante est bien l'unique équivalence régulière ayant S comme classe-unité.

2. Immersion d'un semi-groupe abélien dans un groupe. — Si un demi-groupe D est contenu dans un groupe G , la règle de simplification est nécessairement valable dans D . Il faut donc qu'un demi-groupe (abélien ou non) soit un semi-groupe pour qu'il puisse être plongé dans un groupe.

Montrons que, dans le cas abélien, cette condition nécessaire est aussi suffisante. S étant un semi-groupe abélien, nous nous proposons de construire un groupe abélien Γ contenant S et, d'autre part, minimal, c'est-à-dire tel qu'il n'y ait aucun groupe Γ' contenant S et inclus strictement dans Γ .

⁽¹⁾ D'importantes relations d'équivalence entrent dans la catégorie que nous venons d'étudier : *équivalence d'Artin* ou *quasi-égalité* en Théorie des Idéaux (voir, par exemple, B. L. VAN DER WAERDEN, *Moderne Algebra*, t. 2, § 105, 2^e éd.), équivalences fondamentales de la *Géométrie algébrique* [F. SEVERI, *Il punto di vista gruppale nei vari tipi di equivalenza sulle varietà algebriche* (*Comm. Math., Helvet.*, t. 21, 1948, p. 189-224)].

⁽²⁾ Inversement, comme nous l'avons vu, tout complexe unitaire, dans un groupe, est un sous-groupe (chap. III, § 3, p. 109).

Si un tel groupe Γ existe, il contient nécessairement les éléments r , s , t , ... de S , leurs inverses r^{-1} , s^{-1} , t^{-1} , ... et les produits de la forme rs^{-1} : soit Γ_0 l'ensemble de ces produits. Deux éléments $\alpha = rs^{-1}$ et $\beta = tu^{-1}$ de Γ_0 se composent dans Γ suivant la loi

$$(1) \quad \alpha\beta = rs^{-1}tu^{-1} = (rt)(su)^{-1},$$

ce qui entraîne $\alpha\beta \in \Gamma_0$; comme on a aussi

$$\alpha\beta^{-1} = rs^{-1}ut^{-1} = (ru)(st)^{-1} \in \Gamma_0,$$

Γ_0 est un sous-groupe de Γ , contenant S puisque $s = s^2 \cdot s^{-1}$: par conséquent, Γ coïncide avec Γ_0 , puisque Γ doit être minimal.

Le groupe $\Gamma = \Gamma_0$ est homomorphe, d'après (1), à l'ensemble-produit $S \times S$ dans lequel la multiplication des couples (r, s) , (t, u) est définie par

$$(1') \quad (r, s)(t, u) = (rt, su),$$

ce qui fait de $S \times S$ un *demi-groupe abélien* Δ : l'homomorphisme est défini par

$$(r, s) \rightarrow rs^{-1} = \alpha.$$

Les couples ayant pour image l'élément-unité ε de Γ sont les couples (r, r) et ceux-là seulement.

Nous voyons donc, en tenant compte des résultats du paragraphe 1, que Γ ne peut exister que si l'ensemble U des couples (x, x) est, dans Δ , un *sous-demi-groupe net et unitaire*. Or, U est évidemment un sous-demi-groupe net puisque

$$(r, s)(s, r) = (rs, rs) \in U$$

et unitaire puisque l'égalité

$$(r, s)(x, x) = (y, y)$$

entraîne

$$rx = sx \quad (= y), \quad \text{d'où} \quad r = s.$$

Alors, il existe bien un groupe Γ et, à un isomorphisme près, un seul, homomorphe à Δ et tel que, dans cet homomorphisme, la classe-unité soit U : c'est le groupe $\Delta/\mathbf{P}$, où $\mathbf{P}$ est l'équivalence réversible associée à U .

On a ici

$$(r, s) \equiv (r_1, s_1) \quad (\mathbf{P})$$

s'il existe dans D deux éléments x , x_1 tels que

$$(x, x)(r, s) = (x_1, x_1)(r_1, s_1)$$

c'est-à-dire $xr = x_1 r_1$, $xs = x_1 s_1$, d'où $xr x_1 s_1 = x_1 r_1 xs$ et enfin

$$(2) \quad rs_1 = r_1 s.$$

Réciproquement, si l'on a cette égalité ⁽¹⁾, on peut prendre $x = r_1$, $x_1 = r$.

Soit α_s la classe contenant le couple (sx, x) : les classes α_s de ce type correspondent biunivoquement aux éléments s de S , puisqu'on a

$$(sx, x) \equiv (ty, y) \quad (\mathbf{P})$$

si et seulement si $s = t$. Cette correspondance biunivoque

$$s \leftarrow \rightarrow \alpha_s$$

est, en outre, un isomorphisme : l'ensemble $\bar{S} \subset \Gamma$ des classes α_s étant isomorphe à S , $\Gamma = \Delta/\mathbf{P}$ est bien une *extension* de S (cf. chap. III, § 8, p. 132) :

Il est souvent commode de donner aux couples $(r, s) \in \Delta$ le nom de *fractions*, d'utiliser la notation classique $\frac{r}{s}$ ou r/s , et de dire que r est le *numérateur*, s le *dénominateur* de la fraction. Les règles de calcul prennent l'aspect classique

$$(1'') \quad \frac{r}{s} \frac{t}{u} = \frac{rt}{su},$$

$$(2'') \quad \frac{r}{s} \equiv \frac{r_1}{s_1} (\mathbf{P}) \quad \Leftrightarrow \quad rs_1 = r_1 s$$

(il sera plus correct de dire *fractions équivalentes* que *fractions égales*). Les éléments de Γ sont les *classes de fractions équivalentes* : $\Gamma = \Delta/\mathbf{P}$; il est facile de vérifier directement que $\mathbf{P}$ est régulière par rapport à la multiplication et que Γ est un groupe; les éléments de S sont représentés par les fractions $\frac{sx}{x}$, en particulier par les fractions $\frac{s}{e}$, si S admet un élément-unité e .

Application. — Considérons le *semi-groupe additif*

$$N_0 = \{0, 1, 2, \dots, n, \dots\}.$$

Nous pouvons, d'après ce qui précède, le plonger dans un groupe additif G : celui-ci est l'ensemble des *entiers relatifs* dont ceci est une

⁽¹⁾ A priori, cette forme de l'équivalence d'homomorphisme $\mathbf{P}$ est la seule possible puisque, si l'on suppose l'existence de Γ , la relation $(r, s) \equiv (r_1, s_1) (\mathbf{P})$ signifie $rs^{-1} = r_1 s_1^{-1}$ dans Γ , c'est à dire $rs_1 = r_1 s$ dans D .

autre définition. Dans le demi-groupe $\Delta = N_0 \times N_0$, l'addition des couples (a, b) est définie par

$$(3) \quad (a, b) + (c, d) = (a + c, b + d)$$

et deux couples (a, b) , (a_1, b_1) sont équivalents modulo **P** si l'on a

$$(4) \quad a + b_1 = a_1 + b.$$

Il en résulte, puisque nous avons dans N_0 un élément neutre, o , par rapport à l'addition, que la classe μ contenant un couple (a, b) donné peut être représentée par un couple de la forme

$$\begin{array}{lll} (m, o), & \text{où} & m \in N = \{1, 2, \dots, n, \dots\} \quad \text{si } a > b, \\ (o, o) & & \text{si } a = b, \\ (o, m), & \text{où} & m \in N \quad \text{si } a < b, \end{array}$$

Dans ces cas respectifs, μ est dit *positif*, *nul* ou *négatif* et désigné par les notations abrégées $+m$, o , $-m$, avec lesquelles les règles de l'addition se mettent immédiatement sous la forme usuelle. Le nombre positif $\alpha = +a$, ensemble des couples $(a + x, x)$, où $x \in N_0$, est identifié avec le nombre naturel a .

La définition du *produit de deux entiers relatifs* résulte en premier lieu du *principe de concordance* (chap. III, § 8, p. 132) d'après lequel nous posons

$$(+a)(+b) = +ab$$

et, en second lieu, des règles de calcul que l'on impose à la multiplication. La *distributivité* de la multiplication par rapport à l'addition entraîne d'abord que *tout produit par zéro est nul*

$$\alpha\mu = \alpha(\mu + o) = \alpha\mu + \alpha o, \quad \text{d'où} \quad \alpha o = o,$$

puis, la relation

$$o = \alpha o = \alpha[\mu + (-\mu)] = \alpha\mu + \alpha(-\mu)$$

donne

$$\alpha(-\mu) = -(\alpha\mu).$$

Enfin, nous avons, en imposant en outre à la multiplication d'être *commutative* :

$$(-\mu)\alpha = \alpha(-\mu) = -(\alpha\mu).$$

Ces relations permettent de ramener le calcul du produit de deux entiers de signes quelconques à celui de deux entiers positifs, déjà défini : on est ainsi conduit aux règles habituelles sur lesquelles nous n'insisterons pas davantage.

Les nombres ainsi définis ne sont pas à proprement parler identiques à ceux que nous avons introduits précédemment par un autre procédé, mais les uns et les autres forment des *domaines isomorphes et semblables* : ils peuvent être utilisés indifféremment.

3. Immersion d'un domaine d'intégrité dans un corps. — Soit D un domaine d'intégrité : $D - \{0\}$ est un semi-groupe abélien *multiplicatif* S ; construisons comme au paragraphe 2 le plus petit groupe multiplicatif abélien contenant S , ensemble Γ des classes de fractions $\frac{r}{s}$ équivalentes ($r, s \in S$).

Adjoignons à Γ un élément 0 , multiplicativement permis :

$$(1) \quad 0\alpha = 0 \quad \text{pour tout } \alpha \in \Gamma.$$

Comme deux fractions quelconques de la forme $\frac{0}{s}, \frac{0}{s_1}$ (0 désigne le zéro de D , s et $s_1 \in S$) vérifient la relation qui caractérise les fractions équivalentes, l'élément 0 adjoint à Γ peut être regardé comme la classe qui contient ces fractions (et n'en comprend d'ailleurs pas d'autre).

Désignons par $K = \Gamma + \{0\}$ le demi-groupe multiplicatif ainsi obtenu et, pour faire de K un *corps*, définissons une *addition* distribuée par la multiplication et telle que K soit un groupe additif.

Si $\alpha = ab^{-1}$, $\beta = cd^{-1}$ ($a, c \in D$, $b, d \in S$) sont deux éléments de K , nous devons avoir, pour tout $\xi \in K$,

$$(\alpha + \beta)\xi = \alpha\xi + \beta\xi,$$

d'où, en particulier, pour $\xi = bd$,

$$(\alpha + \beta)bd = (ab^{-1} + cd^{-1})bd = ad + bc$$

et

$$\alpha + \beta = (ad + bc)(bd)^{-1}.$$

Par conséquent, la somme $\alpha + \beta$ doit être la classe contenant la fraction $\frac{ad + bc}{bd}$.

Cette remarque préliminaire nous conduit à appeler *somme* des fractions $\frac{a}{b}, \frac{c}{d}$ la fraction $\frac{ad + bc}{bd}$ et à définir la somme $\alpha + \beta$ des éléments de K représentés par ces fractions comme la classe contenant la fraction somme $\frac{ad + bc}{bd}$. Cette définition nécessite deux justifications, d'ailleurs immédiates.

1° Si l'on remplace une des fractions, $\frac{a}{b}$ par exemple, par une fraction équivalente $\frac{a_1}{b_1}$, la fraction-somme est remplacée elle aussi par une fraction équivalente; $ab_1 = a_1b$ entraîne bien en effet,

$$(ad + bc)b_1d = (a_1d + b_1c)bd;$$

2° Les éléments de D , représentés par les fractions $\frac{ax}{x}$, s'ajoutent comme dans D : on a en effet,

$$\frac{ax}{x} + \frac{by}{y} = \frac{(a+b)xy}{xy}.$$

L'addition ainsi définie possède les propriétés suivantes :

I. On a

$$\frac{a}{b} + \frac{a'}{b} \equiv \frac{a+a'}{b} \quad (\mathbf{P})$$

et

$$\frac{x}{pq} + \frac{x'}{p'q} \equiv \frac{xp' + x'p}{pp'q} \quad (\mathbf{P}).$$

II. L'addition est commutative.

III. L'addition est associative. — Soient α , α' , α'' trois éléments de K , représentés respectivement par les fractions $\frac{x}{y}$, $\frac{x'}{y'}$, $\frac{x''}{y''}$. La fraction $\frac{xy'y'' + x'y''y + x''yy'}{yy'y''}$ représente aussi bien $(\alpha + \alpha') + \alpha''$ que $\alpha + (\alpha' + \alpha'')$: ces deux éléments sont donc égaux.

IV. L'élément 0 de K est neutre pour l'addition :

$$0 + \alpha = \alpha \quad \text{pour tout } \alpha \in K.$$

Si $-\alpha$ désigne la classe représentée par $-\frac{a}{b}$, où $\frac{a}{b} \in \alpha$, on a $\alpha + (-\alpha) = 0$: K est bien un groupe additif.

V. La multiplication est distributive par rapport à l'addition. — Si β est représenté par $\frac{u}{v}$, $\beta(\alpha + \alpha')$ est représenté par $\frac{u(xy' + x'y)}{vy'}$; la somme $\beta\alpha + \beta\alpha'$ est représentée par la même fraction, puisque

$$\frac{uxy'}{vy'v} \equiv \frac{ux}{vy} \quad (\mathbf{P})$$

est un représentant de $\beta\alpha$, et

$$\frac{ux'y}{vy'y} \equiv \frac{ux'}{vy'} \quad (\mathbf{P})$$

un représentant de $\beta\alpha'$. Nous avons donc

$$\beta(\alpha + \alpha') = \beta\alpha + \beta\alpha'.$$

D'après ces propriétés, $\mathbf{K}$ est bien *un corps* : c'est par construction, *le plus petit corps* contenant $\mathbf{D}$; il est défini à un isomorphisme près. On l'appelle le *corps des quotients* ⁽¹⁾ du domaine d'intégrité $\mathbf{D}$.

Si l'on prend comme domaine d'intégrité l'anneau $\mathbf{C}$ des entiers, on obtient un corps des quotients Γ dont les éléments sont appelés *nombre rationnels*. Les fractions ont ici pour numérateur un entier quelconque (positif, négatif ou nul) et pour dénominateur un entier *non nul* (qu'on peut convenir de prendre positif). Un nombre rationnel est une classe de fractions équivalentes.

Dans une classe de fractions équivalentes non nulles, il en existe une et une seule dont le dénominateur est positif et *premier avec le numérateur* : cette fraction est dite *irréductible*.

Comme l'anneau $\mathbf{C}$ des entiers relatifs qu'il contient, le corps Γ des nombres rationnels est de *caractéristique nulle* : c'est le premier corps ayant cette propriété, que nous construisons.

B. — DEMI-GROUPES, PROBLÈMES D'IMMERSION : CAS NON COMMUTATIF.

4. Équivalences principales. Complexes forts. — Nous nous proposons de faire l'étude d'un demi-groupe $\mathbf{D}$ *sans le supposer abélien* et, en particulier, de rechercher les groupes homomorphes à $\mathbf{D}$. Il est clair que, dans une telle étude, on verra intervenir, comme parties remarquables de $\mathbf{D}$, les *sous-ensembles fermés* ou *sous-demi-groupes* (appelés aussi *sous-groupoïdes*) et les *sous-ensembles permis* ou *idéaux* (à droite, à gauche ou bilatères). L'importance de cette dernière notion vient notamment des analogies qui existent entre la théorie des demi-groupes et celle des anneaux : un anneau est un demi-groupe multiplicatif ; en faisant abstraction de la condition additive (condition 1, p. 185), on

⁽¹⁾ E. STEINITZ, *Algebraische Theorie der Körper* (*J. für r. Ang. Math.*, t. 137, 1910, p. 178).

passé de la notion d'idéal dans un anneau à celle d'idéal d'un demi-groupe. ⁽¹⁾.

De même, un élément permis z , s'il existe (et alors, il est nécessairement unique, cf. chap. II, § 4, p. 76), est souvent appelé *élément zéro*, ou simplement *zéro* : le complexe $Z = \{z\}$ est un *idéal bilatère*. Un élément x de D ($\neq Z$) est *diviseur de zéro à gauche* s'il existe dans D un élément y distinct de z tel que l'on ait $xy = z$. On définit symétriquement un diviseur de zéro à droite. Un diviseur de zéro est dit *véritable* s'il est distinct de z .

Dans un demi-groupe D ayant un élément zéro z , appelons *noyau à droite* et désignons par N_d l'ensemble des non-diviseurs de zéro à gauche, donc des éléments a tels que

$$x \neq z \quad \text{entraîne} \quad ax \neq z.$$

On définit symétriquement le *noyau à gauche* N_g ; le *noyau* de D est l'intersection $N_d \cap N_g$, c'est-à-dire l'ensemble des éléments qui ne sont diviseurs de zéro ni à droite ni à gauche.

Les noyaux N , N_d , N_g sont contenus dans $D - Z$; s'ils ne sont pas vides, ce sont des sous-demi-groupes de D . Soit en effet, par exemple, $a \in N_d$, $b \in N_d$; la relation $ab \cdot x = z$ s'écrit $a \cdot bx = z$, donc entraîne $bx = z$, puis $x = z$: nous avons bien $ab \in N_d$.

S'il n'existe pas de véritables diviseurs de zéro à droite, les relations

$$(1) \quad x \neq z, \quad y \neq z \quad xy = z.$$

ne peuvent pas être vérifiées simultanément, et il n'existe pas non plus de véritables diviseurs de zéro à gauche. On a

$$N_d = N_g = N = D - Z.$$

⁽¹⁾ Ce point de vue est l'origine de nombreux et importants travaux que nous devons ici nous borner à mentionner :

D. REES, *On Semi-groups* (Proc. Cambridge Phil. Soc., t. 36, 1940, p. 386); *On the Ideal Structure of a Semi-group satisfying a Cancellation law* (Quart. J. Math., t. 19, 1948, p. 101).

A. SUSCHKEWITSCH, *Ueber die endlichen Gruppen ohne das Gesetz der eindeutigen Umkehrbarkeit* (Math. Ann., t. 99, 1928, p. 30).

ST. SCHWARZ, *Zur Theorie der Halbgruppen* (Sbornik, Bratislava, 1943).

P. LORENZEN, *Abstrakte Begründung der multiplikativen Idealtheorie* (Math. Zeit., t. 45, 1939, p. 533); voir aussi, du même auteur, *Ueber halbgeordnete Gruppen* (ibid., t. 52, 1949, p. 483).

A. H. CLIFFORD, *Semi-groups containing minimal Ideals* (Amer. J. of Math., t. 70, 1948, p. 521); *Semi-groups without nilpotents Ideals* (ibid., t. 71, 1949, p. 834).

A. H. CLIFFORD et D. D. MILLER, *Semi-groups having zeroïd elements* (Amer. J. Math., t. 70, 1948, p. 117).

M. TEISSIER, *Sur la théorie des idéaux dans les demi-groupes* (C. R. Acad. Sc., t. 234, 1952, p. 386). M^{lle} M. Teissier a également étudié les *algèbres d'un demi-groupe fini simple* dans deux Notes (C. R. Acad. Sc., t. 234, 1952, p. 2413 et 2511).

Mais les relations (1) expriment aussi que l'idéal Z est *premier* ou que $D - Z$ est un ensemble multiplicativement fermé. Nous caractériserons ce cas en disant que *le demi-groupe D admet un zéro premier*. Si, en outre, $D - Z = N$ est un groupe, on dit que D est un *pseudo-groupe*; si N est un semi-groupe, D est un *pseudo-semi-groupe*.

Remarque. — Si le zéro d'un anneau A est premier, la règle de simplification est valable dans $A - \{0\} = N$; s'il est commutatif, A est un domaine d'intégrité. L'égalité $ax = bx$ s'écrit, en effet, $(a - b)x = 0$ et, avec $x \neq 0$, entraîne $a = b$. Cette propriété n'est évidemment plus valable pour un demi-groupe quelconque : adjoignons, en effet, un élément permis z à un demi-groupe Δ qui n'est pas un semi-groupe : $zx = xz = z$ pour tout $x \in \Delta$, $z^2 = z$. Dans le demi-groupe $D = \Delta + \{z\}$, ainsi obtenu, le zéro z est premier et l'on a $N = \Delta$: la règle de simplification, cependant, n'est pas valable dans N . Nous rencontrerons plus loin (§ 5, corollaire du lemme 1, p. 250) un type de demi-groupe $\mathcal{F}$ ayant un zéro W et dans lequel tout sous-demi-groupe ne contenant pas W , en particulier le noyau, est un semi-groupe.

Dans un demi-groupe D quelconque, il est commode de regarder la partie vide comme un idéal, donc aussi comme un sous-demi-groupe. L'ensemble $\mathcal{I}_d$ des idéaux à droite (par exemple) vérifie les conditions de Moore : $a. D \in \mathcal{I}_d$; $b.$ toute intersection d'idéaux à droite est un idéal à droite. $\mathcal{I}_d$ est donc un treillis complet. L'union dans $\mathcal{I}_d$ coïncide d'ailleurs avec la réunion au sens de la Théorie des Ensembles, puisque toute réunion de parties permises à droite est une partie permise à droite : $\mathcal{I}_d$ est donc un sous-treillis de $\mathcal{E}(D)$.

L'ensemble $\mathcal{S}$ des sous-demi-groupes ($\emptyset$ compris) vérifie aussi les conditions de Moore : c'est un treillis complet, mais dont l'union, en général, ne coïncide plus avec la réunion au sens de la Théorie des Ensembles.

Dans la recherche des groupes homomorphes à un demi-groupe donné D , problème que nous nous proposons de traiter ici, les deux notions de sous-demi-groupe et d'idéal, à elles seules, ne permettent pas d'aboutir; de plus, la méthode du cas abélien tombe en défaut dans le cas non commutatif. C'est en reprenant à la base les notions fondamentales relatives aux *propriétés d'inversion* dans un demi-groupe (chap. II, § 6, p. 89) que nous obtiendrons le type de relations d'équivalence qui contractent un demi-groupe en un groupe (1).

(1) La théorie générale des relations d'équivalence dans les demi-groupes a été développée dans les travaux suivants :

P. DUBREIL, *Contributions à la théorie des Demi-groupes* (Mémoires de l'Aca-

Considérons, dans le demi-groupe D , un complexe H , un élément a , et le quotient à droite $Q_a = (H : a)_d$, ensemble des éléments x de D vérifiant

$$(2) \quad ax \in H.$$

Le résidu à droite W_H , ensemble des éléments w de D pour lesquels le quotient Q_w est vide, est un idéal à droite dans D , comme nous l'avons déjà vu (*loc. cit.*). Le produit ax appartenant toujours au complexe-produit D^2 , H et $D^2 \cap H$ ont même résidu : si $D^2 \cap H = T$ est vide (H est alors dit *trivial*), W_H est le demi-groupe D tout entier.

Tout élément de D permis à droite et qui n'est pas contenu dans H , appartient à W_H .

THEOREME 1. — Soient H et K deux complexes de D :

- a. $H \subseteq K$ entraîne $W_K \subseteq W_H$;
- b. $H \cap W_K = \emptyset$ entraîne $W_K \subseteq W_H$.

a. La relation d'inclusion $H \subseteq K$ entraîne évidemment

$$(H : a)_d \subseteq (K : a)_d, \quad \text{donc } W_K \subseteq W_H.$$

b. Soit $H \cap W_K = \emptyset$. Si $a \in D - W_H$, il existe un élément x de D vérifiant $ax \in H$, donc $ax \notin W_K$. Il existe alors un élément y tel que $axy \in K$, d'où $a \in D - W_K$: nous avons $D - W_H \subseteq D - W_K$ et, par conséquent, $W_K \subseteq W_H$.

La relation $\mathcal{R}_H$ définie à partir du complexe H en posant

$$(3) \quad a \mathcal{R}_H b \quad \text{si et seulement si} \quad Q_a = Q_b$$

est réflexive, symétrique, transitive : c'est donc une relation d'équivalence appelée *équivalence principale à droite* associée à H . On

démie des Sciences de l'Institut de France, t. 63, 1941, p. 1-52; *Rendiconti di Matematica e delle sue applic.*, s. V, vol. X, 1951, p. 183-200; *Bull. Soc. Math.*, t. 81, 1953, p. 989-306).

M. TEISSIER, *Sur les équivalences régulières dans les demi-groupes* (*C. R. Acad. Sc.*, t. 232, 1951, p. 1987).

M. L. DUBREIL-JACOTIN, *Quelques propriétés des équivalences régulières par rapport à la multiplication et à l'union dans un treillis à multiplication commutative avec élément-unité* (*C. R. Acad. Sc.*, t. 232, 1951, p. 287).

M. L. DUBREIL-JACOTIN et R. CROISOT, *Sur les congruences dans les ensembles où sont définies plusieurs opérations* (*C. R. Acad. Sc.*, t. 233, 1951, p. 1162).

R. CROISOT, *Propriétés des complexes forts et symétriques des demi-groupes* (*Bull. Soc. Math.*, t. 80, 1952, p. 217-223).

écrira (3) sous la forme

$$(3') \quad a \equiv b \pmod{\mathcal{R}_H}.$$

Si le résidu à droite W_H n'est pas vide (en d'autres termes si H n'est pas net à droite), W_H est une classe modulo $\mathcal{R}_H$: c'est la classe qui contient les éléments permis à droite éventuels (en particulier le zéro s'il existe) qui n'appartiennent pas à H .

THEOREME 2. — *L'équivalence principale à droite $\mathcal{R}_H$ est régulière à droite.*

Soit r un élément quelconque de D . Si $x \in Q_{ar}$, nous avons

$$ar.x = a.r x \in H, \quad \text{donc} \quad r x \in Q_a$$

et (3) entraîne $b.r x = br.x \in H$, c'est-à-dire $x \in Q_{br}$, d'où $Q_{ar} \subseteq Q_{br}$; on a de même $Q_{br} \subseteq Q_{ar}$, d'où l'égalité, c'est-à-dire $ar \equiv br \pmod{\mathcal{R}_H}$.

On définit symétriquement, par l'égalité des quotients à gauche ${}_aQ, {}_bQ$ (où ${}_aQ$ par exemple désigne l'ensemble des $y \in D$ vérifiant $ya \in H$), l'équivalence principale à gauche ${}_H\mathcal{R} (a \equiv b \pmod{{}_H\mathcal{R}} \Leftrightarrow {}_aQ = {}_bQ)$ et l'on montre que cette équivalence est régulière à gauche. Le complexe H est dit *équirésiduel* si ses résidus à droite et à gauche coïncident, $W_H = {}_H W$, symétrique s'il est équirésiduel et si l'on a, en outre, $\mathcal{R}_H = {}_H \mathcal{R}$. Si les résidus W_H et ${}_H W$ ne sont pas vides, l'égalité $\mathcal{R}_H = {}_H \mathcal{R}$ entraîne $W_H = {}_H W$: chacun des résidus est en effet une classe mod $\mathcal{R}_H (= {}_H \mathcal{R})$ et si $\omega \in W_H$, $\omega' \in {}_H W$, l'élément $\omega\omega'$ appartient à la fois à W_H et à ${}_H W$. Ces deux classes, ayant un élément commun, coïncident.

Dans la relation (2), a et x jouent des rôles symétriques : si $x \in Q_a$, $a \in {}_x Q$ et inversement. La réunion des quotients Q_a quand a décrit D , ou, aussi bien, quand a décrit $D - W_H$, est le complément du résidu à gauche ${}_H W$:

$$\bigcup_{a \in D} Q_a = \bigcup_{a \in D - W_H} Q_a = D - {}_H W.$$

En associant à chaque élément a de $D - W_H$ son quotient à droite $Q_a = f_H(a)$, nous définissons une application f_H , en général multiforme, de $D - W_H = D_H^*$ dans $D - {}_H W = {}_H D^*$; de même, en associant à chaque élément x de ${}_H D^*$ son quotient à gauche ${}_x Q$, nous définissons une application ${}_H f$ de ${}_H D^*$ dans D_H^* ; les relations

$$x \in f_H(a), \quad a \in {}_H f(x),$$

équivalentes l'une et l'autre à la relation (2), ont lieu en même temps : les applications f_H et ${}_Hf$ sont donc inverses l'une de l'autre

$$f_H^{-1} = {}_Hf.$$

A l'application f_H est associée la relation réflexive et symétrique $\mathfrak{E}_H$ définie dans D_H^* par

$$(4) \quad a \mathfrak{E}_H b \quad \text{si et seulement si} \quad f_H(a) \cap f_H(b) \neq \emptyset,$$

c'est-à-dire si $Q_a \nparallel Q_b$ (chap. I, § 8, p. 31). En désignant par $\mathcal{R}_H^*$ la trace de $\mathcal{R}_H$ sur D_H^* et par $\mathcal{C}_H$ la fermeture transitive de $\mathfrak{E}_H$, c'est-à-dire l'équivalence décomposant D_H^* en parties stables minimales (chap. I, § 12, p. 59), nous avons

$$(5) \quad \mathcal{R}_H^* \subseteq \mathfrak{E}_H \subseteq \mathcal{C}_H.$$

Les applications inverses f_H et ${}_Hf$ sont *semi-uniformes* en même temps : nous dirons alors que H est un *complexe fort*; dire, par exemple, que f_H est semi-uniforme signifie que

$$(\alpha) \quad Q_a \nparallel Q_b \quad \text{entraîne} \quad Q_a = Q_b,$$

c'est-à-dire que l'on a $\mathfrak{E}_H \subseteq \mathcal{R}_H^*$, d'où l'égalité $\mathfrak{E}_H = \mathcal{R}_H^*$. On a alors aussi $\mathfrak{E}_H = \mathcal{C}_H$ (*ibid.*, th. 2, p. 35); ici, d'ailleurs, cette égalité résulte de la précédente et du fait que $\mathcal{C}_H$ est la plus petite équivalence contenant $\mathfrak{E}_H$; les classes modulo

$$\mathcal{R}_H^* = \mathfrak{E}_H = \mathcal{C}_H$$

sont les images inverses $f_H^{-1}(x) = {}_xQ$, pour $x \in {}_H D^*$, c'est-à-dire les quotients à gauche non vides : la classe A contenant a et le quotient ${}_xQ$ coïncident si l'on a $ax \in H$ et seulement dans ce cas.

Nous avons également les propriétés symétriques; en outre, la correspondance biunivoque $E/\mathcal{C} \leftarrow \rightarrow E'/\mathcal{C}'$ de la théorie générale des applications multiformes donne ici

$$D_H^*/\mathcal{R}_H^* \leftarrow \rightarrow {}_H D^*/{}_H \mathcal{R}^*,$$

ce qui, si les résidus W_H et ${}_H W$ sont tous deux vides ou tous deux non vides, permet d'écrire

$$(6) \quad D/\mathcal{R}_H \leftarrow \rightarrow D/{}_H \mathcal{R}.$$

En résumé, nous avons établi le théorème suivant :

THÉOREME 3. — *Pour qu'un complexe H soit fort, il suffit que les quotients à droite, par exemple, vérifient la condition (α) ; les classes*

modulo $\mathcal{R}_H$, distinctes du résidu à droite W_H , sont alors les quotients à gauche non vides ($A = {}_x Q \setminus \{ax \in H\}$); les ensembles-quotients $D/\mathcal{R}_H$ et $D|_H \mathcal{R}$ ont même puissance si W_H et ${}_H W$ sont tous deux vides ou tous deux non vides.

Cas particulier. — Dans un groupe G , toute équivalence régulière à droite, $\mathcal{R}$, est l'équivalence principale à droite définie par l'une quelconque de ses classes H . La classe-unité $\text{mod } \mathcal{R}$ est en effet un sous-groupe S de G , et une classe H est de la forme $H = Sh, h \in H$. Le quotient Q_a correspondant, ensemble des éléments x vérifiant $ax \in Sh$ est le complexe $Q_a = a^{-1}Sh$, et la congruence $a \equiv b(\mathcal{R}_H)$ équivaut à $a^{-1}Sh = b^{-1}Sh$, c'est-à-dire

$$Sa = Sb \quad \text{ou} \quad a \equiv b \quad (\mathcal{R}).$$

Si les quotients $Q_a = a^{-1}Sh$, $Q_b = b^{-1}Sh$ se coupent, on a $ba^{-1} \in S$ d'où $Q_a = Q_b$; la classe considérée H est donc un *complexe fort*.

Considérons maintenant, toujours dans le groupe G , l'équivalence principale à droite $\mathcal{R}_H$ définie par un complexe quelconque H . Puisque $\mathcal{R}_H$ est régulière à droite, la classe $U \text{ mod } \mathcal{R}_H$ qui contient l'élément-unité e de G est un sous-groupe. Par définition, U est l'ensemble des éléments u vérifiant $Qu = Q_e$, c'est-à-dire $u^{-1}H = H$, qui équivaut à $H = uH$ (et entraîne $UH = \bigcup_{u \in U} uH = H$);

tout élément u de U peut donc s'écrire, sous la forme $h_1 h_2^{-1}$.

Nous avons, d'autre part, $e \in Q_h$ pour tout $h \in H$, donc $Q_{h_1} \cap Q_{h_2}$ pour deux éléments h_1, h_2 quelconques de H . Si H est fort, cela entraîne $Q_{h_1} = Q_{h_2}$: H est contenu dans une classe $\text{mod } \mathcal{R}_H$; de plus, l'égalité précédente s'écrit

$$h_1^{-1}H = h_2^{-1}H,$$

d'où, pour tout $h_3 \in H$, $h_2^{-1}h_3 \in h_1^{-1}H$ et enfin

$$(7) \quad h_1 h_2^{-1} h_3 \in H \quad \text{quels que soient} \quad h_1, h_2, h_3 \in H.$$

Réciproquement, supposons vérifiée la condition (7) et supposons que deux quotients Q_a, Q_b se coupent, c'est-à-dire que l'on ait

$$x = a^{-1}h_1 = b^{-1}h_2, \quad \text{avec} \quad h_1, h_2 \in H,$$

d'où $ab^{-1} = h_1 h_2^{-1}$. Un élément m de Q_b est de la forme

$$m = b^{-1}h_3 = a^{-1}ab^{-1}h_3 = a^{-1}h_1 h_2^{-1}h_3 = a^{-1}h, \quad \text{où} \quad h \in H,$$

d'après (7); on a $m \in Q_a$ et, par conséquent, $Q_b \subseteq Q_a$; de même $Q_a \subseteq Q_b$, d'où l'égalité; H est un complexe fort : les complexes forts sont caractérisés par la condition (7).

Si H est fort, deux quelconques de ses éléments h_1, h_2 vérifient, comme on l'a vu, $h_1 \equiv h_2(\mathcal{R}_H)$, d'où $h_1 h_2^{-1} \equiv e$, c'est-à-dire $h_1 h_2^{-1} \in U$; par conséquent, H est contenu dans la classe à droite, par rapport au sous-groupe U , qui contient un quelconque de ses éléments h . Inversement, un élément $uh (h \in H)$ de cette classe s'écrit (toujours) $h_1 h_2^{-1} h$, donc (quand H est fort) appartient à H : le

complexe fort H est une classe à droite par rapport au sous-groupe U : on a, par suite, $\mathcal{R}_H = \mathcal{R}_U$.

Notons encore que, dans un groupe, tout complexe est net.

Enfin, dans un groupe, toute équivalence régulière à droite, est simplifiable à droite; il n'en est évidemment pas de même dans un demi-groupe quelconque ⁽¹⁾, mais nous allons établir, pour l'équivalence principale à droite $\mathcal{R}_H$ provenant d'un complexe fort H , un théorème dont la première partie comprend comme cas particulier la propriété des groupes qui vient d'être rappelée.

Définition. — Une équivalence $\mathcal{S}$ dans un demi-groupe D est dite *simplifiable à droite sur un complexe* K de D si

$$ax \in K, \quad bx \in K, \quad ax \equiv bx \quad (\mathcal{S})$$

entraînent

$$a \equiv b \quad (\mathcal{S}).$$

THÉOREME 4. — *a. Si H est un complexe fort dans le demi-groupe D , l'équivalence principale $\mathcal{R}_H$ est simplifiable à droite sur le complément $D_H^* = D - W_H$ du résidu à droite. Si, en particulier, H est net à droite ($W_H = \emptyset$), $\mathcal{R}_H$ est simplifiable à droite.*

b. Si H ⁽²⁾ n'est pas net à droite, une condition nécessaire et suffisante pour que $\mathcal{R}_H$ soit simplifiable à droite, est que D_H^ soit un idéal à droite. Si W_H est un idéal bilatère non vide, en particulier si l'on a $W_H = {}_H W \neq \emptyset$, la condition précédente n'est réalisée que si H est trivial ($T = D^2 \cap H = \emptyset$: $\mathcal{R}_H$ est l'équivalence universelle).*

a. Soit $ax \equiv bx (\mathcal{R}_H)$, avec $ax \in D_H^*$, $bx \in D_H^*$ (ce qui entraîne $a \in D_H^*$, $b \in D_H^*$). Nous avons $Q_{a,x} = Q_{b,x} \neq \emptyset$, d'où, en désignant par r un élément de ces quotients, $xr \in Q_a \cap Q_b$ et, puisque H est fort, $Q_a = Q_b$, donc $a \equiv b (\mathcal{R}_H)$. En prenant en outre $x \in D_H^*$, on voit que la trace $\mathcal{R}_H^*$ de $\mathcal{R}_H$ sur D_H^* est simplifiable à droite; il faut noter qu'en général D_H^* n'est pas un sous-demi-groupe de D . Si H est net à droite, on a $D_H^* = D$, l'équivalence $\mathcal{R}_H$ est simplifiable à droite.

b. Considérons le cas où H n'est pas net à droite et supposons $\mathcal{R}_H$ simplifiable à droite; soient $a \in D_H^*$, $m \in D$: si le produit am était un élément ω de W_H , on aurait aussi $\omega m \in W_H$, donc $am \equiv \omega m (\mathcal{R}_H)$ et $a \equiv \omega (\mathcal{R}_H)$, d'où $a \in W_H$, ce qui est absurde. Nous avons donc $am \in D_H^*$ et D_H^* est un idéal à droite.

⁽¹⁾ Comme l'a montré récemment M. G. THIERRIN, si un demi-groupe D est tel que toute équivalence régulière à droite soit simplifiable à droite, et que toute équivalence régulière à gauche soit simplifiable à gauche, D est un groupe.

⁽²⁾ Toujours supposé fort. On notera cependant que cette hypothèse sert seulement pour démontrer que la condition est suffisante.

Inversement, supposons que D_H^* soit un idéal à droite. D'après α , $ax \equiv bx(\mathcal{R}_H)$ entraîne $a \equiv b(\mathcal{R}_H)$ toutes les fois que la classe contenant ax et bx est distincte de W_H . Si, au contraire, ax et bx appartiennent à W_H , a et b appartiennent aussi à W_H puisque $D - W_H = D_H^*$ est un idéal à droite : il en résulte encore $a \equiv b(\mathcal{R}_H)$ et $\mathcal{R}_H$ est simplifiable à droite.

Si $W_H (\neq \emptyset)$ est un idéal bilatère, son complément D_H^* ne peut être qu'un idéal à droite *vide*, car $a \in D_H^*$, $w \in W_H$ entraîneraient

$$aw \in D_H^* \cap W_H.$$

COROLLAIRE. — *Dans un demi-groupe abélien D , l'équivalence principale à droite $\mathcal{R}_H$ associée à un complexe fort H , si elle est distincte de l'équivalence universelle, est simplifiable si H est net et seulement dans ce cas.*

En effet D étant abélien, H est équirésiduel.

La comparaison des équivalences régulières ou simplifiables d'un côté avec les équivalences principales du même côté conduit aux résultats suivants.

LEMME 1. — *Soit $\mathcal{R}$ une équivalence régulière à droite dans un demi-groupe D ; si H est un complexe saturé mod $\mathcal{R}$ (c'est-à-dire une somme de classes ou une classe mod $\mathcal{R}$), on a*

$$(8) \quad \mathcal{R} \subseteq \mathcal{R}_H.$$

Montrons que $a \equiv b(\mathcal{R})$ entraîne $Q_a = Q_b$, en posant toujours $Q_a = (H : a)_d$; il suffit évidemment d'établir, par exemple, l'inclusion $Q_a \subseteq Q_b$. Or, si $x \in Q_a$, c'est-à-dire si $ax \in H$, la congruence $ax \equiv bx(\mathcal{R})$ entraîne, puisque H est saturé mod $\mathcal{R}$, $bx \in H$, c'est-à-dire $x \in Q_b$.

COROLLAIRE. — *Si $\mathcal{R}$ est une équivalence régulière à droite, toute classe $H \bmod \mathcal{R}$ est indivisible mod $\mathcal{R}_H$.*

D'après (8), en effet, toute classe $H \bmod \mathcal{R}$ est contenue dans une classe mod $\mathcal{R}_H$.

LEMME 2. — *Considérons dans le demi-groupe D une équivalence $\mathcal{S}$ et un complexe H ; supposons H indivisible mod $\mathcal{S}$ et $\mathcal{S}$ simplifiable à droite sur H . Si les quotients à droite $Q_a = (H : a)_d$, $Q_b = (H : b)_d$ se coupent, on a $a \equiv b(\mathcal{S})$.*

Soit $x \in Q_a \cap Q_b$, c'est-à-dire $ax \in H$, $bx \in H$. Il en résulte

$$ax \equiv bx \quad (\mathcal{S}), \quad \text{d'où} \quad a \equiv b \quad (\mathcal{S}).$$

THÉOREME 5. — Soient $\mathcal{R}$ une équivalence régulière à droite dans le demi-groupe D , et H une classe mod $\mathcal{R}$ sur laquelle $\mathcal{R}$ est simplifiable à droite (ce qui a lieu, en particulier, si $\mathcal{R}$ est une équivalence simplifiable à droite).

a. On a

$$\mathcal{R} \subseteq \mathcal{R}_H$$

et, en désignant respectivement par $\mathcal{R}^*$ et $\mathcal{R}_H^*$ les traces de $\mathcal{R}$ et de $\mathcal{R}_H$ sur D_H^* ,

$$\mathcal{R}^* = \mathcal{R}_H^*.$$

En particulier, si H est en outre net à droite, on a $\mathcal{R} = \mathcal{R}_H$.

b. H est un complexe fort.

a. D'après le lemme 1 et son corollaire, nous avons $\mathcal{R} \subseteq \mathcal{R}_H$ et H est indivisible mod $\mathcal{R}_H$. L'inclusion $\mathcal{R} \subseteq \mathcal{R}_H$ entraîne $\mathcal{R}^* \subseteq \mathcal{R}_H^*$. Pour établir l'égalité, considérons deux éléments a, b de D_H^* congrus mod $\mathcal{R}_H^*$, donc tels que $Q_a = Q_b (\neq \emptyset)$. D'après le lemme 2 où l'on prend $\mathcal{S} = \mathcal{R}$, on a $a \equiv b(\mathcal{R})$ donc $a \equiv b(\mathcal{R}^*)$ et, par conséquent, $\mathcal{R}_H^* \subseteq \mathcal{R}^*$, d'où l'égalité.

Si H est net à droite, on a

$$D_H^* = D, \quad \mathcal{R} = \mathcal{R}^* = \mathcal{R}_H^* = \mathcal{R}_H.$$

b. Pour montrer que H est fort, supposons $x \in Q_a \cap Q_b$. Nous avons, d'après le lemme 2, $a \equiv b(\mathcal{R})$, donc $a \equiv b(\mathcal{R}_H)$, c'est-à-dire $Q_a = Q_b$.

Le théorème suivant permet de préciser dans quelle mesure l'équivalence principale à droite $\mathcal{R}_K$ associée à un complexe fort K , peut être définie par l'une quelconque de ses classes.

THÉOREME 6. — a. Soient K un complexe fort, H une classe mod $\mathcal{R}_K$ distincte du résidu W_K . On a

$$W_K \subseteq W_H, \quad \mathcal{R}_K \subseteq \mathcal{R}_H, \quad \mathcal{R}_K^* = \mathcal{R}_H^*,$$

$\mathcal{R}_K^*$ et $\mathcal{R}_H^*$ désignant les traces de $\mathcal{R}_K$ et de $\mathcal{R}_H$ sur $D_H^* = D - W_H$; H est un complexe fort.

b. Si, en outre, K est contenu dans une classe L mod $\mathcal{R}_K$, différente du résidu W_K , on a

$$W_K = W_L, \quad \mathcal{R}_K = \mathcal{R}_L.$$

c. Avec les hypothèses de *a* et de *b*, et si, en outre, W_H ne coupe pas K , $K \cap W_H = \emptyset$, on a

$$W_K = W_H, \quad \mathcal{R}_K = \mathcal{R}_H.$$

a. Les classes H et W_K étant distinctes, sont disjointes. On a donc, d'après le théorème 1, b , $W_K \subseteq W_H$ et, d'après le théorème 4, l'équivalence régulière à droite $\mathcal{R}_K$ est simplifiable à droite sur H . Cela entraîne, d'après le théorème 5, $\mathcal{R}_K \subseteq \mathcal{R}_H$, $\mathcal{R}_K^* = \mathcal{R}_H^*$ et H est un complexe fort.

b. D'après *a*, nous avons $W_K \subseteq W_L$; mais l'inclusion $K \subseteq L$ entraîne $W_L \subseteq W_K$, d'où l'égalité $W_L = W_K$. Puisque, toujours d'après *a*, $\mathcal{R}_L$ et $\mathcal{R}_K$ ont mêmes traces sur $D - W_L$, nous avons bien $\mathcal{R}_L = \mathcal{R}_K$.

c. Puisque $\mathcal{R}_K$ est contenue dans $\mathcal{R}_H$, W_H est une réunion de classes mod $\mathcal{R}_K$. L'hypothèse $K \cap W_H = \emptyset$ entraîne donc $L \cap W_H = \emptyset$ et $L \subseteq D_H^* = D - W_H$.

Mais alors, puisque les traces $\mathcal{R}_H^*$ et $\mathcal{R}_K^* = \mathcal{R}_L^*$ sur D_H^* coïncident, L est une classe mod $\mathcal{R}_H$, distincte de W_H par hypothèse. Appliquons la première partie *a* de l'énoncé en remplaçant K par H et H par L ; nous obtenons

$$W_H \subseteq W_L = W_K, \quad \mathcal{R}_H \subseteq \mathcal{R}_L = \mathcal{R}_K,$$

d'où

$$W_H = W_K, \quad \mathcal{R}_H = \mathcal{R}_K.$$

Remarques. — 1. Si K est un sous-demi-groupe de D , l'hypothèse $K \cap W_H = \emptyset$, dans *c*, est certainement vérifiée. Soient, en effet, $k \in K$; $h \in H$; considérons un élément x tel que $hx \in K$: nous aurons

$$k h x \in K^2 \subseteq K, \quad \text{donc} \quad x \in (K : k h)_d$$

en même temps que $x \in (K : h)_d$, d'où, puisque K est fort, $kh \equiv h(\mathcal{R}_K)$, c'est-à-dire $kh \in H$, donc enfin $k \notin W_H$.

2. Montrons, par un exemple extrêmement simple, qu'avec les hypothèses de *a*, on peut avoir $\mathcal{R}_K \subset \mathcal{R}_H$ strictement. Considérons le demi-groupe abélien $D = \{0, 1, 2\}$ défini par la table

	0	1	2
0	0	0	0
1	0	1	2
2	0	2	0

[sous-demi-groupe du demi-groupe multiplicatif $C/(4)$ (voir chap. IV, § 1, p. 143). Prenons $K = \{2\}$; nous avons

$$K:0 = \emptyset, \quad K:1 = \{2\}, \quad K:2 = \{1\};$$

K est fort et $\mathcal{R}_K (= {}_K\mathcal{R})$ est l'égalité. Le résidu W_K comprend le seul élément zéro. $H = \{1\}$ est une classe mod $\mathcal{R}_K$, distincte de W_K . Nous avons

$$H:0 = H:2 = \emptyset, \quad H:1 = \{1\}, \quad \text{donc } W_H = \{0, 2\} \supset K,$$

et

$$W_K \subset W_H, \quad \mathcal{R}_K \subset \mathcal{R}_H.$$

On vérifie aisément que H est fort.

Exercices. — 1. Toute intersection non vide de complexes forts d'un demi-groupe D est un complexe fort.

2. Un idéal à gauche $H (H \neq \emptyset)$ dans un demi-groupe D est un complexe net à droite. Que peut-on dire de l'équivalence principale à droite correspondante $\mathcal{R}_H$ quand, en outre, H est fort ?

3. Soit $D = \{1, 2, \dots, n, \dots\}$ le demi-groupe *additif* des nombres naturels. Le complexe M formé par les multiples d'un nombre fixe m est-il fort ? est-il net ? Quelle est l'équivalence principale correspondante $\mathcal{R}_M$ et que peut-on dire de l'ensemble-quotient $D/\mathcal{R}_M$?

Si l'on regarde maintenant D comme un demi-groupe *multiplicatif*, le même complexe M est-il fort ? est-il net ? Caractériser l'équivalence $\mathcal{R}_M$.

Dans le demi-groupe multiplicatif des nombres naturels D , on considère le sous-demi-groupe $S = \{n^\alpha\}_{n \in D}$, ensemble des puissances n^α , où α est un nombre naturel donné. Étudier les propriétés de S et de l'ensemble-quotient $D/\mathcal{R}_S$ (on pourra traiter d'abord le cas $\alpha = 2$).

4. On désigne par $a \cup b$ le plus grand commun diviseur de deux nombres naturels a, b et l'on considère l'ensemble $N = \{1, 2, \dots, n, \dots\}$ de ces nombres comme un *demi-groupe par rapport à l'opération $\cup$* (demi-treillis).

a. Déterminer le résidu W_h du complexe $\{h\}$ formé par un seul élément h de N . Comment faut-il choisir h pour que $\{h\}$ soit net ?

b. Caractériser l'équivalence principale $\mathcal{R}_h$ associée au complexe $\{h\}$.

c. Examiner le cas $h = 1$; montrer qu'une condition nécessaire et suffisante pour que l'on ait $x \equiv y (\mathcal{R}_1)$ est que x et y possèdent les mêmes facteurs premiers.

d. Montrer que $\mathcal{R}_1$ est régulière par rapport à la multiplication. $\mathcal{R}_h$, pour $h \neq 1$, a-t-elle la même propriété ? Peut-on indiquer une autre opération par rapport à laquelle $\mathcal{R}_1$ est régulière ?

5. Soit $\Delta = D \times D'$ le *produit direct* ⁽¹⁾ de deux demi-groupes multiplicatifs D, D' , c'est-à-dire l'ensemble des couples $\xi = (x, x')$, où x décrit D et x' décrit D' , avec la multiplication définie par

$$(x, x')(y, y') = (xy, x'y').$$

(1) Les produits directs de demi-groupes ont été étudiés par J. Ch. HARDEN, *Direct and semi-direct products of semi-groups* (Thèse, University of Tennessee, 1949).

On considère dans D un complexe H , dans D' un complexe H' et, dans Δ , le complexe $K = H \times H'$, ensemble des couples (h, h') , où $h \in H$, $h' \in H'$.

1° $\alpha = (a, a')$ étant un élément de Δ , caractériser le quotient à droite $Q_\alpha = (K : \alpha)$ au moyen des quotients $(H : a)_d$ et $(H' : a')_d$. Déterminer le résidu à droite W_K de K dans Δ à partir des résidus W_H de H dans D et $W_{H'}$ de H' dans D' .

2° Montrer qu'il suffit, pour que K soit un complexe fort dans Δ , que H et H' soient des complexes forts (respectivement dans D et dans D'). Examiner si cette condition est nécessaire.

Pour qu'un complexe fort H soit indivisible mod $\mathcal{R}_H$, il faut et il suffit que l'on ait

$$(9) \quad Q_{h_1} \cap Q_{h_2} \neq \emptyset$$

pour chaque couple d'éléments h_1, h_2 de H : tout complexe fort ayant la propriété (9) est dit parfait à droite. Si H est parfait à droite, il en est de même de $T = D^2 \cap H$. Un complexe parfait à droite, H , est disjoint de son résidu à droite W_H ; la classe $\bar{H} \bmod \mathcal{R}_H$ qui contient H , est distincte de W_H : elle est donc (d'après le théorème 6) un complexe fort, elle a même résidu à droite W_H et elle définit une équivalence principale à droite qui coïncide avec $\mathcal{R}_H$.

La condition (9) signifie qu'il existe, pour chaque couple d'éléments h_1, h_2 de H au moins un élément m de D tel que

$$(9') \quad h_1 m \in H \quad \text{et} \quad h_2 m \in H.$$

Elle se rattache à la notion suivante ⁽¹⁾ : deux complexes H_1, H_2 (dans un groupoïde E) sont dits *codivisibles à droite* si, pour chaque élément h_1 de H_1 et chaque élément h_2 de H_2 , il existe un élément m de E tel que

$$h_1 m \in H_2 \quad \text{et} \quad h_2 m \in H_1.$$

La condition (9) exprime que H est codivisible à droite avec lui-même.

Un complexe H parfait à droite, s'il est unitaire des deux côtés, est une classe mod $\mathcal{R}_H$. Soient $a \in \bar{H}$, où $\bar{H}$ est la classe contenant H , $h \in H$, $m \in Q_a = Q_h (\neq \emptyset)$. La relation $hm \in H$ entraîne $m \in H$, puis $am \in H$ entraîne $a \in H$: nous avons donc $\bar{H} = H$.

Si le demi-groupe D possède un élément-unité à droite, e , tout complexe H a la propriété (9') : il suffit de prendre $m = e$. Tout com-

⁽¹⁾ Cette notion intervient dans les conditions de permutabilité de deux équivalences principales à droite. Voir P. DUBREIL, *Contribution à la Théorie des Demi-groupes*, II (*Rendiconti di Matem. e delle sue applic.*, s. V, vol. X, 1951, p. 189), ainsi que l'exercice 7 p. 248 ci-dessous.

plexe fort, dans D , est donc parfait à droite. S'il est non seulement fort, mais unitaire, le complexe H est une classe mod $\mathcal{R}_H$.

Nous dirons qu'un complexe S est unitaire à droite par rapport à un complexe H si les relations $s \in S$, $xs \in H$ entraînent $x \in H$. S'il en est ainsi, toute partie non vide S' de S est encore un complexe unitaire à droite par rapport à H .

LEMME. — Soient K un complexe du demi-groupe D , U l'ensemble des éléments u de D vérifiant $uK \subseteq K$ (c'est-à-dire $uk \in K$ pour tout $k \in K$).

1° U est un sous-demi-groupe de D .

2° Tout complexe unitaire à droite contenant K contient U .

1° Soient $u_1, u_2 \in U$; nous avons, pour tout $k \in K$,

$$u_1 u_2 . k = u_1 . u_2 k = u_1 k' = k'', \quad \text{où } k', k'' \in K,$$

donc $u_1 u_2 \in U$; U est un sous-demi-groupe.

2° Si V est un complexe unitaire à droite contenant K , la relation $uk = k'$, où $k, k' \in K \subseteq V$ entraîne $u \in V$; on a donc $U \subseteq V$.

Remarque. — Si K est un sous-demi-groupe S , on a $S \subseteq U$.

THÉORÈME 7. — Dans un demi-groupe D , soient H un complexe fort et S un sous-demi-groupe ($\neq \emptyset$) contenu dans H .

1° S est contenu dans une classe $A \bmod \mathcal{R}_H$, distincte de W_H , et les conditions

α . $a \in A$;

β . $a.s \in H$ pour tout $s \in S$;

γ . $a.s_1 \in H$ pour un $s_1 \in S$,

sont équivalentes. Pour que A soit contenu dans H , il faut et il suffit que S soit unitaire à droite par rapport à H .

2° Le sous-demi-groupe $U (\neq \emptyset)$, ensemble des éléments u de D tels que l'on ait $us \in S$ pour tout $s \in S$, est contenu dans A :

$$S \subseteq U \subseteq A.$$

U , donc aussi S , est unitaire à droite par rapport à A .

3° Si l'on a $SH \subseteq H$ ⁽¹⁾, A est un sous-demi-groupe de D .

4° Si $T (= D^2 \cap H)$ est contenu dans S et si S est unitaire à droite, on a

$$S = U = A.$$

1° Quels que soient $s, t \in S$, nous avons $st \in S \subseteq H$, d'où $t \in Q_s$ et $S \subseteq Q_s$. Il en résulte que les quotients à droite de H par deux éléments s_1, s_2 de S , se coupent, donc coïncident puisque H est fort et nous avons

$$s_1 \equiv s_2 \quad (\mathcal{R}_S).$$

Soit alors A la classe $\text{mod } \mathcal{R}_H$ qui contient $S (A \not\equiv W_H)$ et $a \in A$: nous avons $Q_a = Q_s$, donc $S \subseteq Q_a$, c'est-à-dire

$$a.s' \in H \quad \text{pour tout } s' \in S.$$

Mais inversement, si l'on a

$$x.s_1 \in H \quad \text{pour un } s_1 \in S$$

(donc si l'on a $Q_x \not\equiv S$), il en résulte $s_1 \in Q_x \cap Q_s$, où $s \in S$, donc $Q_x = Q_s$ et $x \in A$.

A est donc l'ensemble des éléments x de D ayant la propriété précédente et les deux propositions : $A \subseteq H$, et « S est unitaire à droite par rapport à H » sont équivalentes.

2° U est contenu dans A , puisque $us \in S \subseteq H (s \in S)$ entraîne $u \in A$. De $xu = a$, où $u \in U$, résulte

$$x.us = as = h \in H, \quad \text{où } us = s_1 \in S,$$

donc $xs_1 \in H$ et $x \in A$. U est donc unitaire à droite par rapport à A ; S , contenu dans U , a la même propriété.

3° Soient $a_1, a_2 \in A, s \in S$. Nous avons $a_1 \equiv s(\mathcal{R}_H)$, d'où, puisque $\mathcal{R}_H$ est régulière à droite, $a_1 a_2 \equiv s a_2(\mathcal{R}_H)$. Or, $a_2 s$ est un élément de H et nous avons

$$s a_2 . s = s . a_2 s \in SH \subseteq H,$$

d'où $s a_2 \in A$ et $a_1 a_2 \in A$: A est un sous-demi-groupe.

(1) Cette condition est remplie dans les deux cas suivants :

1° H est un sous-demi-groupe de D :

$$SH \subseteq H^2 \subseteq H,$$

2° S est permis à droite dans H :

$$SH \subseteq S \subseteq H$$

(en particulier, S est un idéal à droite dans D).

4° La relation $a \in A$, c'est-à-dire $as \in H$, où $s \in S$, entraîne

$$as \in D^2 \cap H \subseteq S$$

et, par conséquent, $a \in S$: nous avons donc $A \subseteq S$, d'où la double égalité $S = U = A$,

Remarques. — 1. Tout élément-unité à gauche de D (s'il en existe) appartient au sous-demi-groupe U , donc à la classe A .

2. Si S est contenu dans D^2 , ce qui a lieu toutes les fois que S est globalement idempotent ($S^2 = S$), en particulier quand S se compose d'un élément idempotent a de H , on a $S \subseteq T$, et l'hypothèse de la quatrième partie, $T \subseteq S$, entraîne

$$T = S (= U = A).$$

Considérons maintenant un sous-demi-groupe fort S de D et appliquons le théorème 7 en prenant $H = S$, ce qui entraîne, d'après 1° et 2°, $U = A$. Nous obtenons la proposition suivante :

COROLLAIRE. — 1° Un sous-demi-groupe fort S de D est contenu dans une classe $U \bmod \mathcal{R}_S$ ($U \neq W_S$). U est un sous-demi-groupe fort ⁽¹⁾ et unitaire à droite.

2° U est le plus petit complexe unitaire à droite contenant S ; pour que $U = S$, donc pour que S soit une classe $\bmod \mathcal{R}_S$, il est non seulement nécessaire, mais suffisant que S soit unitaire à droite.

3° On a

$$W_S = W_U, \quad \mathcal{R}_S = \mathcal{R}_U$$

(th. 6, b).

THÉOREME 8. — Soit S un sous-demi-groupe fort de D .

1° Pour tout quotient non vide $Q_a = (S:a)_a$ ou ${}_aQ = (S:a)_g$ et pour toute classe $X \bmod \mathcal{R}_S$ distincte du résidu W_S (si $W_S \neq \emptyset$), on a

$$Q_a \cdot S \subseteq Q_a, \quad S \cdot {}_aQ \subseteq {}_aQ, \quad S \cdot X \subseteq X \quad (X \neq W_S).$$

2° Si D vérifie la règle de simplification à droite et si, dans S , deux éléments quelconques s_1, s ont un quotient à gauche

$$s_1 = qs, \quad q \in S,$$

on a, pour toute classe $X \neq W_S$ et pour tout $x \in X$,

$$X = S \cdot X = S \cdot x;$$

X a même puissance que S .

(1) D'après le théorème 5.

1° Soit $x \in Q_a$, c'est-à-dire $ax = s_1 \in S$ et, par conséquent,

$$axs = s_1s \in S, \quad \text{pour tout } s \in S,$$

d'où

$$xs \in Q_a \quad \text{et} \quad Q_a \cdot S \subseteq Q_a.$$

On a de même $S \cdot {}_aQ \subseteq {}_aQ$. S étant fort, toute classe $X \neq W_s$ est un quotient à gauche non vide, on a donc $S \cdot X \subseteq X$.

2° La relation précédente, $S \cdot X \subseteq X$, met en évidence une analogie partielle avec la décomposition d'un groupe en classes à droite par rapport à un sous-groupe. Avec les hypothèses plus fortes indiquées dans l'énoncé, cette analogie se précise. Soient $x, x_1 \in X (\neq W_s)$: il existe un élément y de D appartenant à $Q_x = Q_{x_1}$:

$$xy = s \in S, \quad x_1y = s_1 \in S,$$

d'où, avec les notations de l'énoncé, $x_1y = qxy$ et $x_1 = qx$ où $q \in S$, donc $x_1 \in Sx$ et

$$X \subseteq Sx \subseteq SX (\subseteq X),$$

ce qui entraîne la double égalité

$$X = S \cdot X = S \cdot x.$$

L'application $s \rightarrow sx$ de S sur $X = Sx$ est biunivoque, puisque

$$s'x = s''x \quad \text{entraîne} \quad s' = s''.$$

Quand le demi-groupe D n'est pas globalement idempotent ($D^2 \neq D$), il y a intérêt, comme nous l'avons vu, à associer à un complexe H (non trivial) l'ensemble $T = D^2 \cap H$ (non vide) : T a mêmes résidus que H , définit les mêmes équivalences principales à droite et à gauche et possède en même temps que H chacune des propriétés fondamentales : fort, symétrique, parfait ou net (à droite ou à gauche). Comme nous allons le voir maintenant, ce complexe T , contenu dans D^2 , joue un rôle important dans l'étude des ensembles-quotients et des homomorphismes.

THEOREME 9. — Soient H un complexe fort non trivial dans le demi-groupe D , $\mathcal{R}_H = \mathcal{R}_T$ l'équivalence principale à droite définie dans D par H ou par $T (= D^2 \cap H)$, $\mathcal{T}$ la trace de cette équivalence sur D^2 , $\mathcal{R}'_T$ l'équivalence principale à droite définie par T dans D^2 , W'_T le résidu de T dans D^2 .

1° T est un complexe fort, non seulement dans D , mais dans D^2 ; on a

$$W_H \cap D^2 \subseteq W'_T, \quad \mathfrak{T} \subseteq \mathcal{R}'_T,$$

$\mathfrak{T}$ et $\mathcal{R}'_T$ ont mêmes traces sur $D^2 - W'_T$.

2° Si, de plus, T et W_H sont disjoints, on a les égalités

$$W_H \cap D^2 = W'_T, \quad \mathfrak{T} = \mathcal{R}'_T.$$

3° Si, en outre, T et ${}_H W$ sont disjoints, en particulier si H est net, on a la correspondance biunivoque

$$D/\mathcal{R}_H \leftarrow \rightarrow D^2/\mathcal{R}'_T$$

qui est un isomorphisme si $\mathcal{R}_H$ (donc aussi $\mathcal{R}'_T$) est régulière des deux côtés.

1° Soient Q_a, Q'_a les quotients à droite de T , respectivement dans D et dans D^2 , par un élément $a \in D^2$: nous avons $Q'_a = Q_a \cap D^2$. Si Q_a est vide, Q'_a l'est aussi : on a donc $W_H \cap D^2 \subseteq W'_T$. Si Q'_a coupe Q'_b , Q_a coupe Q_b , d'où $Q_a = Q_b$, puis $Q'_a = Q'_b$: T est fort dans D^2 . Si a, b sont deux éléments de D^2 , $a \equiv b(\mathfrak{T})$ entraîne $a \equiv b(\mathcal{R}'_T)$, nous avons donc $\mathfrak{T} \subseteq \mathcal{R}'_T$. Puisque $Q'_a \not\subseteq Q'_b$ entraîne $Q_a \not\subseteq Q_b$, $\mathfrak{T}$ et $\mathcal{R}'_T$ ont mêmes traces sur $D^2 - W'_T$.

2° Soit $w = pq \in W'_T$. S'il existait un élément x de D tel que $wx = h \in H$ où, par hypothèse, h , élément de T , n'appartient pas à W_H , on pourrait trouver $y \in D$ vérifiant $hy \in H$, d'où :

$$w.xy \in D^2 \cap H = T, \quad \text{avec } xy \in D^2,$$

c'est-à-dire $Q'_w \neq \emptyset$, ce qui est contradictoire. Nous avons donc

$$w \in W_H, \quad \text{d'où} \quad W'_T \subseteq W_H \cap D^2$$

et, par conséquent, l'égalité.

W'_T étant une classe mod $\mathfrak{T}$ et mod $\mathcal{R}'_T$, ces deux équivalences, qui ont même trace sur $D^2 - W'_T$, coïncident : $\mathfrak{T} = \mathcal{R}'_T$.

3° Toute classe mod $\mathcal{R}_H$ contient un élément de D^2 , car, en premier lieu, le résidu W_H , s'il n'est pas vide, est permis à droite, donc contient des produits; et si maintenant A est une classe distincte de W_H et contenant l'élément a , on a une relation de la forme $a.x = h \in T \subseteq H$, avec par hypothèse, $h \notin {}_H W$: il existe donc un élément m de D tel que $mh = ma.x \in H$, d'où, puisque H est fort, $ma \equiv a(\mathcal{R}_H)$, c'est-à-dire $ma \in A$.

En associant à chaque classe $X \in D/\mathcal{R}_H$ son intersection avec D^2

$$X \cap D^2 = X' \in D^2/\mathcal{C} = D^2/\mathcal{R}_T,$$

nous définissons entre les ensembles quotients $D/\mathcal{R}_H$ et $D^2/\mathcal{R}_T$ une correspondance biunivoque qui est un isomorphisme si $\mathcal{R}_H$ est régulière non seulement à droite mais à gauche. En effet, $\mathcal{C} = \mathcal{R}_T$ est, alors, régulière aussi et les classes X ou X' se multiplient comme des représentants que l'on peut, d'après ce qui précède, prendre dans D^2 .

Remarque. — L'énoncé précédent est valable, dans toutes ses conclusions, lorsque H est un complexe fort, symétrique, disjoint de de son résidu.

Lorsqu'elles proviennent d'un complexe *symétrique* H , les équivalences principales $\mathcal{R}_H = {}_H\mathcal{R} (= \mathcal{R})$ fournissent un *homomorphisme* du demi-groupe D considéré sur le demi-groupe $D/\mathcal{R}$. Le cas important est évidemment celui où, en outre, H est *fort* : le paragraphe § va être consacré à l'étude des *complexes symétriques forts* et aux homomorphismes qui s'en déduisent, notamment à la *recherche des groupes et pseudo-groupes homomorphes à un demi-groupe D donné*.

Exercices ⁽¹⁾. — 6. Si un complexe H est contenu dans un complexe fort K et si $\mathcal{R}_H^*$, $\mathcal{R}_K^*$ sont les traces de $\mathcal{R}_H$ et de $\mathcal{R}_K$ sur $D_H^* = D - W_H$, on a $\mathcal{R}_H^* \subseteq \mathcal{R}_K^*$. Si H et K ont même résidu à droite, $W_H = W_K$, on a $\mathcal{R}_H \subseteq \mathcal{R}_K$.

7. Si H est l'intersection non vide de deux complexes forts H_1 , H_2 , et si H , H_1 , H_2 , ont même résidu à droite, on a

$$\mathcal{R}_H = \mathcal{R}_{H_1} \cap \mathcal{R}_{H_2}.$$

8. Soient S_1 , S_2 deux sous-demi-groupes forts de D dont l'intersection $S = S_1 \cap S_2$ n'est pas vide et a même résidu à droite que S_1 et S_2 .

a. Pour que les équivalences principales à droite $\mathcal{R}_{S_1}$ et $\mathcal{R}_{S_2}$ soient permutables (ou associables), il faut que S_1 et S_2 soient codivisibles à droite.

b. Cette condition nécessaire est aussi suffisante lorsqu'en outre le résidu à gauche de S , ${}_S W$, est disjoint avec un au moins des ensembles S_1 , S_2 .

c. Soient U_1 , U_2 deux sous-demi-groupes forts et unitaires de D dont l'intersection U n'est pas vide et a même résidu à droite que U_1 et U_2 . Si U_1 et U_2 sont échangeables à gauche (c'est-à-dire si, pour chaque couple, $x_1 \in U_1$, $x_2 \in U_2$, il existe $y_1 \in U_1$ et $y_2 \in U_2$ tels que $x_1 y_2 = x_2 y_1$), U_1 et U_2 sont codivisibles à droite.

d. Pour que deux sous-groupes G_1 , G_2 d'un demi-groupe D (en particulier

⁽¹⁾ Au sujet des trois exercices suivants, on pourra consulter P. DUBREIL, *Contribution à la Théorie des demi-groupes*. II (*Rendiconti di Matem. e delle sue applic.*, s. V, vol. X, p. 183, chap. I, n° 3).

d'un groupe) soient codivisibles à droite, il faut et il suffit qu'ils soient permutable : $G_1 G_2 = G_2 G_1$.

9. Dans un demi-groupe D , un élément r tel que le complexe $\{r\}$ soit net à droite (ou à gauche) est appelé *élément zéroïde* à droite (ou à gauche) ⁽¹⁾.

a. L'ensemble des éléments zéroïdes à droite et celui des éléments zéroïdes à gauche sont respectivement un idéal à droite R et un idéal à gauche L (éventuellement vides).

Pour que R ne soit pas vide, il faut et il suffit qu'il existe dans D un idéal à droite non vide minimum.

L'ensemble des éléments zéroïdes bilatères est l'intersection $U = R \cap L$, et contient le complexe produit $V = RL$.

b. $V = RL$ est un groupe. Si z est l'élément-unité de V , on a $R = zD$, $L = Dz$, $U = zDz$, et enfin $U = R = L = V$.

§. Complexes symétriques forts. Pseudo-groupes et groupes homomorphes à un demi-groupe D donné. — Soient H un complexe symétrique dans le demi-groupe D , $W (= W_{||} = {}_{||}W)$ son résidu, $\mathcal{R} (= \mathcal{R}_{||} = {}_{||}\mathcal{R})$ l'équivalence principale correspondante : l'ensemble-quotient $\mathcal{T} = D/\mathcal{R}$ que nous désignerons aussi par D/H , est un demi-groupe homomorphe à D , dont W , s'il n'est pas vide, est élément permis, ou zéro.

THÉOREME 1. — Supposons le complexe symétrique H fort, non trivial : $T = D^2 \cap H \neq \emptyset$, et tel que

$$T \cap W = \emptyset.$$

1° Si $t = ab$ appartient à T , il existe un élément y de D tel que

$$ty \in H, \quad b \equiv by \quad \text{et} \quad t \equiv ty \quad (\mathcal{R}).$$

2° Si $x \equiv t(\mathcal{R})$, on a

$$x \equiv xy \quad (\mathcal{R}), \quad xy \in H$$

et T est saturé dans $D^2 \bmod \mathcal{R}$, c'est-à-dire : si $x (\equiv t \in T)$ appartient à D^2 , on a $x \in T$.

1° Puisque $T (\subseteq H)$ est disjoint de W , il existe dans D un élément y vérifiant $ty = aby \in H$, et nous avons $a \in {}_bQ \cap {}_{by}Q$, donc, puisque H est fort, $b \equiv by(\mathcal{R})$. En multipliant à gauche par a , nous en déduisons $t \equiv ty(\mathcal{R})$.

2° La congruence $x \equiv t(\mathcal{R})$ entraîne $xy \equiv ty(\mathcal{R})$, d'où $x \equiv xy(\mathcal{R})$, avec $xy \in H$ puisque $y \in Q_x = Q_t$.

(1) On pourra consulter A. H. CLIFFORD et D. D. MILLER, *Semigroups having zeroïd elements* (Amer. J. Math., t. 70, 1948, p. 117, nos 1 et 2).

Si $x \in D^2$, c'est-à-dire $x = rs$, nous avons $rs \equiv rsy(\mathcal{R})$. Comme t et, par conséquent, les éléments $x = rs$ et rsy qui lui sont congrus mod $\mathcal{R}$, n'appartiennent pas à W , on peut simplifier, ce qui donne ${}_sQ = {}_{sy}Q$. Or, $y \in Q_x$ entraîne $rsy \in H$, c'est-à-dire $r \in {}_{sy}Q$: nous avons donc aussi $r \in {}_sQ$, c'est-à-dire $x = rs \in H$, d'où $x \in T$.

Nous supposons, jusqu'à nouvel ordre, que le résidu W du complexe symétrique fort H n'est pas vide : $\mathcal{F} = D/H$ admet alors W comme élément zéro, et l'on peut parler des noyaux $\mathcal{N}_d$, $\mathcal{N}_g$ et $\mathcal{N}$ de $\mathcal{F}$ (§ 4, p. 231).

LEMME 1. — *Si trois éléments A, B, X de $\mathcal{F}$ vérifient*

$$AX = BX \neq W,$$

on a ⁽¹⁾

$$A = B \neq W.$$

Chacun des éléments A, B est distinct de W , puisque W est permis. Soient a, b, x des représentants, dans D , des classes A, B, X ; nous avons $ax \equiv bx(\mathcal{R})$, où ax et bx appartiennent à $D^* = D - W$; il en résulte $a \equiv b(\mathcal{R})$ (§ 4, th. 4, p. 237) donc $A = B$.

COROLLAIRE. — *Tout sous-demi-groupe de $\mathcal{F}$ qui ne contient pas W est un semi-groupe.*

Ce corollaire s'applique, en particulier, aux noyaux $\mathcal{N}_d$, $\mathcal{N}_g$ et $\mathcal{N} = \mathcal{N}_d \cap \mathcal{N}_g$ lorsqu'ils ne sont pas vides, puisque W , zéro de $\mathcal{F}$, n'appartient ni à $\mathcal{N}_d$, ni à $\mathcal{N}_g$.

LEMME 2. — *Si le noyau $\mathcal{N}$ de $\mathcal{F}$ n'est pas vide, tout élément X de $\mathcal{N}_d$ est simplifiable à droite dans $\mathcal{F}$:*

$$X \in \mathcal{N}_d \quad \text{et} \quad AX = BX \quad \text{entraînent} \quad A = B.$$

Tout élément de $\mathcal{N}$ est simplifiable.

Si $AX = BX = W$, on a, puisque $X \in \mathcal{N}_d$, $A = W$, $B = W$, donc $A = B$.

Si $AX = BX \neq W$, l'égalité $A = B$ résulte du lemme 1.

De même, tout élément de $\mathcal{N}_g$ est simplifiable à gauche; par conséquent, tout élément du noyau $\mathcal{N}$ est simplifiable.

(1) Nous nous dispensons d'énoncer la proposition symétrique.

LEMME 3. — *Si le complexe symétrique fort H est contenu dans son résidu W , les noyaux $\mathcal{N}_d$, $\mathcal{N}_g$ et $\mathcal{N}$ sont vides.*

Soient A un élément de $\mathcal{F}$ distinct de W , a un élément de la classe A : $a \notin W$. Il existe un élément x de D tel que $ax \in H \subseteq W$ et l'on a $a \in {}_xQ$, donc x n'appartient pas à W . En passant aux classes, nous obtenons $AX = W$, $X \neq W$: A est donc diviseur de zéro dans $\mathcal{F}$ et le noyau à droite $\mathcal{N}_d$ est vide, d'où $\mathcal{N} = \emptyset$. On a, de même, $\mathcal{N}_g = \emptyset$.

LEMME 4. — *Si le demi-groupe-quotient $\mathcal{F} = D/H$ associé au complexe symétrique fort H (non trivial) admet un élément-unité à gauche U , on a*

$$T \cap W = \emptyset \quad (T = D^2 \cap H)$$

et T est saturé, dans D^2 , par rapport à $\mathcal{R}$. La classe U est, dans D , un sous-demi-groupe unitaire à gauche.

Supposons que $\omega \in D^2 \cap H \cap W$, d'où $\omega = xy$. Puisque $UW = W$, nous avons, en désignant par u un élément quelconque de U ,

$$uw = uxy \in W.$$

Or, X désignant la classe à laquelle appartient x , l'égalité $UX = X$ entraîne $ux \equiv x(\mathcal{R})$, donc $Q_x = Q_{ux}$; et, puisque nous avons $\omega = xy \in H$, c'est-à-dire $y \in Q_x$, il vient $uxy = uw \in H$, donc ${}_uQ \neq \emptyset$, ce qui est en contradiction avec $\omega \in W$.

Nous avons donc bien $T \cap W = \emptyset$ et, d'après le théorème 1, T est saturé, dans D^2 , par rapport à $\mathcal{R}$.

Dans D , la classe U , image inverse de l'élément-unité à gauche u du demi-groupe homomorphe $\mathcal{F}$, est un sous-demi-groupe unitaire à gauche (chap. IV, § 2, th. 2, p. 148).

THÉOREME 2. — *Soit $\mathcal{N}$ le noyau du demi-groupe $\mathcal{F} = D/H$ associé à un complexe symétrique fort H du demi-groupe D .*

a. Si $\mathcal{N}$ n'est pas vide, $\mathcal{F}$ possède un élément-unité bilatère U et le complexe $T = D^2 \cap H$ est parfait.

b. Réciproquement, si le complexe T est parfait, $\mathcal{F}$ possède un élément-unité bilatère U et $\mathcal{N}$ n'est pas vide.

a. $\mathcal{N}$ n'étant pas vide, considérons une classe $S \in \mathcal{F}$ appartenant à $\mathcal{N}$, donc distincte du résidu W . Soit s un élément de S : il existe un élément s' de D tel que l'on ait $ss' \in H$. D'après cette relation, s' n'appartient pas à W ; on a donc, en désignant par S' la classe qui le

contient, $S' \neq W$ et, par conséquent, S appartenant à $\mathcal{N}$, la classe-produit SS' est distincte de W .

Il en résulte $ss' \notin W$ et, par conséquent, il existe un élément u de D tel que $uss' \in H$: on a donc $s' \in Q_s \cap Q_{us}$ et, puisque H est fort, $us \equiv s(\mathcal{R})$ donc, dans $\mathcal{F}$, $US = S$.

Or, d'après le lemme 2, S est, dans $\mathcal{F}$, un élément simplifiable : U est, par conséquent, élément-unité bilatère de $\mathcal{F}$ (chap. II, § 5, cor. 1, p. 86). Dans D , la classe U est un sous-demi-groupe unitaire; d'après le lemme 4, le complexe $T = D^2 \cap H$ est disjoint de W et saturé, dans D^2 , par rapport à $\mathcal{R}$.

Soit t un élément quelconque de T : $t = ab \in H$. Puisque T est disjoint de W , il existe dans D , d'après le théorème 1, un élément y tel que $ty \in H$, $b \equiv by(\mathcal{R})$. Or nous avons aussi $b \equiv bu(\mathcal{R})$, donc $by \equiv bu(\mathcal{R})$, d'où $u \equiv y(\mathcal{R})$, puisque la classe B contenant b , bu , by est distincte de W (car $b \in W$ entraînerait $t = ab \in W$). Nous avons, par conséquent, $tu \in H$: quels que soient t et de même $t' \in T$, u appartient à $Q_t \cap Q_{t'}$, le complexe (fort) T est parfait.

b. Réciproquement, T , s'il est parfait, est contenu dans une classe mod $\mathcal{R}_T$, c'est-à-dire mod $\mathcal{R}$. Soit C cette classe, *distincte du résidu* $W (= W_T)$, comme nous le savons. Si A est un élément de $\mathcal{F}$ distinct de W et si a appartient à la classe A , il existe dans D des éléments x, y tels que $ax \in T$, $ya \in T$, d'où, en revenant aux classes, $AX = YA = C$. En particulier, il existe une classe U vérifiant l'égalité $UC = C$. Il en résulte, pour $A \neq W$,

$$UAX = UC = C = AX \quad (C \neq W),$$

d'où, d'après le lemme 1, $UA = A$. Comme on a, en outre, $UW = W$, U est *élément-unité à gauche* de $\mathcal{F}$. De même, $\mathcal{F}$ possède un élément-unité à droite U' et l'on a $U = U' (= U'U)$. L'élément-unité bilatère U de $\mathcal{F}$ appartient aux noyaux à droite $\mathcal{N}_d$ et à gauche $\mathcal{N}_g$, donc au noyau $\mathcal{N}$, qui n'est pas vide. (Dans D , la classe U est un sous-demi-groupe unitaire. On a $U \neq W$.)

THÉORÈME 3. — *S'il n'est pas vide, le noyau $\mathcal{N}$ du demi-groupe quotient $\mathcal{F} = D/H$ de D par le complexe symétrique fort (non trivial) $H \subseteq D$, est un groupe. Le groupe $\mathcal{N}$ est maximal dans $\mathcal{F}$. $\mathcal{F}$ est isomorphe au quotient D^2/T , ($T = D^2 \cap H$).*

Conservons les notations du théorème précédent, en supposant maintenant $A \in \mathcal{N}$. De cette hypothèse et de $C \neq W$ résulte $CA \neq W$.

Il existe donc un élément B de $\mathcal{F}$ tel que

$$CAB = C = CU \quad (\neq W), \quad \text{d'où} \quad AB = U, \quad (B \neq W),$$

et

$$BAB = BU = B = UB \quad \text{d'où} \quad BA = U.$$

De plus, on a $B \in \mathcal{N}$, car $BM = W$ par exemple entraîne, en multipliant à gauche par A , $M = W$. Le demi-groupe $\mathcal{N}$ ayant un élément-unité U , et tout élément A de $\mathcal{N}$ possédant, dans $\mathcal{N}$, un inverse B , $\mathcal{N}$ est un groupe.

Supposons qu'il existe un sous-groupe $\mathcal{G}$ de $\mathcal{F}$ contenant $\mathcal{N}$:

$$\mathcal{N} \subseteq \mathcal{G} \subseteq \mathcal{F},$$

et soit $R \in \mathcal{G}$. L'égalité $RX = W$ entraîne, en multipliant à gauche par l'inverse R^{-1} de R dans $\mathcal{G}$,

$$\begin{aligned} R^{-1}RX &= R^{-1}W = W, \\ &= UX = X, \end{aligned}$$

donc $X = W$ et, par conséquent, $R \in \mathcal{N}_d$; de même, $R \in \mathcal{N}_g$, d'où

$$R \in \mathcal{N} \quad \text{et} \quad \mathcal{G} = \mathcal{N}.$$

D'après le théorème 2, T est parfait, donc disjoint de son résidu W : $T \cap W = \emptyset$, et nous avons (th. 9, § 4, p. 247) l'isomorphisme :

$$\mathcal{F} \simeq D^2/T$$

Résumons les principaux résultats contenus dans les énoncés précédents.

THÉORÈME 4. — *H étant un complexe symétrique, fort, non trivial du demi-groupe D , $\mathcal{R}(= \mathcal{R}_H = {}_H\mathcal{R})$ l'équivalence principale correspondante, $\mathcal{F} = D/H$ le demi-groupe homomorphe associé, ou bien le noyau $\mathcal{N}$ de $\mathcal{F}$ est vide (par exemple quand H est contenu dans son résidu W), ou bien $\mathcal{N}$ n'est pas vide, et alors $\mathcal{N}$ est un sous-groupe maximal de $\mathcal{F}$, dont l'élément-unité U est élément-unité de $\mathcal{F}$. Le complexe fort $T = D^2 \cap H$ est saturé dans D^2 par rapport à $\mathcal{R}$, et parfait; si inversement T est parfait, $\mathcal{N}$, non vide, est un groupe. La classe-unité U est, dans D , un sous-demi-groupe unitaire.*

Cas particulier. — Supposons que le complexe H soit un sous-demi-groupe symétrique fort S ; il est alors parfait, et il en est de même du sous-demi-groupe $T = D^2 \cap S$. Soit E la classe mod $\mathcal{R}$ qui contient S : c'est un sous-demi-groupe fort et unitaire, ayant mêmes résidus et

définissant les mêmes équivalences principales que S , E est donc symétrique lui aussi et distinct du résidu W .

Le sous-demi-groupe E , regardé comme élément de $\mathcal{F} = D/S$ est idempotent. Or, T étant parfait, $\mathcal{F}$ a un élément-unité U , appartenant au noyau $\mathcal{N}$. Nous avons

$$E^2 = E = EU \quad (\neq W),$$

d'où

$$E = U.$$

THÉOREME 4. — *A un sous-demi-groupe symétrique fort S correspond un noyau non vide $\mathcal{N}$ qui est un groupe (maximal dans $\mathcal{F}$); l'élément unité U de $\mathcal{N}$ et de $\mathcal{F}$ n'est autre que la classe mod $\mathcal{R}$ qui contient S : c'est, dans D , un sous-demi-groupe symétrique, fort et unitaire ayant même résidu et définissant la même équivalence principale que S .*

Revenons au demi-groupe quotient $\mathcal{F} = D/H$ associé à un complexe symétrique fort (non trivial) H ayant un résidu non vide W . Le noyau $\mathcal{N}$ de $\mathcal{F}$, contenu dans $\mathcal{F}^* = \mathcal{F} - \{W\}$, est un sous-groupe maximal de $\mathcal{F}$; donc, $\mathcal{F}^*$ est un groupe, et $\mathcal{F}$ un pseudo-groupe, si $\mathcal{N} = \mathcal{F}^*$ et seulement dans ce cas.

Alors, $\mathcal{F}^*$ est multiplicativement fermé dans $\mathcal{F}$; son image inverse $D^* = D - W$ l'est aussi dans D ; par conséquent, l'idéal W est premier. Réciproquement, supposons que W soit, dans D , un idéal premier; si l'on a, dans $\mathcal{F}$, $X \neq W$ et $XX' = W$, des éléments x, x' appartenant aux classes X, X' vérifient $x \notin W$ et $xx' \in W$, ce qui entraîne $x' \in W$, donc $X' = W$: tout élément X de $\mathcal{F}^*$ appartient au noyau à droite $\mathcal{N}_d$ et de même au noyau à gauche $\mathcal{N}_g$, donc à $\mathcal{N}$, d'où enfin $\mathcal{F}^* = \mathcal{N}$, ce qui donne la proposition suivante :

THÉOREME 5. — *H étant un complexe symétrique fort (non trivial) du demi-groupe D , pour que $\mathcal{F} = D/H$ soit un pseudo-groupe, il faut et il suffit que le résidu W de H soit premier.*

Cas particulier. — Pour examiner le cas où le complexe symétrique fort H est un sous-demi-groupe S , il sera utile de faire intervenir la proposition suivante :

LEMME 5. — *Si le résidu à droite W_s d'un sous-demi-groupe S de D est un idéal à gauche (donc un idéal bilatère) et s'il contient le résidu à gauche ${}_sW$, W_s est un idéal premier.*

Soient a, b deux éléments de $D - W_s$. Il existe un élément x tel que $bx \in S$; puisque $a \in D - {}_sW$, il existe un élément y tel que $ya \in S$. Nous avons donc

$$yabx \in S,$$

d'où $yab \in D - W_s$ et, puisque W_s est un idéal à gauche, $ab \in D - W_s$. $D - W_s$ est donc multiplicativement fermé, et W_s est premier.

A fortiori, si S est un sous-demi-groupe équirésiduel, en particulier si S est un sous-demi-groupe symétrique, son résidu $W (= W_s = {}_sW)$ est premier.

Cela étant, appelons *sous-demi-groupe pseudo-normal* tout sous-demi-groupe S de D qui est *symétrique*, fort et possède un résidu non vide W (premier) : $\mathcal{F}$ est alors un pseudo-groupe, la classe $U \bmod \mathcal{R}$ contenant S est, d'après le théorème 4', un sous-demi-groupe pseudo-normal et unitaire; U est élément-unité de $\mathcal{F} = D/S = D/U$, et coïncide avec S si S est lui-même unitaire. Donc,

THÉOREME 5'. — *A tout sous-demi-groupe pseudo-normal et unitaire U du demi-groupe D correspond un pseudo-groupe D/U , homomorphe à D , dont U est l'élément-unité.*

Examinons maintenant le cas où le résidu W du complexe H est vide, c'est-à-dire où H est non seulement fort et symétrique, mais net (donc non trivial : $T = D^2 \cap H \neq \emptyset$).

Adjoignons à D un élément zéro z ($zx = xz = z$ pour tout $x \in D$, $z^2 = z$). Dans le demi-groupe $\Delta = D + \{z\}$, D est multiplicativement fermé : l'idéal $Z = \{z\}$ est premier; de plus, Z est le résidu de H ($\subseteq D$) dans Δ . Soient Q_a, Q'_a les quotients à droite de H par $a \in D$ pris respectivement dans D et dans Δ : comme $x = z$ n'est pas solution de $ax \in H$, nous avons $Q'_a = Q_a$. Par suite, H est fort dans Δ comme dans D et l'équivalence principale à droite $\mathbf{P}_H$ définie par H dans Δ a pour trace sur D l'équivalence $\mathcal{R}_H$: les propriétés symétriques étant, de même, valables, H est symétrique dans Δ ; posons $\mathbf{P} = \mathbf{P}_H = {}_H\mathbf{P}$. Comme le résidu Z de H dans Δ est premier, $\mathcal{F} = \Delta/\mathbf{P}$ est un pseudo-groupe homomorphe à Δ ; $\mathcal{G} = \mathcal{F} - \{Z\} = D/\mathcal{R} = D/H$ est un groupe homomorphe à D .

Inversement, il est clair qu'un complexe symétrique fort H non trivial tel que $\mathcal{F} = D/\mathcal{R}$ soit un groupe, est nécessairement net. Le résidu W de H , s'il n'était pas vide, serait en effet une classe mod $\mathcal{R}$, donc, dans $\mathcal{F}$, un élément permis : alors $\mathcal{F}$ (qui ne se réduit pas à $\{W\}$ puisqu'on suppose H non trivial), ne vérifierait pas la règle de simplification et ne pourrait pas être un groupe. Énonçons le théorème obtenu.

THÉOREME 6. — *H étant un complexe symétrique fort non trivial du demi-groupe D, pour que le demi-groupe quotient D/H soit un groupe, il faut que H soit net. Réciproquement, si H est symétrique, fort et net (donc non trivial), D/H est un groupe homomorphe à $D^{(1)}$.*

Cas particulier. — Appelons sous-demi-groupe normal tout sous-demi-groupe S de D qui est symétrique, fort et net. La classe $U \bmod \mathcal{R}$ ($= \mathcal{R}_S = {}_S\mathcal{R}$) contenant S est, d'après le théorème 4', un sous-demi-groupe normal et unitaire; U est, d'autre part, élément-unité de $\mathcal{F} = D/S$. Enfin, si S est unitaire, il coïncide avec U. Donc,

THÉOREME 6'. — *A tout sous-demi-groupe normal et unitaire U du demi-groupe D correspond un groupe D/U , homomorphe à D, dont U est l'élément-unité.*

Montrons maintenant que les pseudo-groupes ou groupes homomorphes à D obtenus par la méthode précédente, sont les seuls, à des isomorphismes près. Nous utiliserons, à cet effet, le théorème suivant :

THÉOREME 7. — *Soient $\bar{D}$ un demi-groupe homomorphe au demi-groupe D, $\mathcal{R}$ l'équivalence d'homomorphisme. Supposons que $\bar{D}$ soit la somme d'un groupe $\bar{G}$ et d'un idéal $\bar{Z}$ (éventuellement vide) : $\bar{D} = \bar{G} + \bar{Z}$. Désignons par G le sous-demi-groupe image inverse de $\bar{G}$, par Z l'idéal image inverse de $\bar{Z}$ ⁽²⁾ : $D = G + Z$.*

a. $\mathcal{R}$ est simplifiable sur toute classe $H \bmod \mathcal{R}$ contenue dans G, c'est-à-dire image inverse d'un élément $\bar{h}$ de $\bar{G}$; H est un complexe fort, ses résidus W_H et ${}_H W$ coïncident avec Z; $\mathcal{R}$ et $\mathcal{R}_H$ (ou ${}_H\mathcal{R}$) ont même trace sur G : H est symétrique.

b. Si $\bar{Z}$ est vide ou se réduit à un élément, on a $\mathcal{R} = \mathcal{R}_H = {}_H\mathcal{R}$.

c. La classe-unité U est un sous-demi-groupe unitaire de D.

a. Les relations $ax \in G$, $bx \in G$ (d'où $a, b, x \in G$, puisque $D - G$ est un idéal Z) et $ax \equiv bx (\mathcal{R})$ entraînent, pour les éléments-images $\bar{a}, \bar{b}, \bar{x} \in \bar{G}$ l'égalité $\bar{a}\bar{x} = \bar{b}\bar{x}$, d'où $\bar{a} = \bar{b}$. $\mathcal{R}$ est donc, sur G, simplifiable à droite (et, de même, à gauche); en particulier, $\mathcal{R}$ est simplifiable sur H qui est, par suite, un complexe fort (§ 4, th. 5, p. 239).

(¹) Les théorèmes 4 à 6 sont dus à R. CROISOT, *Propriétés des complexes forts et symétriques des demi-groupes* (Bull. Soc. Math., t. 80, 1952, p. 217).

(²) Cf. chap. IV, § 2, th. 3, p. 149.

H et l'idéal Z étant disjoints, le résidu W_H de H contient Z , $Z \subseteq W_H$; d'autre part, si $a \in G$, la condition $ax \in H$ est vérifiée par toute image inverse x de l'élément $\bar{x} = (\bar{a})^{-1} \bar{h}$. Nous avons donc $G \cap W_H = \emptyset$, c'est-à-dire $W_H \subseteq Z$, d'où $W_H = Z$; de même, ${}_H W = Z$. On sait, de plus, que $\mathcal{R}_H$ a même trace que $\mathcal{R}$ sur $D - W_H = G$; ${}_H \mathcal{R}$ également; nous avons donc $\mathcal{R}_H = {}_H \mathcal{R}$ et H est symétrique.

b. S'il se réduit à un élément, $\bar{Z}$ est un zéro premier de $\bar{D}$, qui est un pseudo-groupe. Z est une classe mod $\mathcal{R}$ ou $\mathcal{R}_H$ et nous avons

$$\mathcal{R} = \mathcal{R}_H = {}_H \mathcal{R}.$$

Si $\bar{Z}$ est vide, $\bar{D}$ est le groupe $\bar{G}$, nous avons

$$D = G \quad \text{et} \quad \mathcal{R} = \mathcal{R}_H = {}_H \mathcal{R}.$$

c. La classe-unité U est un sous-demi-groupe de D , fort et symétrique comme toute classe H contenue dans G . En outre, U est *unitaire*. Soit, en effet, $ux \in U$, où $u \in U (\subseteq G)$ et $x \in D$. Si x appartenait à l'idéal Z , nous aurions $ux \in Z$, ce qui est impossible puisque Z est disjoint de G , donc de U . Par conséquent, x appartient à G et la relation $ux \in U$ entraîne, dans $\bar{G}$, $\bar{u}\bar{x} = \bar{u}$, où $\bar{u}$ est l'élément-unité de G , donc $\bar{x} = \bar{u}$ et $x \in U$.

Les hypothèses du théorème 7 sont vérifiées en premier lieu toutes les fois qu'on a un groupe $\bar{G}$ homomorphe à D ; alors, $\bar{Z}$ et Z sont *vides*, G coïncide avec D et le théorème prend la forme suivante :

THÉOREME 7' (théorème d'homomorphisme). — *Si $\bar{G}$ est un groupe homomorphe au demi-groupe D*

$$D \sim \bar{G}$$

et si $\mathcal{R}$ désigne l'équivalence d'homomorphisme, toute classe H mod $\mathcal{R}$ est un complexe fort, symétrique et net ($W_H = Z = \emptyset$). L'équivalence d'homomorphisme $\mathcal{R}$, régulière et simplifiable, coïncide avec l'équivalence principale $\mathcal{R}_H = {}_H \mathcal{R}$ définie par H . La classe-unité U est un sous-demi-groupe normal et unitaire. On a les isomorphismes

$$\bar{G} \simeq D/H \simeq D/U.$$

D'après les théorèmes 6' et 7', il existe une correspondance

biunivoque entre les groupes homomorphes à D et les sous-demi-groupes normaux et unitaires de D ⁽¹⁾.

Les hypothèses du théorème 7 sont encore vérifiées lorsqu'il existe un pseudo-groupe $\bar{P}$ homomorphe à D : on a ici $\bar{P} = \bar{G} + \bar{Z}$, où $\bar{G}$ est un groupe et où $\bar{Z} = \{\bar{z}\}$ est l'idéal constitué par le zéro de $\bar{P}$. Le théorème 7 prend la forme suivante :

THÉORÈME 7". — *S'il existe un pseudo-groupe $\bar{P} = \bar{G} + \{\bar{z}\}$ homomorphe au demi-groupe D, et si Z est l'idéal image inverse du zéro $\bar{z}$ de P, l'équivalence d'homomorphisme $\mathcal{R}$, simplifiable sur $G = D - Z$, coïncide avec les équivalences principales $\mathcal{R}_H$ et ${}_H\mathcal{R}$ définies par une quelconque H des classes mod $\mathcal{R}$ qui sont distinctes de Z. Une telle classe H est un complexe symétrique, fort, ayant pour résidu l'idéal premier Z. La classe-unité U est un sous-demi-groupe pseudo-normal et unitaire de D.*

D'après les théorèmes 5' et 7", il existe une correspondance biunivoque entre les pseudo-groupes homomorphes à D et les sous-demi-groupes pseudo-normaux et unitaires.

Proposons-nous maintenant de comparer les résultats précédents avec ceux que nous avons obtenus dans le cas abélien (§ 1, p. 220) Considérons la relation binaire σ_H définie de la façon suivante dans un demi-groupe D, à partir d'un complexe H : on pose $a\sigma_H a'$ s'il existe $h, h' \in H$ tels que $ha = h'a'$, et seulement dans ce cas. Cette relation σ_H , appelée relation de réversibilité à droite associée à H est réflexive, symétrique et régulière à droite : $a\sigma_H a'$ entraîne $(ax)\sigma_H(a'x)$ pour tout $x \in D$. Mais, en général, σ_H n'est pas transitive.

Soit donc Σ_H la fermeture transitive de σ_H , définie par $a\Sigma_H a'$ s'il existe un entier naturel ν tel que $a\sigma_H^\nu a'$, ou encore s'il existe $m_1, \dots, m_{\nu-1} \in D$ tels que

$$Ha \{ H m_1 \} \dots \{ H m_{\nu-1} \} H a',$$

$Hx \{ Hy$ signifiant que les complexes Hx, Hy ne sont pas disjoints. Σ_H est une équivalence régulière à droite associée au complexe H et appelée équivalence réversible généralisée. On définit symétriquement

(1) On trouvera dans la première édition de cette Algèbre (chap. V, § 3, p. 160), une démonstration de l'isomorphisme $\bar{G} \simeq D/U$ et de la correspondance biunivoque entre les groupes homomorphes et les sous-demi-groupes normaux et unitaires, qui se limite strictement à ces propriétés.

la relation régulière à gauche ${}_H\sigma(a{}_H\sigma a'$ s'il existe $h, h' \in H$ tels que $ah = a'h'$) et sa fermeture transitive ${}_H\Sigma$, équivalence régulière à gauche.

L'inclusion $H \subseteq K$ entraîne

$$\sigma_H \subseteq \sigma_K, \quad \Sigma_H \subseteq \Sigma_K.$$

Un cas remarquable est celui où H est un *sous-demi-groupe réversible à droite* S . Montrons qu'alors σ_S est transitive, ce qui entraîne l'égalité $\sigma_S = \Sigma_S$; Σ_S est appelée *équivalence réversible à droite* associée à S . Soient les égalités

$$sa = s'a', \quad s'_1 a' = s''_1 a'', \quad s, s', s'_1, s''_1 \in S.$$

Nous avons

$$s_0 s' = s'_0 s'_1, \quad \text{avec } s_0, s'_0 \in S,$$

d'où

$$s_0 s. a = s'_0 s''_1. a'',$$

c'est-à-dire

$$s_2 a = s''_2 a'',$$

où $s_2 = s_0 s$ et $s''_2 = s'_0 s''_1$ appartiennent à S .

La condition de réversibilité à droite (quels que soient $y, y_1 \in S$ il existe $x, x_1 \in S$ tels que $xy = x_1 y_1$) est vérifiée, en particulier, dans les deux cas suivants :

1° S est un *groupe* (il suffit de prendre $x = y^{-1}, x_1 = y_1^{-1}$). Un tel sous-groupe S de D est d'ailleurs non seulement *réversible*, mais *unitaire* puisque, par exemple, $sa = s_1 \in S$ entraîne $a = s^{-1} s_1 \in S$. L'équivalence réversible correspondante $\Sigma_S = \sigma_S$ est définie par

$$a \equiv b \quad (\Sigma_S) \quad \text{si} \quad s_1 a = s_2 b \quad (s_1, s_2 \in S)$$

ou, ce qui revient au même, si

$$b = s_2^{-1} s_1. a = sa \quad (s \in S),$$

et seulement dans ce cas. Cette condition, de même forme que celle qui intervient dans la décomposition d'un groupe G en classes par rapport à un sous-groupe S , entraîne que S est une *classe mod* Σ_S . Σ_S est régulière à droite; si la règle de simplification à droite est valable dans D , Σ_S est simplifiable à droite : S est alors un *complexe fort* ⁽¹⁾

(1) La propriété d'être un complexe fort étant symétrique, nous voyons qu'un sous-groupe S d'un demi-groupe D est un complexe fort dès que la *règle de simplification* est valable dans D d'un certain côté. Si cette condition n'est pas remplie, la propriété

et l'on a

$$\Sigma_S \subseteq \mathcal{R}_S.$$

Nous avons rencontré un exemple de ce cas à propos des *éléments associés* dans un semi-groupe D ou dans un domaine d'intégrité : S était le *groupe des unités*, E (chap. IV, § 14, B' , p. 216). Remarquons que l'équivalence principale à droite $\mathcal{R}_E$ décompose D en deux classes seulement, E et $D - E$, car, a étant donné, la relation $ax = \varepsilon \in E$ entraîne $a \cdot x\varepsilon^{-1} = \varepsilon\varepsilon^{-1} = e$, donc $a \in E$, $x \in E$ et nous avons :

$$Q_a = E \quad \text{si } a \in E, \quad Q_a = \emptyset \quad \text{si } a \in D - E.$$

2° S est un sous-demi-groupe abélien de D ($x = y_1$, $x_1 = y$). Plus particulièrement, D est abélien et S en est un sous-demi-groupe (cf. § 1).

Dans un demi-groupe D qu'on ne suppose pas abélien, l'équivalence réversible généralisée Σ_S associée à un sous-demi-groupe quelconque S , a les propriétés suivantes :

THEOREME 8. — S étant un sous-demi-groupe de D , on a

$$sa \equiv a \quad (\Sigma_S) \quad \text{pour tout } s \in S \text{ et tout } a \in D.$$

Σ_S est la plus fine des équivalences $\mathbf{P}$ telles que $sa \equiv a(\mathbf{P})$ pour tout $s \in S$ et tout $a \in D$.

Désignons par s_1 un élément quelconque de S : nous avons

$$s_1 s = s_2 \in S, \quad \text{d'où} \quad s_1 \cdot sa = s_2 a,$$

c'est-à-dire $(sa)\sigma_S a$ et, par conséquent,

$$sa \equiv a \quad (\Sigma_S).$$

Soit $\mathbf{P}$ une équivalence telle que $sa \equiv a(\mathbf{P})$ pour tout $s \in S$ et tout $a \in D$. La relation $a\sigma_S a'$, c'est-à-dire $sa = s'a'$, entraîne

$$a \equiv sa = s'a' \equiv a' \quad (\mathbf{P});$$

nous avons $\sigma_S \subseteq \mathbf{P}$, d'où $\Sigma_S \subseteq \mathbf{P}$, puisque Σ_S est la fermeture transitive de σ_S .

peut cesser d'être vraie. Considérons, par exemple, le demi-groupe $D = \{a, b\}$ défini par la table

	a	b
a	a	a
b	a	b

D contient les deux groupes $A = \{a\}$, $B = \{b\}$. B est un complexe fort, mais A n'en est pas un ($A:a = \{a, b\}$, $A:b = \{a\}$).

Remarque. — D'après le théorème 8, la relation

$$a \equiv a' \quad (\Sigma_S),$$

où a et a' sont des éléments quelconques de D , entraîne $sa \equiv s'a' \quad (\Sigma_S)$ quels que soient les éléments s, s' du sous-demi-groupe S ; inversement, s'il existe deux éléments s et s' de S tels que $sa \equiv s'a' \quad (\Sigma_S)$, on a

$$a \equiv a' \quad (\Sigma_S).$$

THÉORÈME 9. — *a. L'extension saturée $\bar{S}$ du sous-demi-groupe S par Σ_S est un sous-demi-groupe unitaire à gauche; $\bar{S}$ est le plus petit sous-demi-groupe unitaire à gauche contenant S et, pour que S coïncide avec $\bar{S}$, il est non seulement nécessaire, mais suffisant que S soit unitaire à gauche. On a (dans tous les cas)*

$$\Sigma_{\bar{S}} = \Sigma_S.$$

b. Si S est unitaire à gauche, on a

$$\Sigma_S \subseteq \mathcal{R}_S.$$

a. $\bar{S}$ est l'ensemble des éléments x de D vérifiant $x \equiv s \quad (\Sigma_S)$, avec $s \in S$. On a alors une suite d'égalités

$$s_0 x = s'_0 m_1, \quad s_1 m_1 = s'_1 m_2, \quad \dots, \quad s_v m_v = s'_v s = s^* \in S.$$

Multiplions à droite par un élément y de $\bar{S}$:

$$y \equiv s' \quad (\Sigma_S), \quad \text{où } s' \in S.$$

Nous obtenons

$$xy \equiv y \quad (\Sigma_S), \quad \text{d'où} \quad xy \equiv s' \quad (\Sigma_S)$$

et, par conséquent, $xy \in \bar{S}$; $\bar{S}$ est donc un sous-demi-groupe de D .

Les relations

$$xa \in \bar{S} \quad \text{et} \quad x \in \bar{S},$$

c'est-à-dire

$$xa \equiv s_1 \quad \text{et} \quad x \equiv s \quad (\Sigma_S), \quad (s, s_1 \in S),$$

entraînent, en tenant compte du théorème 8 et puisque Σ_S est régulière à droite,

$$a \equiv sa \equiv xa \equiv s_1 \quad (\Sigma_S),$$

donc $a \in \bar{S}$; par suite, $\bar{S}$ est unitaire à gauche.

Soit U un sous-demi-groupe unitaire à gauche contenant S . Si $x \in \bar{S}$, nous avons

$$x \equiv s \quad (\Sigma_S), \quad \text{où } s \in S \subseteq U,$$

d'où, Σ_S étant contenue dans Σ_U , $x \equiv s(\Sigma_U)$, c'est-à-dire

$$u_0 x = u'_0 p_1, \quad \dots, \quad u_{k-1} p_{k-1} = u'_{k-1} p_k, \quad u_k p_k = u'_k s,$$

où $u_i, u'_i, s \in U$. Puisque U est un sous-demi-groupe unitaire à gauche, ces relations entraînent successivement

$$p_k \in U, \quad p_{k-1} \in U, \quad \dots, \quad x \in U.$$

et nous avons bien $\bar{S} \subseteq U$. Cette propriété entraîne l'égalité $S = \bar{S}$ dès que S est unitaire à gauche.

Supposons $a \equiv a'(\Sigma_S)$, c'est-à-dire

$$t_i q_i = t'_i q_{i+1} \quad (i = 0, 1, \dots, l),$$

où l'on pose $a = q_0$, $a' = q_{l+1}$ et où $t_i, t'_i \in \bar{S}$, donc

$$t_i \equiv s_i, \quad t'_i \equiv s'_i \quad (\Sigma_S), \quad \text{avec} \quad s_i, s'_i \in S.$$

Nous avons

$$s_i q_i \equiv t_i q_i = t'_i q_{i+1} \equiv s'_i q_{i+1} \quad (\Sigma_S),$$

d'où

$$q_i \equiv q_{i+1}(\Sigma_S) \quad \text{et} \quad a \equiv a' \quad (\Sigma_S), \quad \text{donc} \quad \Sigma_S \subseteq \Sigma_S;$$

comme S est contenu dans $\bar{S}$, nous avons bien l'égalité

$$\Sigma_S = \Sigma_{\bar{S}}.$$

b. Supposons S unitaire à gauche et soit

$$s a = s' a' \quad (s, s' \in S).$$

La relation $ax \in S$ entraîne $sax \in S$, c'est-à-dire

$$s' a' x \in S, \quad \text{d'où} \quad a' x \in S;$$

$a \sigma_S a'$ implique donc $Q_a \subseteq Q_{a'}$ et, de même, $Q_{a'} \subseteq Q_a$, donc l'égalité, c'est-à-dire $a \equiv a'(\mathcal{R}_S)$. Nous avons, par conséquent,

$$\sigma_S \subseteq \mathcal{R}_S, \quad \text{d'où} \quad \Sigma_S \subseteq \mathcal{R}_S.$$

Remarque. — Quel que soit le sous-demi-groupe S , Σ_S est contenue dans l'équivalence principale à droite $\mathcal{R}_{\bar{S}}$ définie par $\bar{S}$, puisque nous avons

$$\Sigma_S = \Sigma_{\bar{S}} \subseteq \mathcal{R}_{\bar{S}}.$$

THÉORÈME 10. — Soit S un sous-demi-groupe unitaire à gauche ⁽¹⁾ et fort du demi-groupe D . Pour que les traces Σ_S^* , $\mathcal{R}_S^*$ des équi-

⁽¹⁾ Le théorème subsiste si l'on remplace l'hypothèse : S unitaire à gauche, par une autre plus faible, mais moins simple qui, lorsque S est fort, entraîne également $\Sigma_S \subseteq \mathcal{R}_S$. Voir P. DUBREIL, *Contribution à la Théorie des Demi-groupes*, II (*Rendiconti di Matem. e delle sue applic.*, s. V. vol. X, 1951, p. 183, th. 11 et 13a).

valences réversible généralisée et principale à droite définies par S , sur le complément $D^* = D - W_s$ du résidu à droite de S , coïncident,

$$(2) \quad \Sigma_s^* = \mathcal{R}_s^*,$$

il faut et il suffit que Σ_s soit simplifiable à droite sur D^* et que $S (\subseteq D^*)$ soit indivisible mod Σ_s .

1° La condition est nécessaire. — L'égalité (2) étant supposée vraie, les relations

$$ax \in D^*, \quad a'x \in D^*$$

(qui entraînent $a, a' \in D^*$, puisque W_s est permis à droite) et $ax \equiv a'x (\Sigma_s^*)$ entraînent $ax \equiv a'x (\mathcal{R}_s^*)$, donc (th. 4, § 4, p. 237)

$$a \equiv a' (\mathcal{R}_s^*) \quad \text{et} \quad a \equiv a' (\Sigma_s^*).$$

Σ_s est donc simplifiable sur D^* . De plus, $S (\subseteq D^*)$ étant indivisible mod $\mathcal{R}_s^*$ l'est aussi mod Σ_s^* .

2° La condition est suffisante. — Soit $a \equiv a' (\mathcal{R}_s^*)$, où $a, a' \in D^*$, c'est-à-dire $Q_a = Q_{a'} (\neq \emptyset)$. Si $x \in Q_a = Q_{a'}$, nous avons

$$ax = s \in S, \quad a'x = s' \in S,$$

d'où, puisque S est supposé indivisible mod Σ_s , $ax \equiv a'x (\Sigma_s)$. On peut simplifier à droite cette congruence, puisqu'on a $ax \in D^*$, $a'x \in D^*$: il vient donc $a \equiv a' (\Sigma_s)$ ou (Σ_s^*) et, par suite, $\mathcal{R}_s^* \subseteq \Sigma_s^*$, d'où l'égalité (2).

Pour qu'un sous-demi-groupe S soit indivisible mod Σ_s , il faut et il suffit que l'on ait, quels que soient $s, s' \in S$,

$$(3) \quad ss' \equiv s's (\Sigma_s).$$

Il faut et il suffit, en effet, que l'on ait $s \equiv s' (\Sigma_s)$; or, nous avons

$$s \equiv s's \quad \text{et} \quad s' \equiv ss' (\Sigma_s),$$

d'où la condition (3), qui a la signification d'une commutativité atténuée.

S'il est indivisible mod Σ_s et unitaire à gauche, S constitue une classe mod Σ_s .

Si l'égalité $\Sigma_s^* = \mathcal{R}_s^*$ a lieu, $S (\subseteq D^*)$ est une classe mod $\mathcal{R}_s^*$, donc est aussi un sous-demi-groupe unitaire à droite.

Si D vérifie la règle de simplification à droite (plus généralement si l'égalité est simplifiable à droite sur le complexe SD^2) et si la relation σ_s est transitive (c'est-à-dire coïncide avec Σ_s), Σ_s est simplifiable à droite dans D (donc sur D^*).

En effet, la congruence $ax \equiv a'x (\Sigma_s)$ s'écrit

$$sax = s'a'x \quad (s, s' \in S, sax \in SD^2)$$

et entraîne

$$sa = s'a', \quad \text{donc} \quad a \equiv a' (\Sigma_s).$$

Si S est un sous-demi-groupe réversible à droite, on a, comme nous l'avons vu, $\sigma_s = \Sigma_s$; S est indivisible mod Σ_s puisque, s, s' étant deux éléments de S , il existe deux éléments s_1, s'_1 de S vérifiant l'égalité $s_1s = s'_1s$, ce qui donne $s \equiv s' (\Sigma_s)$.

Si S est, en outre, unitaire à gauche, nous aurons, d'après le théorème 9, $S = S$; S sera donc une classe mod Σ_s . Or, Σ_s est régulière à droite. Si Σ_s est simplifiable à droite sur S , ce qui a lieu notamment quand D vérifie la règle de simplification à droite, S est fort et nous avons $\Sigma_s^* = \mathcal{R}_s^*$ (§ 4, th. 5, p. 239), enfin S est unitaire (à droite comme à gauche, d'après la corollaire p. 245) ⁽¹⁾.

Si S est net à droite, l'égalité $\Sigma_s^* = \mathcal{R}_s^*$, si elle a lieu, s'écrit

$$\Sigma_s = \mathcal{R}_s.$$

Quand il existe un groupe $\bar{G}$ homomorphe à un demi-groupe abélien D , la classe-unité U est, comme nous l'avons vu au paragraphe 1, un sous-demi-groupe net, unitaire et, évidemment, réversible; l'équivalence d'homomorphisme Σ_U est simplifiable (puisque la règle de simplification est valable dans G). Nous avons donc $\Sigma_U = \mathcal{R}_U$, ce qui met en évidence la concordance des résultats obtenus dans le cas abélien (§ 1) et dans le cas général (§ 5).

Exemple. — Considérons le demi-groupe $D = \{x_0, x_1, x_2, x_3\}$ défini par la table

	x_0	x_1	x_2	x_3
x_0	x_0	x_0	x_2	x_2
x_1	x_1	x_1	x_3	x_3
x_2	x_2	x_2	x_0	x_0
x_3	x_3	x_3	x_1	x_1

On vérifie aisément que le produit $x_i x_j$ est égal à x_p , où $p \equiv i + 2E\left(\frac{j}{2}\right) \pmod{4}$, ce qui montre que D est bien un demi-groupe; d'ailleurs, D est le produit

⁽¹⁾ Ces propriétés se vérifient aisément par un calcul direct. Voir P. DUBREIL, *Contribution à la Théorie des Demi-groupes*. I [Mémoires de l'Académie des Sciences, t. 63, 1941, note ⁽¹⁰⁾, p. 44].

direct ⁽¹⁾ du groupe $\Gamma = \{a, b\}$ par le demi-groupe $\Delta = \{c, d\}$ définis respectivement par les tables

Γ		a	b
a		a	b
b		b	a

Δ		c	d
c		c	c
d		d	d

Dans le demi-groupe D , la règle de simplification est valable à droite, mais ne l'est pas à gauche.

Considérons dans D le sous-demi-groupe $S = \{x_0, x_1\}$ et le complexe $H = \{x_2, x_3\}$. On a

$$(S; x_0)_d = S = (S; x_0)_g,$$

$$(S; x_1)_d = S = (S; x_1)_g,$$

$$(S; x_2)_d = H = (S; x_2)_g,$$

$$(S; x_3)_d = H = (S; x_3)_g,$$

S est un sous-demi-groupe normal et unitaire; l'ensemble quotient D/S est un groupe : c'est le groupe cyclique d'ordre 2, isomorphe à Γ . On vérifie que le complexe H est symétrique, fort et net, et que l'on a

$$\mathcal{R}_H = \mathcal{R}_S.$$

On a, d'autre part,

$$Sx_0 = S = Sx_1, \quad Sx_2 = H = Sx_3,$$

Σ_S coïncide donc avec $\mathcal{R}_S$. Mais les égalités

$$x_0 S = \{x_0\}, \quad x_1 S = \{x_1\}, \quad x_2 S = \{x_2\}, \quad x_3 S = \{x_3\}$$

montrent que ${}_S\Sigma$ est l'égalité, donc ne coïncide pas avec

$${}_S\mathcal{R} = \mathcal{R}_S = \Sigma_S.$$

Exercices. — 1. On considère le demi-groupe $D = \{x_0, x_1, x_2\}$ défini par la table

	x_0	x_1	x_2
x_0	x_0	x_0	x_2
x_1	x_1	x_1	x_2
x_2	x_2	x_2	x_2

Étudier le sous-demi-groupe $S = \{x_0, x_1\}$. Montrer qu'il est fort et symétrique; que peut-on dire du demi-groupe quotient $\mathcal{F} = D/S$?

2. Soient Σ_S l'équivalence réversible généralisée à droite définie par un sous-demi-groupe S d'un demi-groupe D , S l'extension saturée de S par Σ_S , V le complexe

$$V = \bigcup_{s \in S} (S; s)_d.$$

(¹) Voir exerc. 5 (§ 4, p. 241).

a. On a

$$S \subseteq V \subseteq \bar{S} \quad \text{et} \quad \Sigma_V = \Sigma_S (= \Sigma_{\bar{S}}).$$

b. S est dit *uni à gauche* si l'on a $SV \subseteq V$. Montrer :

1° Que tout sous-demi-groupe unitaire à gauche est uni à gauche;

2° Que tout sous-demi-groupe réversible à droite est uni à gauche.

c. Si S est fort, on a $V = \bar{S}$.

d. Pour que $V = \bar{S}$, il faut et il suffit que S soit uni à gauche ⁽¹⁾.

3. Soit Z le centre d'un demi-groupe D, c'est-à-dire l'ensemble des éléments z permutables avec tout élément a de D ($az = za$).

Z est un sous-demi-groupe abélien de D; les équivalences réversibles à gauche et à droite définies par Z coïncident :

$$\Sigma_Z = z\Sigma.$$

Si D est un *semi-groupe*, Z est unitaire, fort et symétrique.

4. Soit x un élément d'un demi-groupe D; on considère les couples d'éléments a, b de D vérifiant l'égalité

$$(4) \quad xa = bx.$$

On désigne par J_x l'ensemble des éléments a , par J_x l'ensemble des éléments b . J_x (par exemple) est un sous-demi-groupe contenant x et le centre Z.

Si l'on a $J_x = D$, x est dit *intérieur à droite*. L'ensemble des éléments intérieurs à droite est, par définition, l'*intérieur à droite* I_d de D. On définit symétriquement l'*intérieur à gauche* I_g . L'intérieur I de D est l'intersection $I_d \cap I_g$. Quel est l'intérieur d'un groupe ?

L'intérieur d'un demi-groupe D est un sous-demi-groupe (éventuellement vide) contenant le centre Z de D.

Si D est un *semi-groupe* dont l'intérieur I n'est pas vide, la relation (4) définit, pour tout élément x de I, un automorphisme $a \rightarrow b$ de D, appelé *automorphisme intérieur* ⁽²⁾.

6. **Immersion d'un demi-groupe régulier à droite dans un groupe.** — Abordée seulement dans un passé récent, l'étude des problèmes d'immersion dans le *cas non abélien* a été entreprise par O. Ore ⁽³⁾,

⁽¹⁾ Cf. P. DUBREIL, *Contribution à la Théorie des Demi-groupes*. II (*Rendiconti di Matem. e delle sue applic.*, s. V, vol. X, 1951, p. 183, th. 9 et 10).

⁽²⁾ Cf. P. DUBREIL, *Contribution à la Théorie des Demi-groupes*. I (*Mémoires de l'Académie des Sciences*, t. 63, 1941, p. 47-51).; R. CROISOT, *Automorphismes intérieurs d'un semi-groupe*, *Bull. Soc. Math. de France*, t. 82, 1954, à paraître.

⁽³⁾ O. ORE, *Linear Equations in non commutative Fields* (*Annals of Math.*, t. 32, 1931, p. 463).

A. Malcev ⁽¹⁾ et poursuivie par plusieurs auteurs ⁽²⁾. Nous suivrons ici, dans ses grandes lignes, la méthode de Ore ⁽³⁾ : le résultat auquel elle conduit, s'il n'est pas le plus général, se distingue par sa simplicité et son élégance, et trouve des applications utiles dans la Théorie des équations linéaires et dans celle des modules ⁽⁴⁾. Il peut s'énoncer de la façon suivante : *tout demi-groupe régulier à droite* ⁽⁵⁾ (*ou à gauche*) *peut être plongé dans un groupe*.

Le second problème d'immersion consiste à construire un *corps* contenant un anneau donné, qui doit évidemment ne pas contenir de véritables diviseurs de zéro. (Dans le cas abélien, comme nous l'avons vu, cette condition nécessaire est aussi suffisante).

Soit S un semi-groupe, non nécessairement abélien. *Pour que S admette comme extension un groupe G , il faut que les égalités*

$$\begin{aligned} (1) \quad & bs = b's', \\ (1') \quad & as = a's', \\ (1'') \quad & bt = b't', \end{aligned}$$

entr'éléments de S , entraînent

$$(2) \quad at = a't',$$

(condition Z de Malcev). On a, en effet, dans G ,

$$a'^{-1}a = s's^{-1} = b'^{-1}b = t't^{-1}.$$

⁽¹⁾ A. MALCEV, *On the immersion of an algebraic Ring into a Field* (*Math. Ann.*, t. 113, 1937, p. 686); *Über die Einbettung von assoziativen Systemen in Gruppen* (*Rec. Math. Moscou*, t. 6, 1939, p. 331 et t. 8, 1940, p. 251).

⁽²⁾ L. LESIEUR, *Sur les anneaux réguliers, avec ou sans diviseurs de zéro* (*C. R. Acad. Sc.*, t. 223, 1946, p. 1083 et t. 224, 1947, p. 321); *Anneaux réguliers, anneaux de matrices*, (*J. Math. pures et applic.*, t. 27, 1948, p. 205-253).

M. L. DUBREIL-JACOTIN, *Sur l'immersion d'un semi-groupe dans un groupe* (*C. R. Acad. Sc.*, t. 225, 1947, p. 787).

R. DOSS, *Sur l'immersion d'un semi-groupe dans un groupe* (*Bull. Sciences Math.*, 2^e s., t. 72, 1948, p. 1).

J. LAMBEK, *The immersibility of a semi-group into a group* (*Canad. J. Math.*, t. 3, 1951, p. 34).

D. TAMARI, *Sur l'immersion d'un semi-groupe topologique dans un groupe topologique*, (*Colloque d'Algèbre et de Théorie des Nombres*, C. N. R. S., Paris, 1950, p. 217); *Monôïdes préordonnés et chaînes de Malcev* (*Thèse*, Paris, 1951).

⁽³⁾ Quelques détails de démonstration seront empruntés à J. H. M. WEDDERBURN, *Non commutative domains of integrity* (*J. f. Math.*, t. 167, 1932, p. 129). Ce Mémoire est consacré aux anneaux euclidiens : Wedderburn résout pour ces anneaux, qui sont un cas particulier de ceux que considère Ore, le problème de l'immersion dans un corps.

⁽⁴⁾ P. DUBREIL, *L'indépendance linéaire dans un module sur un anneau non nécessairement commutatif* (*Bull. Sc. Math.*, t. 67, 1943, p. 1-18).

⁽⁵⁾ Cf. chap. II, § 5, p. 86.

Remarque ⁽¹⁾. — Un *groupoïde* S ayant un élément-unité bilatère e et vérifiant la condition Z , est un *demi-groupe*. Prenons, en effet, $b = s' = e$, $s = b'$ et posons $as = a'$, $t = b't'$; les relations (1) , $(1')$ $(1'')$ sont vérifiées; nous avons donc l'égalité (2) , qui s'écrit

$$a(st') = (as)t',$$

où a , s , t' sont arbitraires.

Dans un semi-groupe abélien, la condition Z de Malcev est vérifiée d'elle-même : $(1')$ et $(1'')$ donnent, en effet,

$$as.bt = a's'.b't',$$

d'où

$$at.bs = a't'.b's',$$

et, par conséquent,

$$at = a't'.$$

Nous allons voir que, tout comme la commutativité que d'ailleurs elle généralise, la *régularité à droite* de S ⁽²⁾ entraîne la condition Z de Malcev. A cet effet, nous utiliserons la propriété suivante :

LEMME. — Si, dans un demi-groupe S régulier à droite, on a

$$bs = b's' \quad \text{et} \quad bt = b't',$$

tout couple d'éléments m , n vérifiant .

$$sm = tn,$$

vérifie également

$$s'm = t'n.$$

On a, en effet,

$$b's'm = bsm = btn = b't'n,$$

d'où l'égalité à démontrer en utilisant la règle de simplification à gauche.

Cela posé, les relations (1) , $(1')$, $(1'')$ entraînent

$$atn = asm = a's'm = a't'n$$

et, par conséquent (2) , en utilisant cette fois la règle de simplification à droite : la condition Z est donc bien vérifiée.

⁽¹⁾ Communiquée par D. Tamari.

⁽²⁾ Rappelons que la régularité à droite de S signifie : 1° que la *règle de simplification* est valable dans S ; 2° que deux éléments s , t quelconques de S ont un multiple commun à droite $sm = tn$, autrement dit, S est *réversible à gauche*.

Or, l'hypothèse de la régularité à droite du demi-groupe S apparaît précisément si l'on particularise, avec O . Ore, le problème général d'immersion, en imposant à tout élément ξ du groupe G d'admettre au moins une représentation de la forme

$$\xi = ab^{-1}, \quad \text{avec } a \text{ et } b \in S$$

(condition $\mathcal{C}$). Si un tel groupe G existe, le semi-groupe S doit être régulier à droite, car si nous considérons deux éléments s et $s' \in S$ et l'élément $\xi = s^{-1}s' \in G$, nous avons

$$s^{-1}s' = r'r^{-1}, \quad \text{c'est-à-dire } sr' = s'r, \quad \text{avec } r \text{ et } r' \in S.$$

THÉOREME 1. — *Tout demi-groupe S régulier à droite est contenu dans un groupe G qui, en outre, vérifie la condition $\mathcal{C}$.*

Pour établir cette proposition il suffit, d'après une remarque déjà faite (chap. III, § 8, p. 131), de construire un groupe G_1 contenant un semi-groupe S_1 isomorphe à S et vérifiant la condition $\mathcal{C}$.

Considérons, sous le nom de *fractions à droite*, les couples a/b (« a sur b ») d'éléments de S : a est appelé *numérateur*, b *dénominateur*, et posons les règles de calcul suivantes. Soient a/b , a'/b' deux fractions à droite; il existe deux éléments s , $s' \in S$ tels que l'on ait

$$(3) \quad bs = b's'.$$

Nous dirons que, dans l'ensemble Δ des fractions à droite, a/b et a'/b' vérifient la relation $\mathcal{E}_\Delta$, et nous écrirons

$$a/b \mathcal{E}_\Delta a'/b',$$

si (3) entraîne

$$(3') \quad as = a's'.$$

La relation $\mathcal{E}_\Delta$ ainsi définie a un sens, puisque la condition Z est vérifiée et que, par conséquent, la propriété précédente est indépendante du choix des éléments s et s' vérifiant l'égalité (3).

La relation $\mathcal{E}_\Delta$ est évidemment *réflexive* et *symétrique*. Elle est aussi *transitive*, car si l'on a en outre

$$a'/b' \mathcal{E}_\Delta a''/b'',$$

on peut prendre (p. 85)

$$bs = b's' = b''s'' \quad (s, s' \text{ et } s'' \in S),$$

et l'on a

$$as = a's', \quad a's' = a''s'',$$

d'où

$$a/b \mathcal{E}_\Delta a''/b''.$$

La relation $\mathcal{E}_\Delta$ est donc une *équivalence*. On a, quel que soit $m \in S$,

$$am/bm \equiv a/b \quad (\mathcal{E}_\Delta).$$

Dans l'ensemble Δ des fractions à droite, nous dirons que la fraction a/b est *multipliable à droite* par c/d si l'on a $b \equiv c$, et nous poserons alors

$$a/b \cdot c/d = a/d.$$

On vérifie sans peine que cette définition fait de Δ un *groupoïde de Brandt* ⁽¹⁾ (chap. II, § 2, p. 70) à partir duquel nous allons obtenir le groupe cherché G_1 comme *ensemble-quotient* $\Delta/\mathcal{E}_\Delta$ ⁽²⁾.

Étant donné deux classes $\xi, \eta \in \Delta/\mathcal{E}_\Delta$, nous pouvons trouver une fraction $a/b \in \xi$ multipliable à droite par une fraction $b/c \in \eta$, et le produit

$$a/b \cdot b/c = a/c$$

appartient à une classe fixe. Soit, en effet,

$$p/q \in \xi, \quad u/v \in \eta;$$

il existe $m, n \in S$ tels que $qm = un = b$; posons $a = pm, c = vn$; nous avons bien

$$a/b \in \xi, \quad b/c \in \eta.$$

Soit, d'autre part,

$$a'/b' \in \xi, \quad \text{et} \quad b'/c' \in \eta;$$

l'égalité $cs = c's'$ entraîne $bs = b's'$ qui entraîne à son tour $as = a's'$; nous avons par conséquent,

$$a/c \equiv a'/c' \quad (\mathcal{E}_\Delta).$$

La classe fixe à laquelle appartient $a/c = pm/vn$ (où $qm = un$) est, par définition, le produit $\xi\eta$.

La multiplication ainsi définie dans $G_1 = \Delta/\mathcal{E}_\Delta$ est *associative*. On peut en effet trouver, dans trois classes données ξ, η, ζ , des fractions de

⁽¹⁾ Cette propriété, en elle-même très intéressante, n'intervient pas essentiellement dans ce qui suit.

⁽²⁾ On remarquera l'analogie de ce procédé avec celui qui fait passer du groupoïde de Brandt des segments au groupe additif des vecteurs libres.

la forme a/b , b/c , c/d ⁽¹⁾, et l'on a

$$c/d = a/b \cdot (b/c \cdot c/d) = (a/b \cdot b/c) \cdot c/d,$$

d'où

$$\xi \cdot \eta \zeta = \xi \eta \cdot \zeta.$$

Les fractions de la forme s/s constituent une classe ε modulo $\mathcal{E}_\Delta$: ε est visiblement élément-unité dans G_1 .

Une classe quelconque ξ , contenant la fraction a/b , a pour inverse la classe ξ' contenant la fraction b/a : $\xi' = \xi^{-1}$. G_1 est donc un groupe appelé *groupe des quotients à droite* du demi-groupe régulier S .

Les fractions de la forme as/s , où s est un élément arbitraire de S , constituent une classe α ; l'ensemble S_1 des classes de cette nature correspond biunivoquement à S par la loi $a \leftrightarrow \alpha$, puisque $as/s \equiv a's'/s' (\mathcal{E}_\Delta)$ entraîne $st = s't'$, $ast = a's't'$ (t et $t' \in S$), d'où $a = a'$. S_1 est un demi-groupe *isomorphe* à S , car la classe $\alpha\beta$ contient la fraction

$$(a \cdot bp)/bp \cdot (b \cdot p)/p = (ab \cdot p)/p$$

donc correspond à l'élément $ab \in S$.

Enfin, la condition $\mathcal{C}$ est vérifiée. Soit, en effet,

$$\xi \in G_1, \quad \text{avec } a/b \in \xi.$$

Nous avons, quel que soit $m \in S$,

$$am/m \in \alpha, \quad bm/m \in \beta, \quad \text{où } \alpha \in S_1, \quad \beta \in S_1,$$

d'où

$$m/bm \in \beta^{-1} \quad \text{et} \quad am/bm \in \alpha\beta^{-1},$$

donc

$$\xi = \alpha\beta^{-1}, \quad \text{avec } \alpha \text{ et } \beta \in S_1.$$

D'après le principe déjà rappelé (chap. III, § 8, p. 131), nous pouvons identifier les éléments de S_1 et ceux de S ; nous écrirons donc, confor-

⁽¹⁾ Soient, en effet, $p/q \in \xi$, $u/v \in \eta$, $x/y \in \zeta$. Nous avons

$$qm_1 = um'_1, \quad vm'_2 = xm''_2$$

et

$$m'_1 s_1 = m'_2 s_2.$$

Posons

$$\begin{aligned} a &= pm_1 s_1, & b &= qm_1 s_1 = um'_1 s_1, \\ c &= vm'_1 s_1 = vm'_2 s_2 = xm''_2 s_2, & d &= ym''_2 s_2. \end{aligned}$$

Nous avons bien

$$a/b \in \xi, \quad b/c \in \eta, \quad c/d \in \zeta.$$

mément à l'usage, les éléments du groupe G sous la forme

$$\xi = ab^{-1}, \quad \text{où } a \text{ et } b \in S.$$

Soient a, b, a', b' quatre éléments du semi-groupe S ; il existe deux éléments a'_1, b_1 tels que l'on ait

$$a'b_1 = ba'_1,$$

d'où, dans tout groupe extension de S ,

$$ab^{-1} \cdot a'b'^{-1} = a \cdot a'_1 b_1^{-1} \cdot b'^{-1} = aa'_1 \cdot (b'b_1)^{-1}.$$

Il en résulte d'abord que si, dans deux groupes G et G' , extensions de S et vérifiant la condition $\mathcal{C}$, on fait se correspondre les éléments qui admettent une même représentation ab^{-1} , cette correspondance est un *isomorphisme* (relatif par rapport à S). D'autre part, dans un groupe G_0 extension *quelconque* de S , les éléments de la forme ab^{-1} (a et $b \in S$) forment un sous-groupe G vérifiant la condition $\mathcal{C}$: *le groupe des quotients à droite, défini à un isomorphisme relatif près, est donc le plus petit groupe extension de S .*

Généralisation. — Considérons maintenant un *demi-groupe* D et supposons qu'il existe un sous-ensemble S de D vérifiant les conditions suivantes :

- I. S est *multiplicativement fermé*.
- II. Tout élément de S est *simplifiable* dans D à gauche et à droite.
- III. Si b et $b' \in S$, il existe au moins un couple d'éléments s et $s' \in S$ tels que $bs = b's'$.
- IV. Si $s \in S$ et $t \in D$, il existe au moins un couple d'éléments $m \in D$ et $n \in S$ tels que $sm = tn$.

D'après I, II, III, S est un *D-semi-groupe régulier à droite*; les conditions III et IV sont vérifiées trivialement si D est abélien.

THÉOREME 2. — *Moyennant les hypothèses I-IV, on peut définir dans l'ensemble-produit $\Delta = D \times S$ une équivalence $\mathcal{E}_\Delta$, et dans l'ensemble-quotient $\mathcal{Q} = \Delta / \mathcal{E}_\Delta$ une multiplication, de façon que $\mathcal{Q}$ soit un demi-groupe où tout élément de S possède un inverse : $\mathcal{Q}$ est à la fois extension du demi-groupe donné D et du groupe des quotients à droite, G , du semi-groupe régulier S . Tout élément de $\mathcal{Q}$ est de la forme ab^{-1} , où $a \in D$ et $b \in S$ (condition $\mathcal{C}$ généralisée).*

Pour établir ce théorème, nous commencerons par deux remarques qui généralisent le lemme de la page 268 et la condition Z de Malcev.

Les égalités

$$bs = b's', \quad bt = b't', \quad sm = tn$$

(entre éléments de D) entraînent, dès que b' est simplifiable à gauche,

$$s'm = t'n,$$

puisque

$$b's'm = bsm = btn = b't'n.$$

Les égalités

$$as = a's', \quad bs = b's', \quad bt = b't'$$

entraînent, dès que $s \in S$ et que b' est simplifiable à gauche,

$$at = a't'$$

(condition Z généralisée). Il existe, en effet, d'après IV, $m \in D$ et $n \in S$ tels que $sm = tn$, et nous avons aussi $s'm = t'n$, d'où

$$atn = asm = a's'm = a't'n$$

et l'égalité à établir en résulte, puisque n est simplifiable à droite, d'après II.

Soit $\Delta = D \times S$ l'ensemble des couples ou fractions à droite a/b ($a \in D$, $b \in S$). Si nous considérons deux telles fractions a/b , a'/b' , il existe d'après III au moins un couple d'éléments s et $s' \in S$ vérifiant l'égalité $bs = b's'$. Si l'on a aussi $as = a's'$, nous poserons

$$a/b \mathcal{E}_\Delta a'/b'.$$

Cette propriété est, d'après II et la condition Z, indépendante du choix de s et s' (vérifiant $bs = b's'$) : c'est donc une relation parfaitement définie dans Δ , évidemment réflexive et symétrique et, de plus, transitive (démonstration comme plus haut, p. 269), par conséquent une équivalence. On a

$$am/bm \equiv a/b \quad (\mathcal{E}_\Delta) \quad \text{pour tout } m \in S.$$

Dans l'ensemble-quotient $\mathcal{O} = \Delta/\mathcal{E}_\Delta$, nous conserverons pour la multiplication la même définition formelle que précédemment, mais il n'y a pas lieu de considérer des fractions multipliables. Soient ξ , η deux éléments de $\mathcal{O}$, représentés par les fractions p/q et u/v (q et $v \in S$) : il existe, d'après IV, $m \in D$ et $n \in S$ tels que

$$qm = un.$$

La classe à laquelle appartient la fraction pm/vn ne dépend que de ξ et η : c'est par définition le produit $\xi\eta$. Remplaçons d'abord, en effet, p/q par $p'/q' \in \xi$, et soit

$$q'm' = un' \quad (m' \in D, n' \in S),$$

montrons que

$$p'm'/vn' \equiv pm/vn \quad (\mathcal{E}_\Delta).$$

On a, d'une part,

$$ps = p's' \quad \text{et} \quad qs = q's', \quad \text{avec} \quad s \text{ et } s' \in S,$$

et, d'autre part, d'après III, $nt = n't'$, avec t et $t' \in S$, d'où

$$vn.t = vn'.t',$$

puis

$$qmt = unt = un't' = q'm't'.$$

En appliquant la condition Z, il vient

$$pm.t = p'm'.t',$$

d'où l'équivalence à établir.

Remplaçons, de même, u/v par $u'/v' \in \eta$ et soit $qm_1 = u'n_1$ ($n_1 \in S$). On a par hypothèse

$$us_1 = u's'_1 \quad \text{et} \quad vs_1 = v's'_1 \quad \text{avec} \quad s_1 \text{ et } s'_1 \in S.$$

Comme vn et $v'n_1 \in S$, on a, d'après III,

$$vnt_1 = v'n_1t'_1, \quad \text{avec} \quad t_1 \text{ et } t'_1 \in S.$$

La condition Z donne

$$unt_1 = u'n_1t'_1 \quad \text{et, par conséquent,} \quad qmt_1 = qm_1t'_1,$$

donc, d'après II, $mt_1 = m_1t'_1$, puis

$$pm.t_1 = pm_1.t'_1,$$

d'où l'équivalence à établir,

$$pm/vn \equiv pm_1/v'n_1 \quad (\mathcal{E}_\Delta).$$

Remarque. — Les dénominateurs décrivant seulement S , alors que les numérateurs décrivent D , il n'y avait pas lieu, ici, de considérer les fractions multipliables. Cependant, lorsqu'on est dans le cas particulier $u = q \in S$, on a $m = n$ et la fraction p/v , équivalente à pm/vn , appartient à la classe-produit $\xi\eta$. De même, si l'on a $qh = u$ ($h \in D$), l'égalité $qm = un$, où $q \in S$, entraîne, d'après II, $m = hn$; la fraction pm/vn s'écrit donc phn/vn , et la fraction équivalente ph/v appartient à $\xi\eta$.

La multiplication ainsi définie dans $\mathcal{O}$ est *associative*. Soient, en effet, $\xi, \eta, \zeta \in \mathcal{O}$ et $p/q, u/v, x/y$ des fractions représentant respectivement les classes ξ, η, ζ . On a, d'après IV,

$$qm = un \quad (n \in S) \quad \text{et} \quad vn.r = xs \quad (s \in S),$$

d'où

$$pm/vn \in \xi\eta \quad \text{et} \quad pmr/ys \in \xi\eta.\zeta.$$

D'autre part,

$$un/vn \in \eta,$$

donc

$$unr/ys \in \eta\zeta$$

et, par suite,

$$pmr/ys \in \xi.\eta\zeta,$$

donc

$$\xi\eta.\zeta = \xi.\eta\zeta.$$

$\mathcal{O}$ est donc bien un *demi-groupe*.

Considérons une classe $\alpha \in \mathcal{O}$ représentée par une fraction de la forme as/s ($a \in D, s \in S$). Pour qu'une fraction b/s' ($s' \in S$) appartienne à cette classe α , il faut et il suffit que l'on ait

$$ss_1 = s's'_1 \quad \text{et} \quad ass_1 = bs'_1, \quad \text{avec} \quad s_1, s'_1 \in S,$$

donc

$$as's'_1 = bs'_1,$$

c'est-à-dire

$$b = as'.$$

La classe α se compose donc des fractions as/s , où s décrit S . Soit D_1 l'ensemble des classes de cette forme : les éléments $\alpha, \dots$ de D_1 correspondent biunivoquement aux éléments $a, \dots$ de D . Cette correspondance est un *isomorphisme*; soit, en effet,

$$as/s \in \alpha, \quad bt/t \in \beta \quad (s, t \in S);$$

nous avons, d'après IV,

$$sm = bt.n \quad (n \in S)$$

et la classe $\alpha\beta$ est celle qui contient la fraction $as.m/tn$; or, celle-ci s'écrit $ab.tn/tn$ (où $tn \in S$) : $\alpha\beta$ appartient donc à D_1 et est bien l'image de ab . Nous avons

$$D \simeq D_1$$

et, par conséquent, $\mathcal{O}$ est une extension de D .

D'autre part, $\mathcal{O}$ contient le groupe G des quotients à droite de S , ensemble des classes représentables par des fractions de la forme r/s , où $r \in S$ (et $s \in S$). On vérifie immédiatement que l'élément-unité ε de G , représenté par les fractions s/s , est élément-unité bilatère de $\mathcal{O}$.

Un élément quelconque de $\mathcal{O}$, représenté par la fraction a/b , peut être regardé comme le produit des éléments $a \in D$ et $b^{-1} \in G$ représentés par les fractions a/s et s/b ($s \in S$), ce qui généralise la condition $\mathcal{C}$. On voit comme plus haut (p. 272), mais en utilisant cette fois l'hypothèse IV, que le demi-groupe $\mathcal{O}$ possédant les propriétés envisagées, est défini à un isomorphisme relatif près.

Parmi les hypothèses faites sur S , I et II sont seules symétriques. Désignons par III' et IV' les conditions symétriques de III et IV. Si un semi-groupe $S \subseteq D$ vérifie les hypothèses I, II, III' et IV', on peut, d'une façon analogue, définir dans l'ensemble $\Gamma = S \times D$ des fractions à gauche $v \backslash u$ (« v sous u », $v \in S$, $u \in D$), une équivalence $\mathcal{E}_\Gamma$ en posant

$$v \backslash u \mathcal{E}_\Gamma v' \backslash u' \quad \text{si } sv = s'v' \text{ (} s \text{ et } s' \in S \text{)} \quad \text{entraîne} \quad su = s'u'.$$

Pour définir dans l'ensemble quotient $\mathcal{O}^* = \Gamma / \mathcal{E}_\Gamma$ une multiplication associative, il suffit de remarquer que, si $v \backslash u$ et $s \backslash r$ sont deux fractions à gauche et si, d'après IV', $nu = ms$ ($n \in S$), la fraction $nv \backslash mr$ appartient à une classe fixe. Dans le demi-groupe $\mathcal{O}^*$, extension de D , ainsi construit, chaque élément de S possède un inverse, et tout élément de $\mathcal{O}^*$ est de la forme $v^{-1}u$, où $v \in S$, $u \in D^{(1)}$.

Si maintenant les hypothèses I, II, III et III', IV et IV' sont vérifiées simultanément, les demi-groupes $\mathcal{O}$ et $\mathcal{O}^*$, définis respectivement à partir des fractions à droite et des fractions à gauche, sont isomorphes. La démonstration de cette propriété repose sur la notion suivante. Nous dirons qu'une fraction à droite a/b et une fraction à gauche $v \backslash u$ sont homologues et nous écrirons

$$v \backslash u \doteq a/b,$$

si l'on a $va = ub$.

LEMME. — Pour que deux fractions à droite a/b , a'/b' soient homologues d'une même fraction à gauche, il faut et il suffit qu'elles soient équivalentes modulo $\mathcal{E}_\Delta$.

(1) Les démonstrations sont symétriques de celles qui ont été données plus haut.

Cette condition est *nécessaire*, car si l'on a

$$va = ub, \quad va' = ub',$$

l'égalité $bs = b's'$ entraîne

$$vas = ub s = ub's' = va's', \quad \text{où } v \in S,$$

d'où

$$as = a's'.$$

Elle est aussi *suffisante* puisque, si l'on a

$$bs = b's' \quad \text{et} \quad as = a's', \quad \text{où } s \text{ et } s' \in S,$$

l'égalité $va = ub$ entraîne

$$va's' = vas = ub s = ub's',$$

d'où

$$va' = ub'.$$

L'énoncé symétrique du précédent est, bien entendu, également valable. On voit aisément qu'en associant à chaque fraction à droite a/b l'ensemble des fractions à gauche homologues $v u$, on définit une application *semi-uniforme*; la relation $\mathcal{C} = \mathcal{C}$ correspondante (cf. chap. I, § 8) n'est autre que l'équivalence $\mathcal{E}_\Delta$.

En associant à chaque élément α^* de $\Gamma/\mathcal{E}_\Gamma$ l'élément α de $\Delta/\mathcal{E}_\Delta$ représenté par les fractions à droite homologues des fractions à gauche de la classe α^* , nous établissons entre $\mathcal{O}^*$ et $\mathcal{O}$ une *correspondance biunivoque*.

Cette correspondance est un *isomorphisme*. Soit, en effet,

$$\begin{aligned} a/b \in \alpha, & \quad v \setminus u \in \alpha^*, \\ a'/b' \in \beta, & \quad v' \setminus u' \in \beta^*, \end{aligned}$$

donc $va = ub$, $v'a' = u'b'$. Nous avons, d'après IV, $bm = a'n$ ($n \in S$), d'où $am/b'n \in \alpha\beta$; de même, d'après IV',

$$yu = xv' \quad (y \in S) \quad \text{et} \quad yv \setminus xu' \in \alpha^*\beta^*.$$

Les égalités

$$yv.am = yubm = xv'a'n = xu'.b'n$$

donnent

$$yv \setminus xu' = am/b'n$$

et, par conséquent,

$$(\alpha\beta)^* = \alpha^*\beta^*.$$

Il est donc légitime de parler du demi-groupe des quotients de D par rapport à S et, en particulier, du groupe des quotients d'un demi-groupe régulier.

Dans le cas abélien, les règles de calcul sur les fractions se transforment d'une façon remarquable et reprennent la forme usuelle. Utilisons, par exemple, la notation des fractions à droite : deux telles fractions a/b , a'/b' sont équivalentes modulo $\mathcal{E}_\Delta$ si toute égalité de la forme

$$(4) \quad bs = b's'$$

entraîne

$$(4') \quad as = a's'.$$

Or, (4) est vérifiée pour $s = b'$ et $s' = b$: deux fractions a/b , a'/b' sont donc équivalentes si et seulement si

$$(5) \quad ab' = ba'.$$

Le produit de deux éléments ξ , η de l'ensemble quotient $G = \Delta/\mathcal{E}_\Delta$, représentés respectivement par les fractions p/q et u/v , est la classe contenant la fraction pm/vn , où $qm = un$. Nous pouvons prendre ici $m = u$, $n = q$, d'où

$$pm/vn = pu/qv,$$

La fraction définissant la classe produit s'obtient donc en multipliant, dans les fractions données, les numérateurs entre eux et les dénominateurs entre eux.

La règle précédente peut être prise comme définition du produit de deux fractions quelconques,

$$(6) \quad p/q \cdot u/v = pu/qv.$$

La multiplication ainsi définie dans l'ensemble Δ des fractions à droite est associative et commutative comme celle de D . L'équivalence $\mathcal{E}_\Delta = \mathcal{E}$ est régulière par rapport à cette multiplication, car les relations

$$a/b \equiv a'/b' \quad (\mathcal{E})$$

et

$$a/b \cdot x/y \equiv a'/b' \cdot x/y, \quad \text{c'est-à-dire} \quad ax/by \equiv a'x/b'y \quad (\mathcal{E})$$

s'écrivent respectivement

$$(7) \quad ab' = ba',$$

$$(7') \quad axb'y = a'xby;$$

la multiplication étant commutative, la première de ces égalités entraîne la seconde, qui s'écrit encore, puisque $y (\in S)$ est simplifiable :

$$(7'') \quad ab'x = a'bx.$$

Si D est lui-même un semi-groupe, $(7'')$ entraîne (7) , et l'équivalence $(\mathcal{E})$ est simplifiable. Si l'on a, en outre, $D = S$, on retombe sur le cas traité au paragraphe 2 dans lequel on passe du semi-groupe donné S à son groupe des quotients Γ par les opérations suivantes :

1° Définition de la multiplication dans l'ensemble $\Delta = S^2$ des fractions, conformément à (6) ;

2° Passage de Δ au groupe homomorphe $G(= \Gamma)$ au moyen de l'équivalence $\mathcal{E}(= \mathbf{P})$ définie par (5) .

7. Immersion d'un anneau régulier dans un corps. Généralisation. — Considérons un anneau R et supposons qu'un sous-ensemble S de R possède, par rapport à la multiplication de R , les propriétés I, II, III, IV utilisées plus haut :

I. S est multiplicativement fermé.

II. Tout élément de S est simplifiable dans R à gauche et à droite.

III. Si b et $b' \in S$, il existe au moins un couple d'éléments s, s' de S tels que $bs = b's'$.

IV. Si $s \in S$ et $t \in R$, il existe au moins un couple d'éléments $m \in R$ et $n \in S$ tels que $sm = tn$.

Remarques. — 1. Les conditions III et IV sont vérifiées d'elles-mêmes quand R est un anneau commutatif.

2. La condition II exprime que S ne contient aucun diviseur de zéro de R . Si, en effet, a , par exemple, est diviseur de zéro à gauche, on a

$$ab = 0 = a \cdot 0, \quad \text{avec } b \neq 0$$

et a n'est pas simplifiable à gauche. Inversement, si a n'est pas diviseur de zéro, l'égalité $ax = ay$ s'écrit $a(x - y) = 0$ et entraîne $x = y$.

3. L'ensemble $\mathcal{N}_d$ des non-diviseurs de zéro à gauche est, visiblement, multiplicativement fermé ($\mathcal{N}_d$ est le noyau à droite du demi-groupe multiplicatif R , cf. § 4, p. 231). Dans le cas commutatif, cet ensemble $\mathcal{N}_d(= \mathcal{N})$ vérifie les conditions I, III et IV : c'est le plus grand ensemble S répondant à la question. En particulier, quand R est un domaine d'intégrité, on peut prendre $S = R - \{0\}$; le complément $S = R - \mathfrak{p}$ d'un idéal premier $\mathfrak{p}$ répond aussi à la question.

4. Lorsque R est un anneau régulier à droite, c'est-à-dire sans diviseurs de

zéro et tel qu'il existe, pour chaque couple d'éléments *non nuls* r, r' de R un multiple commun à droite

$$rm = r' m' \neq 0,$$

ce qui a lieu notamment quand R est un *domaine d'intégrité*, on peut satisfaire aux hypothèses I, II, III, IV en prenant $S = R - \{0\}$.

THÉOREME 1. — *Si un sous-ensemble S d'un anneau R vérifie les hypothèses I, II, III, IV, il existe un anneau K extension de R , dans lequel tout élément de S possède un inverse : K est appelé anneau des quotients à droite de R par rapport à S ; chaque élément de K est de la forme ab^{-1} , où $a \in R$, $b \in S$. Si R est régulier à droite et si $S = R - \{0\}$, K est un corps, appelé corps des quotients à droite de R (1).*

Pour établir ce théorème, remarquons que l'anneau R est, par rapport à la multiplication, un demi-groupe, ce qui nous permet de construire le demi-groupe multiplicatif $\mathcal{O}$ des quotients à droite de R par rapport à S : prenons $K = \mathcal{O}$. Pour faire de K un *anneau*, il ne reste qu'à y définir *l'addition*. Cette construction va résulter de deux conditions que nous devons évidemment imposer : le *principe de concordance*, et la *distributivité* de la multiplication par rapport à l'addition. Si deux éléments de K appartiennent à R , leur somme est, d'après le principe de concordance, la même que dans R .

Considérons ν éléments quelconques $\alpha_1, \dots, \alpha_\nu$ de K , représentés respectivement, par les fractions a_i/b_i

$$(1) \quad a_i/b_i \in \alpha_i \quad (b_i \in S, i = 1, \dots, \nu).$$

Nous avons des égalités de la forme (*cf.* p 85)

$$(2) \quad b_1 s_1 = \dots = b_\nu s_\nu = n,$$

où les s_i et, par conséquent, n appartiennent à S ; en posant $a_i s_i = c_i$, nous obtenons une représentation des α_i par des fractions c_i/n ayant toutes mêmes dénominateurs (« *réduction au même dénominateur* »). Les relations $\alpha_i = c_i n^{-1}$ dans K entraînent (2)

$$(1') \quad \alpha_i n = c_i \in R.$$

(1) Le *dénominateur* b d'une fraction a/b est alors assujéti seulement à la condition usuelle d'être *différent de zéro*. L'immersion d'un anneau régulier, en particulier d'un domaine d'intégrité, dans un corps a en Algèbre une importance fondamentale.

(2) Dans une extension K d'un anneau R , un élément μ tel que $\alpha_i \mu \in R$ ($\alpha_i \in K$, $i = 1, \dots, \nu$) est appelé *multiplicateur commun à droite* des α_i : les relations (1') expriment qu'on peut trouver un tel multiplicateur, $\mu = n$, dans le semi-groupe S .

Cela étant, si l'on peut définir dans K une addition par rapport à laquelle la multiplication est distributive, on aura *nécessairement*

$$\left(\sum_{i=1}^v \alpha_i\right)n = \left(\sum_{i=1}^v \alpha_i n\right) = \sum_{i=1}^v c_i \in R.$$

La somme $\sum_{i=1}^v \alpha_i$ ne peut donc être que l'élément de K représenté par la fraction $\left(\sum_{i=1}^v c_i\right)/n$,

Nous pouvons effectivement définir la somme $\sum_{i=1}^v \alpha_i$ comme la classe contenant la fraction $\left(\sum_{i=1}^v c_i\right)/n$, car cette classe est indépendante du choix des éléments n et c_i vérifiant les relations (1'). Si, en effet, n' et c'_i vérifient ces mêmes relations, il existe deux éléments p, p' de S tels que

$$np = n'p', \quad c_i p = c'_i p',$$

d'où, puisque la multiplication dans R est distributive par rapport à l'addition

$$\left(\sum_{i=1}^v c_i\right)p = \left(\sum_{i=1}^v c'_i\right)p'$$

et, par conséquent,

$$\left(\sum_{i=1}^v c_i\right)/n \equiv \left(\sum_{i=1}^v c'_i\right)/n' \quad (\mathcal{E}_\Delta).$$

Cette définition est conforme au principe de concordance.

De plus, il est clair que l'addition dans K est *associative* et *commutative* comme dans R ; K possède un élément zéro, $\mathbf{O}$, représenté par les fractions équivalentes o/s ($o \in R, s \in S$). Les éléments $\alpha = ab^{-1}$ et $\alpha' = (-a)b^{-1}$ sont *opposés* : K est donc un groupe abélien par rapport à l'addition. Quel que soit $\alpha \in K$, on a $\alpha \mathbf{O} = \mathbf{O} \alpha = \mathbf{O}$.

Pour montrer que K est un anneau, il ne nous reste plus qu'à établir dans toute sa généralité la *distributivité* de la multiplication par rapport à l'addition. Soient donc α, α', β trois éléments de K , avec

$$a/b \in \alpha, \quad a'/b \in \alpha', \quad r/s \in \beta,$$

d'où

$$(a + a')/b \in \alpha + \alpha'.$$

Il existe $m \in R$ et $n \in S$ tels que $bm = rn$; il en résulte

$$(a + a')m/sn = (am + a'm)/sn \in (\alpha + \alpha')\beta$$

et

$$am/sn \in \alpha\beta, \quad a'm/sn \in \alpha'\beta,$$

d'où

$$(am + a'm)/sn \in \alpha\beta + \alpha'\beta;$$

nous avons donc bien

$$(\alpha + \alpha')\beta = \alpha\beta + \alpha'\beta.$$

Nous avons aussi des égalités de la forme

$$st = au, \quad st' = a'u', \quad \text{avec } u \text{ et } u' \in S,$$

puis $uv = u'v' = y$, où v, v' et, par conséquent, y appartiennent à S ; d'où, en posant $tv = x$, $t'v' = x'$,

$$sx = ay, \quad sx' = a'y, \quad s(x + x') = (a + a')y.$$

il en résulte

$$r(x + x')/by = (rx + rx')/by \in \beta(\alpha + \alpha')$$

et

$$rx/by \in \beta\alpha, \quad rx'/by \in \beta\alpha, \quad \text{d'où } (rx + rx')/by \in \beta\alpha + \beta\alpha',$$

et, par conséquent,

$$\beta(\alpha + \alpha') = \beta\alpha + \beta\alpha',$$

ce qu'il fallait démontrer.

Enfin, l'anneau K est défini à un *isomorphisme relatif* près, non seulement par rapport à la multiplication, mais aussi par rapport à l'addition, puisqu'on a, dans K , $ab^{-1} + a'b^{-1} = (a + a')b^{-1}$.

Si R est *régulier à droite* et si $S = R - \{0\}$, $K - \{0\}$ est le *groupe* G des quotients à droite de S , ensemble des classes représentables par les fractions s'/s , où s et $s' \in S$. K est donc un *corps*, extension de l'anneau R . Ce résultat contient comme cas particulier celui qui a été établi, pour un domaine d'intégrité au paragraphe 3 (p. 228).

On définit de même l'anneau des quotients à gauche K^* d'un anneau R par rapport à un sous-ensemble S vérifiant les conditions I, II, III', et IV'.

Si S vérifie simultanément les conditions I, II, III et III'; IV et IV', les anneaux K et K^* sont isomorphes non seulement par rapport à la multiplication, mais aussi par rapport à l'addition. Soit, en effet,

$$\begin{aligned} \alpha &= ab^{-1} \in K, & \alpha^* &= v^{-1}u \in K^* \\ \beta &= a'b^{-1} \in K, & \beta^* &= v^{-1}u' \in K^* \end{aligned} \quad (b \text{ et } v \in S),$$

avec $va = ub$, $va' = u'b$. Nous avons, dans K ,

$$\alpha + \beta = (a + a')b^{-1},$$

dans K^*

$$\alpha^* + \beta^* = v^{-1}(u + u')$$

et l'égalité $v(a + a') = (u + u')b$ entraîne bien

$$(\alpha + \beta)^* = \alpha^* + \beta^*.$$

Enfin, si R est un anneau commutatif, l'addition dans l'anneau des quotients K de R par rapport à un semi-groupe $S \subseteq R$ reprend la forme usuelle. Si $a/b \in \alpha$, et $a'/b' \in \beta$, nous pouvons prendre (cf. p. 000.),

$$n = bb', \quad c = ab', \quad c' = a'b,$$

d'où

$$(ab' + ba')/bb' \in \alpha + \beta.$$

Dans ce cas abélien, le théorème 1 prend la forme suivante :

THÉOREME. 1'. — *A tout semi-groupe multiplicatif S contenu dans un anneau commutatif R et tel que tout élément de S soit simplifiable dans R , correspond un anneau de quotients K , extension de R , dans lequel tout élément de S a un inverse ⁽¹⁾. En particulier, l'ensemble T des éléments de R non diviseurs de zéro est multiplicativement fermé, et tout élément de T est évidemment simplifiable : T est donc un semi-groupe; pour $S = T$, nous obtenons un anneau de quotients Q en quelque sorte maximum appelé anneau de quotients total de R (« Gesamtquotientenring ») ⁽²⁾. Si R est un domaine d'intégrité, il suffit que S ne contienne pas zéro et soit multiplicativement fermé : ces deux conditions sont vérifiées notamment quand S est l'ensemble des éléments de R qui n'appartiennent pas à un idéal premier $\mathfrak{p}$: $S = R - \mathfrak{p}$ ⁽³⁾. En prenant $S = R - (0)$, on retrouve que tout domaine d'intégrité peut être plongé dans un corps, son corps des quotients.*

Exercice. — Dans un anneau commutatif R pouvant posséder de véritables diviseurs de zéro, on considère un semi-groupe multiplicatif S (en particulier, R pourra être un domaine d'intégrité, et S le complément $R - \mathfrak{p}$ d'un idéal

⁽¹⁾ Cf. H. GRELL, *Beziehungen zwischen Idealen verschiedener Ringe* (Math. Ann., t. 97, 1927, p. 499).

⁽²⁾ Cf. W. KRULL, *Idealtheorie* (Ergebn. der Math., IV, 3, 1935, p. 18 et 19); B. L. VAN DER WAERDEN, *On Hilbert's Function...* (Proc. Koninklijke Akad. van Wetensch., Amsterdam, t. 31, 1928, p. 760).

⁽³⁾ Voir note p. 199.

premier $\mathfrak{p}$). Soit K l'anneau de quotients $A \times S / \mathcal{E}$ obtenu au moyen des fractions a/s ($a \in A, s \in S$).

1° A tout idéal $\mathfrak{m}'$ de l'anneau K , on associe l'ensemble $\mathfrak{m}$ des numérateurs α des fractions représentant un élément α de $\mathfrak{m}'$. Montrer que $\mathfrak{m}$ est un idéal dans A .

2° L'inclusion stricte $\mathfrak{m}'_1 \subset \mathfrak{m}'_2$ entraîne $\mathfrak{m}_1 \subset \mathfrak{m}_2$.

3° Si A est noethérien, K est noethérien aussi.

C. — CORPS ORDONNÉS.

8. Domaines ordonnés. Convergence. — Un domaine d'intégrité D de caractéristique nulle, en particulier un corps commutatif de caractéristique nulle, est dit *ordonné* s'il existe dans D une relation

$$\alpha > 0 \quad (\alpha \text{ positif})$$

ayant les deux propriétés suivantes :

1° Pour tout élément $\alpha \in D$, on a

$$\text{soit } \alpha > 0, \quad \text{soit } \alpha = 0, \quad \text{soit } -\alpha > 0$$

(dans ce dernier cas, on écrit encore $\alpha < 0$, « α négatif »).

2° Les relations $\alpha > 0, \beta > 0$ entraînent $\alpha + \beta > 0$ et $\alpha\beta > 0$ ⁽¹⁾.

Par exemple, si l'on donne, dans l'anneau $\mathbb{C}$ des entiers, la signification usuelle à la relation $\alpha > 0$, $\mathbb{C}$ est un domaine d'intégrité ordonné.

Les propriétés 1° et 2° permettent de définir dans D une *relation d'ordre*, au sens des ensembles ordonnés (cf. chap. I, § 4, p. 17 et § 9, p. 36), en posant ⁽²⁾

$$\alpha > \beta \quad \text{si} \quad \alpha - \beta > 0.$$

Un domaine d'intégrité ordonné est donc un ensemble ordonné, et les

(1) Cette deuxième propriété ne peut évidemment pas appartenir à un anneau de caractéristique non nulle, ni à un anneau possédant de véritables diviseurs de zéro. La notion de *corps ordonné* a été introduite par E. Artin et O. Schreier, dans le Mémoire intitulé *Algebraische Konstruktion reeller Körper* (*Abh. math. Sem.*, Hambourg, t. V, p. 86).

(2) Seule, la première partie de la condition 2° intervient pour établir que cette relation est une relation d'ordre. Un domaine d'intégrité ordonné est donc quelque chose de plus qu'un domaine d'intégrité pourvu d'une relation d'ordre. D'ailleurs, dans l'anneau $\mathbb{C}$ des entiers, la relation $\alpha < \beta$ (au sens usuel) est bien une relation d'ordre, mais les égalités $\alpha < 0, \beta < 0$ n'entraînent pas $\alpha\beta < 0$, : *par rapport à cette relation*, $\mathbb{C}$ n'est donc pas un domaine d'intégrité ordonné.

notions de majorant, minorant, borne supérieure ou inférieure y peuvent être utilisées.

Si α et β sont deux éléments quelconques de D , on a

$$(1) \quad (-\alpha)\beta = -(\alpha\beta).$$

Par suite, le produit d'un élément négatif par un élément positif est négatif; le produit de deux éléments négatifs est positif. En particulier, *dans un domaine d'intégrité ou dans un corps ordonné, tout carré est positif ou nul, toute somme de carrés est positive ou nulle et l'égalité*

$$\alpha_1^2 + \dots + \alpha_n^2 = 0$$

exige

$$\alpha_i = 0 \quad (i = 1, 2, \dots, n).$$

En particulier, l'élément-unité $e = e^2$ est nécessairement positif.

Les inégalités

$$\alpha > \beta \quad \text{et} \quad \alpha + \lambda > \beta + \lambda$$

sont équivalentes quel que soit $\lambda \in D$. Les inégalités

$$\alpha > \beta \quad \text{et} \quad \alpha\lambda > \beta\lambda$$

sont équivalentes si λ est positif.

Soit K le corps des quotients d'un domaine d'intégrité ordonné D . *Il existe une manière et une seule d'ordonner le corps K de façon à respecter l'ordre de D .* Supposons, en effet, K ordonné, et soit $\alpha = \frac{a}{b}$ un élément quelconque de K . Les éléments α et $ab^2 = ab$ sont positifs, négatifs, ou nuls, en même temps l'un que l'autre; la relation $\alpha > 0$ dans K doit donc être définie par la condition $ab > 0$ dans D . Inversement cette définition est, en premier lieu, indépendante du choix de la fraction $\frac{a}{b}$ qui représente α . D'autre part, les éléments positifs sont ceux qui peuvent être représentés par des fractions dont les deux termes sont positifs : il en résulte immédiatement que $\alpha > 0$, $\beta > 0$ entraînent $\alpha + \beta > 0$ et $\alpha\beta > 0$.

En particulier, *le corps des nombres rationnels est un corps ordonné.* Pour que $\sigma = \frac{a}{b}$ soit supérieur à $\sigma' = \frac{a'}{b'}$ ($b > 0$, $b' > 0$), il faut et il suffit que l'on ait

$$ab' > ba'.$$

A tout élément α d'un domaine d'intégrité ordonné D , nous asso-

cierons un élément positif ou nul du même domaine, appelé *valeur absolue* de α , désigné par $|\alpha|$ et défini par les relations

$$\begin{aligned} |\alpha| &= \alpha, & \text{si } \alpha \geq 0, \\ |\alpha| &= -\alpha, & \text{si } \alpha < 0. \end{aligned}$$

On a les propriétés suivantes :

1° Deux éléments opposés ont même valeur absolue.

2° Quels que soient α et β , on a

$$|\alpha\beta| = |\alpha| \cdot |\beta|.$$

Cette relation est évidente si α et β sont positifs ou nuls. D'autre part, elle subsiste d'après (1), si l'on y remplace un élément, α par exemple, par l'élément opposé.

3° Si $\alpha < \lambda < \beta$, on a

$$|\lambda| < \text{Max}(|\alpha|, |\beta|),$$

le second membre désignant le plus grand des deux nombres $|\alpha|$, $|\beta|$, ou leur valeur commune s'ils sont égaux. Cette inégalité est immédiate si α est positif ou nul, ou si β est négatif ou nul. Supposons donc $\alpha < 0 < \beta$. Si λ est positif ou nul, par exemple on a

$$|\lambda| < |\beta| \leq \text{Max}(|\alpha|, |\beta|),$$

et l'inégalité est encore établie.

Si L est un sous-ensemble borné de D , nous avons des inégalités de la forme

$$\alpha \leq \lambda \leq \beta \quad \text{pour tout } \lambda \in L,$$

d'où, d'après ce qui précède,

$$|\lambda| \leq \mu \quad \text{pour tout } \lambda \in L,$$

avec $\mu = \text{Max}(|\alpha|, |\beta|)$. Cette dernière inégalité, qui entraîne inversement

$$-\mu \leq \lambda \leq \mu \quad \text{pour tout } \lambda \in L,$$

équivalant à la propriété : L est borné.

4° Quels que soient α et β , on a

$$|\alpha + \beta| \leq |\alpha| + |\beta|.$$

L'égalité a lieu si α et β sont de même signe (c'est-à-dire tous deux

positifs ou tous deux négatifs), ou encore si l'un des deux est nul. Si l'on a, par exemple,

$$\alpha > 0, \quad \beta < 0,$$

on en déduit

$$\beta < \alpha + \beta < \alpha$$

et la propriété 3° donne

$$|\alpha + \beta| < \text{Max}(|\alpha|, |\beta|) < |\alpha| + |\beta|.$$

5° Si l'on a l'inégalité

$$|\beta - \alpha| < |\beta|,$$

les deux éléments α et β sont de même signe. Dans le cas contraire, en effet, β et $\alpha' = -\alpha$ seraient de même signe et l'on aurait

$$|\beta - \alpha| = |\beta + \alpha'| = |\beta| + |\alpha'| \geq |\beta|.$$

Considérons, dans un corps ordonné K , l'ensemble A des éléments $n = ne$, où e désigne l'élément-unité et n un entier naturel. Si cet ensemble A n'est pas majoré, c'est-à-dire si, quel que soit l'élément α de K , il existe un entier naturel n tel que l'on ait

$$n > \alpha,$$

le corps ordonné K est dit *archimédien*.

Le corps Γ des nombres rationnels, par exemple, est archimédien.

Si K est un corps ordonné archimédien, on constate, en appliquant la propriété précédente à l'élément $-\alpha$, qu'il existe aussi un entier relatif m tel que l'on ait

$$m < \alpha$$

Par suite, on peut toujours trouver un entier relatif a tel que l'on ait

$$a \leq \alpha < a + 1.$$

En remplaçant α par $q\alpha$, où q est un entier positif donné, nous voyons qu'il existe un entier relatif p tel que l'on ait

$$\frac{p}{q} \leq \alpha < \frac{p+1}{q}.$$

De même, α étant un élément positif de K , il existe un entier n supérieur à α^{-1} , ce qui entraîne

$$\frac{1}{n} < \alpha.$$

Si, au contraire, dans le corps ordonné K , l'ensemble $A = \{ne\}$ est majoré K est dit *non archimédien*. Un corps ordonné non archimédien est, d'après cette définition, caractérisé par l'existence d'éléments *infiniment grands*, c'est-à-dire d'éléments α vérifiant

$$|\alpha| > n \quad \text{pour tout nombre naturel } n.$$

De même, un élément β est *infiniment petit* si l'on a

$$0 < |\beta| < \frac{1}{n} \quad \text{pour tout nombre naturel } n.$$

L'inverse d'un élément infiniment grand est infiniment petit et inversement ⁽¹⁾.

Étant donné un anneau commutatif $\mathcal{R}$, soit

$$A = \{a_n\} = \{a_1, a_2, \dots, a_n, \dots\}$$

une suite dans $\mathcal{R}$, c'est-à-dire une suite dont les éléments a_i appartiennent à $\mathcal{R}$. Deux suites $\{a_n\}$, $\{a'_n\}$ sont *distinctes* dès que l'égalité $a_n = a'_n$ n'a pas lieu pour toutes les valeurs de n . On appelle *somme*, *différence* et *produit* des deux suites

$$A = \{a_n\}, \quad B = \{b_n\},$$

les suites respectives

$$A + B = \{a_n + b_n\}, \quad A - B = \{a_n - b_n\}, \quad AB = \{a_n b_n\}.$$

L'addition et la multiplication des suites ayant les mêmes propriétés d'associativité, de commutativité, et de distributivité que celles des éléments de $\mathcal{R}$, l'ensemble des suites dans $\mathcal{R}$ est un *anneau commutatif* $\mathcal{S}$, dont l'élément zéro est la suite

$$O = \{0, 0, \dots, 0, \dots\}$$

⁽¹⁾ On peut aisément, en anticipant un peu, donner un exemple simple de corps ordonné non archimédien. Convenons de dire qu'un polynôme

$$f(x) = a_0 x^r + a_1 x^{r-1} + \dots + a_r \quad (a_i \in \Gamma, a_0 \neq 0)$$

à coefficients rationnels est *positif* si le coefficient a_0 de la plus haute puissance de x est un nombre positif. La somme et le produit de deux polynômes positifs sont bien des polynômes positifs. Par cette convention, le corps des fractions rationnelles $\frac{f(x)}{g(x)}$, à coefficients rationnels, se trouve lui-même ordonné :

$$\frac{f(x)}{g(x)} = \frac{a_0 x^r + \dots}{b_0 x^s + \dots} > 0 \quad \text{si } f(x)g(x) > 0,$$

c'est-à-dire si $a_0 b_0 > 0$. Ce corps ordonné K est *non archimédien*, car $x, x^2, \dots, x^n, \dots$ sont des infiniment grands.

et qui a en même temps que $\mathcal{R}$ un élément unité, qui est la suite

$$\mathbf{1} = \{1, 1, \dots, 1, \dots\}.$$

Dans un *corps ordonné* K , une suite $\{a_n\}$ est *monotone croissante* si

$$a_n < a_{n+1} \quad \text{quel que soit } n,$$

monotone non décroissante si

$$a_n \leq a_{n+1} \quad \text{quel que soit } n.$$

Une suite dans un *corps ordonné* K est *bornée* si l'ensemble de ses éléments est borné. Il suffit pour cela qu'il existe un élément positif L de K et un nombre naturel N tel que l'inégalité.

$$n > N \quad \text{entraîne} \quad |a_n| < L,$$

car la réunion de l'ensemble fini, donc borné $\{a_1, a_2, a_N\}$ et de l'ensemble borné $\{a_{N+1}, \dots, a_n, \dots\}$ est un ensemble borné.

La somme ou la différence, et le produit de deux suites bornées étant des suites bornées, l'ensemble des suites bornées est un sous-anneau $\mathcal{B}$ de l'anneau $\mathcal{S}$ des suites dont les éléments appartiennent à K .

Par définition, la suite

$$A = \{a_n\} = \{a_1, a_2, \dots, a_n, \dots\}$$

converge, dans le corps ordonné K , *vers la limite* a s'il existe un élément a de K ayant la propriété suivante :

A tout élément ε *positif* de K correspond un nombre naturel N tel que l'inégalité $n > N$ entraîne l'inégalité

$$|a - a_n| < \varepsilon.$$

A cette définition se rattachent les propriétés suivantes :

1° Une même suite ne peut pas converger vers deux limites distinctes a et b . En effet, dans le cas contraire, en désignant par ε un élément positif de K moindre que $\frac{|b-a|}{2}$, on aurait, pour n assez grand,

$$|b-a| \leq |b-a_n| + |a-a_n| < 2\varepsilon < |b-a|,$$

ce qui est absurde.

2° Toute suite convergente $A = \{a_n\}$ est bornée.

En effet, si a est la limite de la suite convergente A , nous avons

$$a - \varepsilon < a_n < a + \varepsilon \quad \text{pour } n > N,$$

d'où

$$|a_n| < |a| + \varepsilon \quad \text{pour } n > N.$$

3° Toute suite $\{a_{n_i}, a_{n_2}, \dots, a_{n_k}, \dots\}$, où les nombres naturels n_i vont en croissant, extraite d'une suite convergente $\{a_1, a_2, \dots, a_n, \dots\}$, est elle-même convergente et admet la même limite ⁽¹⁾.

4° Une suite dans laquelle tous les éléments sont, à partir d'un certain rang, égaux à un même élément a , est convergente et admet pour limite a .

Appelons *suites nulles* les suites dans K qui convergent vers zéro, *suites nulles triviales* les suites dont les éléments sont, à partir d'un certain rang, égaux à zéro.

5° *a. La somme de deux suites nulles est une suite nulle* (immédiat).

COROLLAIRE (limite d'une somme). — Si les suites $A = \{a_n\}$, $B = \{b_n\}$ convergent respectivement vers les limites a et b , la suite $A + B$ est convergente et admet la limite $a + b$. En effet, la suite $\{(a_n + b_n) - (a + b)\}$, somme des deux suites nulles $\{a_n - a\}$ et $\{b_n - b\}$, est elle-même une suite nulle.

b. Le produit d'une suite nulle par une suite bornée est une suite nulle (immédiat).

COROLLAIRE (limite d'un produit). — Si les suites $A = \{a_n\}$ et $B = \{b_n\}$ convergent respectivement vers les limites a et b , la suite $AB = \{a_n b_n\}$ est convergente et a pour limite ab . On a, en effet,

$$ab - a_n b_n = a(b - b_n) + b_n(a - a_n)$$

et chacune des suites $\{a(b - b_n)\}$, $\{b_n(a - a_n)\}$ est le produit d'une suite nulle par une suite bornée.

Pour les suites nulles triviales, nous avons de même les propriétés suivantes :

c. La somme de deux suites nulles triviales est une suite nulle triviale.

d. Le produit d'une suite nulle triviale par une suite quelconque est une suite nulle triviale.

⁽¹⁾ Cette propriété et la suivante, prises comme axiomes, ont servi de point de départ à certaines généralisations de la notion de convergence. Cf. MAURICE FRÉCHET, *Les Espaces abstraits*, Paris, 1928, p. 164

En réunissant les propriétés précédentes et en désignant par $\mathfrak{Z}_0$ l'ensemble des suites nulles triviales, par $\mathfrak{Z}$ l'ensemble des suites nulles, par $\mathcal{C}$ l'ensemble des suites convergentes, nous voyons que $\mathfrak{Z}_0$ est un sous-anneau de $\mathfrak{Z}$, que $\mathfrak{Z}$ est un sous-anneau de $\mathcal{C}$, que $\mathcal{C}$ est un sous-anneau de l'anneau $\mathcal{B}$ des suites bornées, lui-même sous-anneau de l'anneau $\mathfrak{S}$ de toutes les suites :

$$\mathfrak{Z}_0 \subseteq \mathfrak{Z} \subset \mathcal{C} \subset \mathcal{B} \subseteq \mathfrak{S}.$$

Nous avons même obtenu des propriétés un peu plus fortes : par rapport à la multiplication, $\mathfrak{Z}_0$ est un sous-groupeïde permis dans $\mathfrak{S}$, et $\mathfrak{Z}$ un sous-groupeïde permis dans $\mathcal{B}$: donc $\mathfrak{Z}_0$ est un *idéal* dans $\mathfrak{S}$ et, par conséquent, dans $\mathcal{B}$, $\mathcal{C}$ et $\mathfrak{Z}$; $\mathfrak{Z}$ est un *idéal* dans $\mathcal{B}$, donc aussi dans $\mathcal{C}$.

$\mathfrak{Z}$ n'est pas un idéal dans $\mathfrak{S}$: dans le corps des nombres rationnels, par exemple, le produit de la suite nulle $\left\{\frac{1}{n}\right\}$, par la suite non bornée $\{n\}$ n'est pas une suite nulle.

$\mathfrak{Z}$ est un *idéal premier* dans l'anneau $\mathcal{C}$ des suites convergentes, d'après le théorème sur la limite d'un produit et puisque le corps K ne contient pas de diviseur de zéro. Dans l'anneau $\mathcal{B}$ des suites bornées, l'idéal $\mathfrak{Z}$ n'est pas premier, car les deux suites bornées non nulles $\{1, 0, 1, 0, \dots\}$ et $\{0, 1, 0, 1, \dots\}$, par exemple, ont pour produit une suite nulle.

On voit clairement que les propriétés d'être un idéal ou un idéal premier ne sont pas, pour un ensemble, des propriétés intrinsèques, mais qu'elles dépendent à la fois de cet ensemble et de l'anneau dans lequel on le considère.

Exemples et remarques. — Si K est un *corps ordonné archimédien*, la suite $\left\{\frac{1}{n}\right\}$ est une suite nulle, non triviale : on a donc $\mathfrak{Z}_0 \subset \mathfrak{Z}$; la suite $\{n\}$ est une suite non bornée : $\mathcal{B} \subset \mathfrak{S}$.

Connaissant une suite nulle, on peut en former d'autres à l'aide de la remarque suivante, connue sous le nom de « *théorème de comparaison* », et valable dans tout corps ordonné (archimédien ou non).

Étant donné une suite nulle $\{u_n\}$ à éléments positifs et une suite $\{v_n\}$ telle qu'on ait, à partir d'un certain rang,

$$|v_n| < u_n,$$

la suite $\{v_n\}$ est une suite nulle (démonstration immédiate).

Par exemple, dans un corps ordonné archimédien, la suite $\left\{\frac{1}{n^2+1}\right\}$ est une suite nulle.

Remarquons enfin que, dans un corps ordonné non archimédien, la suite $\left\{\frac{1}{n}\right\}$ ne tend pas vers zéro puisqu'on a quel que soit n ,

$$\frac{1}{n} > |\alpha|;$$

où α est un infiniment petit quelconque.

Exercices. — 1. Dans un corps ordonné, l'égalité $a^m = b^m$ entraîne, si a et b sont positifs, $a = b$; si a et b sont quelconques $|a| = |b|$. Les seuls éléments tels que $x^m = \pm 1$ sont $x = +1$ et $x = -1$.

2. Dans un corps ordonné K , on considère l'ensemble E des éléments positifs x qui vérifient l'inégalité

$$x^m \leq a,$$

où a est un élément positif donné et m un nombre naturel. Montrer :

1° que l'ensemble E n'est pas vide ;

2° que la condition nécessaire et suffisante pour que l'ensemble E admette une borne supérieure l dans K est qu'il existe un élément α de K vérifiant l'égalité

$$\alpha^m = a$$

et que, cette condition étant remplie, on a

$$l = \alpha.$$

(L'élément α est, par définition, la racine $m^{\text{ième}}$ positive de a .)

3. Si la suite $A = \{a_n\}$ converge vers la limite a , et si l'on a, quel que soit n ,

$$a_n < b \quad \text{ou} \quad a_n \leq b,$$

la limite a vérifie l'inégalité

$$a \leq b.$$

9. Corps ordonnés complets. Nombres réels. — La définition d'une suite convergente fait intervenir la limite de cette suite. On ne peut donc, au moyen de cette définition, montrer qu'une suite est convergente qu'à condition d'avoir déterminé d'abord la valeur de sa limite, ce qui n'est pas toujours possible, surtout quand la suite est définie par des conditions générales. Il y a donc lieu de chercher à caractériser les suites convergentes par une propriété indépendante de leur limite. C'est ce qu'a fait Cauchy, en établissant, pour certains corps ordonnés, le critère de convergence qui porte son nom, et qui repose sur la notion de suite fondamentale.

Définition. — Dans un corps ordonné K , une suite $A = \{a_n\}$ est

fondamentale si, à tout élément positif ε de K , on peut associer un entier naturel N tel que les inégalités

$$p > N \quad q > N \quad \text{entraînent} \quad |a_p - a_q| < \varepsilon.$$

Toute suite convergente dans K γ est fondamentale. — Si, en effet, la suite $A = \{a_n\}$ converge vers a , l'inégalité

$$|a_p - a_q| \leq |a - a_p| + |a - a_q|$$

montre immédiatement que cette suite est fondamentale. En particulier, une suite dont les éléments sont tous égaux à partir d'un certain rang, est fondamentale.

Inversement, dans tout corps ordonné K , les suites fondamentales ont les propriétés suivantes, qui les rapprochent des suites convergentes.

1° *L'ensemble $\mathfrak{F}$ des suites fondamentales est un sous-anneau de l'anneau $\mathcal{B}$ des suites bornées.*

Toute suite fondamentale $A = \{a_n\}$ est *bornée*, puisque, avec les notations utilisées dans la définition, l'inégalité $n > N$ entraîne

$$a_{N+1} - \varepsilon < a_n < a_{N+1} + \varepsilon,$$

d'où

$$|a_n| < |a_{N+1}| + \varepsilon = L,$$

où L est un élément fixe.

Si $A = \{a_n\}$ et $B = \{b_n\}$ sont deux suites fondamentales, leur somme $A + B$ en est une également, d'après l'inégalité

$$|(a_p + b_p) - (a_q + b_q)| \leq |a_p - a_q| + |b_p - b_q|.$$

De même pour leur différence $A - B$.

Enfin, le produit AB est également une suite fondamentale. Nous avons, en effet,

$$|a_p b_p - a_q b_q| \leq |a_p| |b_p - b_q| + |b_q| |a_p - a_q|.$$

Comme toute suite fondamentale est bornée, nous avons, quand p et q dépassent un certain entier,

$$|a_p| < L, \quad |b_q| < L'.$$

Comme les suites $\{Lb_n\}$ et $\{L'a_n\}$ sont évidemment fondamentales, la propriété est établie.

2° *Il est impossible d'extraire d'une suite fondamentale $A = \{a_n\}$*

deux suites partielles $A' = \{a_{i_1}, a_{i_2}, \dots\}$, $A'' = \{a_{j_1}, a_{j_2}, \dots\}$ qui convergent vers des limites a' et a'' différentes ⁽¹⁾.

Si la chose était possible, on pourrait, en effet, ε étant un élément positif donné de K , trouver des indices i et j arbitrairement grands tels que

$$|a_i - a'| < \varepsilon, \quad |a_j - a''| < \varepsilon,$$

d'où

$$|a' - a''| < |a_i - a_j| + 2\varepsilon$$

et, en prenant $\varepsilon < \frac{1}{3} |a' - a''|$,

$$|a_i - a_j| > \varepsilon,$$

ce qui est en contradiction avec le fait que la suite A est fondamentale.

Malgré ces analogies, il n'y pas identité, dans n'importe quel corps ordonné K , entre suites fondamentales et suites convergentes. En particulier, comme nous allons le voir, *une suite fondamentale dans le corps Γ des nombres rationnels n'y est pas nécessairement convergente* ⁽²⁾.

On définit en Arithmétique élémentaire un procédé [extraction de la racine carrée approchée ⁽³⁾] permettant de calculer une suite de nombres rationnels $x_1, x_2, \dots; x_n, \dots$ tels que l'on ait

$$|x_n^2 - 2| < \varepsilon_n,$$

où la suite $\{\varepsilon_n\}$ est une suite nulle dans Γ , donnée une fois pour toutes. La suite $\{x_n\}$ est *fondamentale*. En effet, la suite $\{x_n^2\}$ converge, dans Γ , vers la limite 2, donc est fondamentale. Or, nous avons

$$|x_p - x_q| = \frac{|x_p^2 - x_q^2|}{|x_p + x_q|}.$$

et il est clair que, pour p et q assez grands, on a

$$x_p > 1, \quad x_q > 1,$$

donc

$$|x_p - x_q| < \frac{1}{2} |x_p^2 - x_q^2|.$$

(1) Pour les suites convergentes, cette propriété résulte immédiatement de l'énoncé 3, p. 290.

(2) Connue, au fond, dès l'Antiquité, ce fait mathématique est d'une grande importance : imposant la distinction entre grandeurs commensurables et grandeurs incommensurables, c'est lui qui confère aux Mathématiques leur caractère de sciences exactes.

(3) Voir, par exemple, JULES TANNERY, *Arithmétique*, p. 269 (Paris, Armand Colin, 1894).

Bien que fondamentale, la suite $\{x_n\}$ n'est pas convergente dans Γ , car, si elle l'était, sa limite serait un nombre rationnel de carré égal à 2 : on sait qu'un tel nombre n'existe pas.

De ce qui précède, résulte que la diagonale d'un carré dont on prend le côté pour unité de longueur, n'a pas pour mesure un nombre rationnel.

Considérons encore, dans Γ , la suite $\{u_n\}$ définie par

$$u_n = 1 + \frac{1}{1} + \frac{1}{2!} + \dots + \frac{1}{n!}.$$

D'après l'inégalité classique ⁽¹⁾ :

$$0 < u_q - u_p < \frac{1}{p \cdot p!} \quad (p < q),$$

cette suite est fondamentale. Si elle convergeait dans Γ , nous aurions, en désignant par l sa limite,

$$0 < l - u_p \leq \frac{1}{p \cdot p!}.$$

En prenant $p = 2$ dans cette inégalité, on voit que l ne peut pas être un entier rationnel. Si maintenant nous avons

$$l = \frac{m}{n} \quad (n > 1),$$

il en résulterait, en prenant $p = n$,

$$0 < \frac{m}{n} - \left(1 + \frac{1}{1} + \dots + \frac{1}{n!}\right) \leq \frac{1}{n \cdot n!}.$$

Or, cette double inégalité est absurde, puisque, multipliée par $n!$, elle exprime qu'un entier positif est inférieur ou égal à $\frac{1}{n}$.

Ces remarques nous conduisent à distinguer, parmi les corps ordonnés, ceux dans lesquels *toute suite fondamentale est convergente* (*critère de Cauchy*) : ces corps sont dits *complets*.

L'existence de corps ordonnés complets résulte de la proposition suivante, que nous allons maintenant établir.

⁽¹⁾ On a

$$\begin{aligned} u_q - u_p &= \frac{1}{(p+1)!} + \dots + \frac{1}{q!} < \frac{1}{(p+1)!} \left[1 + \frac{1}{p+1} + \dots + \frac{1}{(p+1)^{q-p-1}} \right] \\ &< \frac{1}{(p+1)!} \frac{1}{1 - \frac{1}{p+1}} = \frac{1}{p \cdot p!}. \end{aligned}$$

Tout corps ordonné incomplet K admet une extension Σ_K qui est un corps ordonné complet.

Le procédé général que nous allons indiquer pour construire Σ_K à partir de K , si on l'applique au corps $\mathbf{I}$ des nombres rationnels, fournit un corps complet $\mathbf{P}$ qui est, par définition, le *corps des nombres réels*.

Le corps cherché Σ_K s'obtient comme ensemble-quotient $\mathcal{F}/R$ de l'anneau $\mathcal{F}$ des suites fondamentales dans K par une équivalence R dont la définition est au fond immédiate : les suites fondamentales dans K seront convergentes dans Σ_K ; deux telles suites doivent donc être regardées comme équivalentes lorsqu'elles convergent vers la même limite, c'est-à-dire lorsque leur différence est une suite nulle. Cette dernière propriété ayant un sens dans K , nous définissons l'équivalence R en posant

$$A \equiv B(R) \quad \text{si} \quad A - B \in \mathcal{Z},$$

ou $\mathcal{Z}$ désigne l'ensemble des suites nulles (dans K). Cette relation R est bien réflexive, symétrique et transitive.

LEMME 1. — *L'équivalence R est régulière.*

Elle est évidemment régulière par rapport à l'addition. Elle est aussi régulière par rapport à la multiplication, puisque toute suite fondamentale X est bornée et que le produit $(A - B)X$ d'une suite nulle par une suite bornée est une suite nulle.

Ce lemme entraîne que l'ensemble-quotient $\mathcal{F}/R$ est un *anneau*, homomorphe à $\mathcal{F}$, qui admet comme élément-zéro la classe $\mathcal{Z}$ des suites nulles : $\mathcal{Z} = \mathbf{0}$, représentée par la suite $\{0, 0, \dots, 0, \dots\}$, et comme élément-unité $\mathbf{1}$ la classe contenant la suite-unité $\{1, 1, \dots, 1, \dots\}$. Nous allons montrer que l'anneau $\mathcal{F}/R$ est un *corps* au moyen de la proposition suivante, qui exprime que, dans un corps ordonné K , toute suite fondamentale *non nulle* est, en valeur absolue, bornée inférieurement.

LEMME 2. — *Si $A = \{a_n\}$ est une suite fondamentale non nulle, il existe un élément $r > 0$ de K et un entier naturel N tels que l'inégalité*

$$n > N \quad \text{entraîne} \quad |a_n| > r (> 0).$$

Sinon, en effet, quels que soient l'élément $r > 0$ de K et le nombre naturel N , il existerait au moins un indice $k > N$ tel que l'on ait

$$|a_k| \leq r;$$

r ayant été fixé, nous pouvons supposer, puisque A est une suite fondamentale, N choisi assez grand pour que les inégalités

$$p > N, \quad q > N \quad \text{entraînent} \quad |a_p - a_q| < r.$$

Il en résulterait, pour tout indice n supérieur à N ,

$$|a_n| \leq |a_n - a_k| + |a_k| < 2r.$$

Comme r est arbitraire, cela exprime que A est une suite nulle, contrairement à l'hypothèse.

THÉOREME. — *L'anneau $\mathcal{F}/R$ est un corps, Σ .*

Il suffit de montrer que toute classe α non nulle admet un inverse α^{-1} .

Soit $A = \{a_n\}$ une suite de la classe α : cette suite n'étant pas nulle, il existe d'après le lemme 2 un entier N_1 et un élément $r > 0$ de K tels que l'on ait

$$|a_n| > r \quad \text{pour} \quad n > N_1.$$

Considérons la suite B définie par

$$b_1 = 1, \quad \dots, \quad b_{N_1} = 1, \quad b_{N_1+1} = \frac{1}{a_{N_1+1}}, \quad \dots, \quad b_n = \frac{1}{a_n}, \quad \dots$$

Elle est fondamentale, car nous avons, pour $p > N_1, q > N_1$:

$$|b_p - b_q| = \frac{|a_p - a_q|}{|a_p a_q|} < \frac{|a_p - a_q|}{r^2}$$

et le numérateur peut être rendu inférieur à $r^2 \varepsilon$, à la seule condition de choisir p et q supérieurs à un certain entier.

Le produit des suites fondamentales A, B est la suite

$$a_1, \quad \dots, \quad a_N, \quad 1, \quad 1, \quad \dots, \quad 1, \quad \dots$$

qui appartient à la classe **1**. La classe β à laquelle appartient la suite B est donc l'inverse de la classe α , $\beta = \alpha^{-1}$.

Soit K' l'ensemble des classes **a** qui contiennent les suites fondamentales $\{a, a, \dots, a, \dots\}$ dont tous les éléments sont égaux. La correspondance

$$a \longleftrightarrow a$$

entre K' et K est un *isomorphisme* et, par conséquent, K' est un sous-corps de $\Sigma = \mathcal{F}/R$ isomorphe à K . Le corps Σ est donc bien une *extension* de K .

Si nous prenons comme corps K le corps Γ des nombres rationnels, Σ est, par définition, le corps des *nombres réels* ⁽¹⁾.

Il nous reste à montrer que le corps Σ est un corps *ordonné complet*, ce qui nous permettra d'écrire : $\Sigma = \Sigma_K$.

LEMME 3. — Si $A = \{a_n\}$ est une suite fondamentale non nulle, tous ses termes, à partir d'un certain rang, ont le même signe.

Il existe, d'après le lemme 2, un entier N_1 et un élément positif $r \in K$ tels que l'on ait

$$|a_i| > r > 0, \quad \text{dès que } i > N_1.$$

D'autre part, on a

$$|a_p - a_q| < r, \quad \text{dès que } p > N_2, \quad q > N_2,$$

d'où, pour $n > N = \max(N_1, N_2)$,

$$|a_n - a_{n+1}| < r < |a_{n+1}|$$

et, par conséquent, a_n a le même signe que a_{n+1} .

Une suite non nulle est dite *positive* si tous ses termes sont positifs à partir d'un certain rang, *négative* si tous ses termes sont, à partir d'un certain rang, négatifs. D'après ce qui précède, il n'y a pas d'autre possibilité pour une suite fondamentale non nulle.

Si $A = \{a_n\}$ est une suite positive, toute suite équivalente $B = \{b_n\}$ est également positive. A partir d'un certain rang N_1 , en effet, les a_n sont tous minorés par un certain élément positif r du corps K . D'autre part, la différence $a_n - b_n$ est, en valeur absolue, inférieure à r dès que n dépasse une certaine valeur N_2 . On a, par suite, $b_n > 0$ pour $n > N = \max(N_1, N_2)$.

Cela posé, un élément α non nul de Σ est par définition *positif* si l'une quelconque des suites fondamentales de la classe α est positive,

(1) Cette définition des nombres réels est due à Cantor; celle qui utilise les coupures est due à Dedekind, mais, pour y simplifier la définition des opérations sur les nombres réels, on l'expose souvent en faisant des emprunts, plus ou moins apparents, à la définition de Cantor (« coupures généralisées »). Une définition, remarquable par sa simplicité, proposée récemment par M. Lesieur (voir un article à paraître dans la *Revue de Mathématiques spéciales*, 1954) repose sur le principe suivant. Soit $\mathcal{S}$ l'ensemble des parties de l'ensemble Γ_+ des nombres rationnels positifs qui sont majorées (dans Γ_+); soit α la relation d'équivalence défini dans $\mathcal{S}$ par :

$A \alpha B$ si et seulement si A et B admettent les mêmes majorants (dans Γ_+).

L'ensemble-quotient $\alpha/\mathcal{S}$ est l'ensemble des nombres réels positifs ou nuls.

néglatif si l'une quelconque de ces suites est négative. Tout élément de Σ est ou nul, ou positif, ou négatif. Il est, d'autre part, évident que la somme et le produit de deux éléments positifs sont positifs, puisque cette propriété est vérifiée dans K et, par conséquent, dans $\mathcal{F}$. *Le corps Σ est donc un corps ordonné.* L'ordre relatif de deux éléments appartenant à K' est le même que celui des éléments correspondants dans K . Les corps K et K' sont donc, non seulement isomorphes, mais *semblables*. Suivant l'usage, nous ne ferons plus de distinction entre les éléments de K et ceux de K' .

Soient $A = \{a_n\}$, $B = \{b_n\}$ deux suites fondamentales. Si l'on a constamment à partir d'un certain rang $a_n \geq b_n$, il en résulte, pour les éléments α et β de Σ définis par ces suites, l'inégalité $\alpha \geq \beta$. Si l'on avait, en effet, $\alpha < \beta$, c'est-à-dire $\beta - \alpha > 0$, la suite $B - A$ serait positive, ce qui est contraire à l'hypothèse.

Soit α un élément positif de Σ , représenté par la suite fondamentale A . Cette suite étant bornée, il existe un élément r de K tel que l'on ait

$$(1) \quad r > \alpha.$$

Par conséquent, si K est archimédien, Σ l'est aussi, car on peut trouver un entier n tel que l'on ait

$$(0 < r) \alpha < r < n.$$

D'autre part (K étant quelconque), si nous écrivons l'inégalité (1) en prenant $\alpha = \frac{1}{\varepsilon}$, ou ε désigne un élément positif quelconque de Σ , nous voyons, en posant $s = \frac{1}{r}$, qu'il existe un élément s de K positif et inférieur à ε

$$0 < s < \varepsilon, \quad \text{où } s \in K.$$

Cela posé, étudions les propriétés de convergence dans le corps ordonné Σ , et montrons qu'il est complet. Soit α un élément de Σ , représenté par une suite fondamentale dans K : $A = \{a_n\}$, $a_n \in K$.

LEMME 4. — Dans Σ , la suite fondamentale A converge vers la limite α .

Soit ε un élément positif de Σ . Il existe dans K un élément s vérifiant la double inégalité

$$0 < s < \varepsilon.$$

D'autre part, il existe un entier N tel que les inégalités

$$n > N, \quad p > N \quad \text{entraînent} \quad a_p - s < a_n < a_p + s$$

En comparant la suite $A = \{a_1, a_2, \dots, a_n, \dots\}$ aux deux suites $\{a_p - s, a_p - s, \dots, a_p - s, \dots\}, \{a_p + s, a_p + s, \dots, a_p + s, \dots\}$ dont les éléments sont tous égaux respectivement à $a_p - s$ et à $a_p + s$, p restant fixe, il en résulte

$$a_p - s \leq \alpha \leq a_p + s, \quad \text{dès que } p > N,$$

d'où

$$|\alpha - a_p| < \varepsilon, \quad \text{dès que } p > N,$$

ce qui exprime que la suite A converge, dans Σ , vers la limite α .

Considérons maintenant les *suites fondamentales* dans Σ .

THÉORÈME DE CAUCHY. — *Dans le corps Σ , toute suite fondamentale $A = \{a_n\}$ est convergente. En d'autres termes, le corps ordonné Σ est complet*

$$\Sigma = \Sigma_K.$$

Pour démontrer ce théorème, supposons d'abord K *archimédien*, Σ est aussi archimédien. Désignons par $\{\varepsilon_n\}$ une suite nulle dans Σ , à éléments *positifs* ⁽¹⁾. D'après le lemme 4, chaque élément a_n de A est la limite d'une suite d'éléments de K et, par conséquent, nous pouvons trouver, pour chaque valeur de n un élément a_n de K tel que l'on ait

$$(2) \quad |a_n - a_n| < \varepsilon_n \quad (a_n \in K).$$

Cela étant, nous avons

$$|a_p - a_q| \leq |a_p - x_p| + |x_p - x_q| + |x_q - a_q| < \varepsilon_p + \varepsilon_q + |x_p - a_q|.$$

La suite $\{\varepsilon_n\}$ étant nulle et la suite $A = \{a_n\}$ étant fondamentale, le second membre est inférieur à un élément positif ε de Σ (ou, en particulier, de K), dès que p et q dépassent un certain entier N . Par conséquent, la suite $\{a_n\}$ est fondamentale dans K , donc admet dans Σ une limite α . D'après (2), α est aussi limite de la suite A .

Supposons maintenant Σ *non archimédien*. Le théorème est évident si la suite A a tous ses éléments égaux à partir d'un certain rang. Et s'il n'en est pas ainsi, on peut, en supprimant tout élément égal à celui qui le précède, extraire de la suite A une suite $\{\beta_i\}$, également fondamentale, et telle que l'on ait : $\beta_{i+1} - \beta_i \neq 0$. Dans ces conditions, la suite de terme général

$$\varepsilon_i = |\beta_{i+1} - \beta_i|$$

(1) On peut prendre, par exemple, $\varepsilon_n = \frac{1}{n}$. La suite $\{\varepsilon_n\}$ peut d'ailleurs s'obtenir à partir de n'importe quelle suite nulle non triviale en supprimant les termes nuls et en remplaçant les termes négatifs par leur valeur absolue

a tous ses éléments positifs et est une suite nulle : l'existence de la suite $\{\varepsilon_n\}$ est donc assurée, et la démonstration s'achève comme dans le cas archimédien.

Dans le cas où le corps Σ est *archimédien*, nous avons encore l'importante proposition suivante.

THÉOREME. — *Dans un corps ordonné, archimédien, complet, Σ , tout ensemble E qui possède un majorant admet une borne supérieure.*

Σ étant archimédien, il existe, pour chaque valeur de l'entier naturel n , un entier relatif k_n ayant les deux propriétés suivantes :

1° L'élément

$$c_n = \frac{k_n}{n}$$

est un majorant de E ;

2° L'élément

$$c_n - \frac{1}{n} = \frac{k_n - 1}{n}$$

n'est pas un majorant de E.

Si p et q sont deux nombres naturels différents, on a, d'après les propriétés précédentes,

$$c_p - \frac{1}{p} < c_q, \quad c_q - \frac{1}{q} < c_p,$$

d'où

$$|c_p - c_q| < \text{Max}\left(\frac{1}{p}, \frac{1}{q}\right),$$

et, par conséquent, la suite $\{c_n\}$ est fondamentale : soit γ sa limite dans Σ .

Dans Σ , γ est borne supérieure de l'ensemble E. En effet, il en est d'abord un majorant, car si a est un élément arbitraire de E, l'inégalité

$$a \leq c_n \quad \text{pour tout } n$$

entraîne

$$a \leq \gamma.$$

D'autre part, quel que soit l'élément positif $\varepsilon \in \Sigma$, $\gamma - \varepsilon$ n'est pas un majorant de E : en effet, la suite $\left\{c_n - \frac{1}{n}\right\}$ converge, comme $\{c_n\}$, vers γ , et nous pouvons trouver un entier n tel que l'on ait

$$\gamma - \varepsilon < c_n - \frac{1}{n}.$$

Or, par définition, $c_n - \frac{1}{n}$ n'est pas un majorant de E.

COROLLAIRE. — Dans un corps Σ ordonné, archimédien, complet, toute suite monotone non décroissante admettant un majorant est convergente.

Cette suite, en tant qu'ensemble, admet en effet une borne supérieure, et elle converge vers cette borne.

Des propositions analogues sont valables, dans un corps ordonné, archimédien, complet, pour les ensembles et les suites monotones non croissantes qui possèdent un minorant.

Enfin, les propriétés précédentes s'appliquent en particulier au corps $\mathbf{P}$ des nombres réels, extension ordonnée, archimédienne et complète du corps $\mathbf{I}$ des nombres rationnels ⁽¹⁾, ⁽²⁾.

Exercices. — 1. Tout élément positif a d'un corps ordonné, archimédien, complet admet dans ce corps une racine $m^{\text{ième}}$ positive.

2. Σ étant le corps complet construit à partir d'un corps ordonné K , il existe, entre deux éléments distincts α et β de Σ , un élément de K (et par conséquent une infinité).

10. Sous-corps et sur-corps. — Si un sous-ensemble k d'un corps K ⁽³⁾ est lui même un corps (par rapport à l'addition et à la multiplication de K), k est, par définition, un *sous-corps* de K ; K est un *sur-corps* ou une *extension* de k .

⁽¹⁾ On peut encore donner, comme application du théorème de la borne supérieure, une élégante démonstration d'un théorème classique sur les fonctions continues. Soit $y = f(x)$ une fonction définie dans un corps ordonné archimédien complet Σ et prenant ses valeurs dans un corps ordonné Σ' : la définition d'une fonction continue s'applique évidemment, et nous nous proposons de montrer que si $f(x)$ est continue pour $a \leq x \leq b$, et si l'on a $f(a) < 0$, $f(b) > 0$, il existe au moins un élément $c \in \Sigma$ et compris entre a et b tel que $f(c) = 0$.

L'ensemble $\mathcal{N}$ des éléments x compris entre a et b pour lesquels $f(x)$ est négatif, est majoré donc a une borne supérieure c : on a $c \leq b$.

Si $f(c)$ était négatif, on pourrait, en raison de la continuité, trouver $h > 0$ tel que $|f(c+h) - f(c)| < |f(c)|$, d'où $f(c+h) < 0$, et c ne serait pas majorant de $\mathcal{N}$.

Si $f(c)$ était positif, on pourrait trouver $r > 0$ tel que $0 < h < r$ entraîne $|f(c-h) - f(c)| < |f(c)|$, d'où $f(c-h) > 0$, c'est-à-dire $f(x) > 0$ dès que $x > c - r$: $c - r$ serait donc majorant de $\mathcal{N}$, ce qui est impossible, puisque c est borne supérieure.

On a donc $f(c) = 0$ et le théorème est démontré.

⁽²⁾ L'extension des corps ordonnés a été étudiée par J. P. SERRE, *Extensions des corps ordonnés* (C. R. Acad. Sc., t. 229, 1949, p. 576).

⁽³⁾ Parmi les propriétés qui vont être indiquées, les premières restent valables si K est un *corps gauche*. Lorsque l'hypothèse de la commutativité interviendra, nous le signalerons explicitement.

Pour cela, il faut et il suffit que k soit un *sous-groupe additif* de K , et que $k - \{0\}$ soit *sous-groupe multiplicatif* de $K - \{0\}$, donc que les relations $a \in k, b \in k$ entraînent $a - b \in k$ et, si $b \neq 0$, $ab^{-1} = \frac{a}{b} \in k$. Tout sous-corps k d'un corps K contient nécessairement l'élément zéro et l'élément-unité e de K , donc aussi le groupe cyclique additif (e) ; par suite, *tout sous-corps k de K a même caractéristique que K .*

Si K est un corps de caractéristique p , les éléments $n = ne$ du groupe cyclique (e) , ($n = 0, 1, \dots, p-1$), forment eux-mêmes un corps Π , isomorphe à $C/(p)$ ou C désigne l'anneau des entiers. Si K est un corps de caractéristique 0 , les éléments $n = ne$ (n entier relatif arbitraire) du même groupe cyclique, forment un anneau isomorphe à C , et leurs quotients forment un corps Π isomorphe au corps Γ des nombres rationnels. Le corps Π ainsi défini dans tous les cas n'a évidemment aucun sous-corps véritable : un corps ayant cette propriété est dit *premier*.

Si K_1 est un sous-corps de K_2 et K_2 un sous-corps de K_3 , K_1 est un sous-corps de K_3 .

L'intersection Δ d'un ensemble de sous-corps de K n'est jamais vide ($0 \in \Delta, e \in \Delta$) et est évidemment un sous-corps de K . En particulier, l'intersection Π' de *tous* les sous-corps de K est un sous-corps, qui, d'après sa définition, est *premier*. De plus, Π' coïncide nécessairement avec le sous-corps premier Π défini plus haut; si, en effet, le corps K admettait deux sous-corps premiers distincts Π et Π' , l'intersection $\Pi \cap \Pi'$ serait un véritable sous-corps de Π ou de Π' , ce qui est impossible. Nous avons ainsi la proposition suivante :

Tout corps K admet un sous-corps premier unique, isomorphe au corps des classes résiduelles $C/(p)$ si K est de caractéristique p , au corps Γ des nombres rationnels si K est de caractéristique nulle.

Étant donné, dans un corps K , un sous-corps k , et un sous-ensemble S , considérons le sous-corps Σ intersection de tous les sous-corps de K qui contiennent k et S : Σ , qui est le plus petit sous-corps de K contenant k et S , est désigné par la notation

$$\Sigma = k(S),$$

et l'on dit que Σ se déduit de k par *adjonction* de l'ensemble S . Si $S \subseteq k$, on a

$$k(S) = k.$$

Il peut arriver aussi que l'on ait

$$k(S) = K$$

(par exemple pour $S = K$ ou $K - k$).

Tout sous-corps de K contenant k et S contient chaque *expression rationnelle* en S par rapport à k , c'est-à-dire chaque élément de K se déduisant d'un nombre fini d'éléments de S par des additions, soustractions, multiplications et divisions ⁽¹⁾ portant sur ces éléments et des éléments de k (« opérations rationnelles »). Inversement, ces expressions rationnelles forment un sous-corps de K contenant k et S : par conséquent, ce sous-corps n'est autre que $k(S)$.

Lorsque l'ensemble S est fini, $S = \{\alpha_1, \alpha_2, \dots, \alpha_n\}$, on écrit

$$k(S) = k(\alpha_1, \alpha_2, \dots, \alpha_n).$$

Si $S = S_1 \cup S_2$, le corps $k(S)$ peut s'obtenir en formant d'abord le corps $k(S_1)$ puis en adjoignant à celui-ci l'ensemble S_2

$$k(S_1 \cup S_2) = k(S_1)(S_2).$$

En effet, le corps $k(S_1)(S_2)$ contient $k(S_1)$ et S_2 , donc k et $S_1 \cup S_2$, d'où

$$k(S_1 \cup S_2) \subseteq k(S_1)(S_2).$$

Inversement, $k(S_1 \cup S_2)$ contient k et S_1 , donc $k(S_1)$; et comme il contient également S_2 , nous avons

$$k(S_1 \cup S_2) \supseteq k(S_1)(S_2).$$

En particulier, on peut remplacer l'adjonction de n éléments $\alpha_1, \alpha_2, \dots, \alpha_n$ au corps k par n adjonctions successives d'un seul élément. Un corps $k(\alpha)$ obtenu en adjoignant un seul élément à k est appelé *extension simple* de k .

Il importe de remarquer que les sur-corps obtenus en adjoignant à k des sous-ensembles différents $S, S', S'', \dots$ de K peuvent très bien coïncider. Par exemple, si K est le corps $\mathbf{P}$ des nombres réels, et k le corps $\mathbf{F}$ des nombres rationnels, on a

$$\mathbf{F}(\sqrt{2}) = \mathbf{F}(-\sqrt{2}) = \mathbf{F}\left(\frac{1}{\sqrt{2}}\right).$$

Considérons une *extension simple* $k(\alpha)$ de k . Le corps $k(\alpha)$, ensemble

⁽¹⁾ Bien entendu, tout élément figurant en dénominateur est supposé différent de zéro.

des expressions rationnelles en α par rapport à k , comprend en particulier les *expressions rationnelles entières*, c'est-à-dire celles qui se déduisent de α et d'éléments de k par un nombre fini d'additions, de soustractions et de multiplications. Une telle expression peut toujours, *dans le cas commutatif*, se mettre sous la forme

$$(1) \quad \sum_{i=1}^n a_i \alpha^i = a_n \alpha^n + a_{n-1} \alpha^{n-1} + \dots + a_0, \quad \text{où } a_i \in k.$$

L'ensemble de ces éléments est un *anneau*, que l'on désigne souvent par $k[\alpha]$, et tout élément du corps $k(\alpha)$ peut se mettre sous la forme du quotient de deux éléments de cet anneau.

Cela posé, il y a lieu de distinguer les deux cas suivants, pour lesquels les règles de calcul dans le corps $k(\alpha)$ sont, comme nous le verrons plus loin (chap. VII, § 2, p. 368), bien différentes.

1° Une expression rationnelle entière (1) n'est nulle que si tous les a_i sont nuls : l'élément α est dit alors *transcendant* par rapport à k ; $k(\alpha)$ est appelé *extension transcendante simple* de k .

2° Il existe au moins une expression de la forme (1), avec des a non tous nuls, qui est égale à zéro : α est alors, par définition, un élément *algébrique* par rapport à k et $k(\alpha)$ est appelé *extension algébrique simple* de k . La relation

$$a_n \alpha^n + \dots + a_0 = 0, \quad a_i \in k \quad (a_n \neq 0),$$

est appelée *équation algébrique de degré n sur k* .

Prenons en particulier pour corps k le corps $\mathbf{I}$ des nombres rationnels, comme corps $\mathbf{K}$ le corps $\mathbf{P}$ des nombres réels : on appelle *nombres algébriques réels* les éléments de $\mathbf{P}$ qui sont algébriques par rapport à $\mathbf{I}$, *nombres transcendants* les nombres qui ne sont pas algébriques. Par exemple, $\sqrt{2}$ est un nombre algébrique, puisque l'on a $(\sqrt{2})^2 - 2 = 0$ (voir § 8, exerc. 2, et § 9, exerc. 1), tandis que les nombres π et

$$e = 1 + \frac{1}{1} - \dots + \frac{1}{n!} + \dots$$

sont transcendants ⁽¹⁾.

(1) La transcendance de e a été établie en 1873 par Hermite, celle de π par Lindemann. Voir, par exemple, pour les démonstrations, G. VALIRON, *Théorie des Fonctions* p. 104 (Paris, Masson, 1942). D'autre part, Liouville a indiqué un procédé simple pour former des nombres transcendants (*ibid.*, p. 15). Enfin, l'existence de nombres transcendants résulte encore des résultats fondamentaux de Cantor : l'ensemble des nombres algébriques est dénombrable, tandis que l'ensemble des nombres réels a la puissance du continu (voir Note V, à la fin du présent volume).

Nous étudierons d'une manière plus précise les extensions simples, transcendantes ou algébriques, lorsque nous aurons introduit la notion de *polynomes*. Cette notion nous permettra, d'autre part, de construire de telles extensions *à partir du corps* k , c'est-à-dire sans faire intervenir le sur-corps K dans lequel k et $k(\alpha)$ étaient ici plongés l'un et l'autre : nous obtiendrons, en particulier, une définition directe des nombres algébriques, indépendante de la notion de nombre réel.

Exercice. — Montrer que le nombre $\alpha = \sqrt{2} + \sqrt{3}$ est algébrique; former une équation algébrique de degré 4 à laquelle il satisfait. Montrer que toute puissance impaire de ce nombre est de la forme $a\sqrt{2} + b\sqrt{3}$, où a, b appartiennent au corps Γ des nombres rationnels. En déduire l'égalité

$$\Gamma(\sqrt{2}, \sqrt{3}) = \Gamma(\sqrt{2} + \sqrt{3}).$$



CHAPITRE VI.

ANNEAUX.

A. — FACTORISATION.

1. **Éléments premiers entre eux; semi-groupes cohérents; semi-groupes complets.** — Considérons un *semi-groupe abélien* S , avec *élément-unité* e : S sera souvent le demi-groupe multiplicatif des éléments non nuls d'un domaine d'intégrité $\mathfrak{O}$. Comme l'a souligné Emmy Noether ⁽¹⁾, la notion de nombres premiers entre eux se généralise de plusieurs façons différentes.

I. Nous dirons que a et b sont *sans diviseurs communs* (teilerfrei) s'ils n'ont pas d'autres diviseurs communs que des unités (il est clair que tout élément x est divisible par une unité ε car $x = \varepsilon \cdot \varepsilon^{-1}x$).

II. Nous dirons que b est *premier à* a (prim zu a) si, pour tout $x \in S$ tel que $a \mid bx$, on a $a \mid x$.

A priori, cette propriété II est dissymétrique, tandis que I est symétrique. Si b et b' sont premiers à a , leur produit bb' l'est aussi.

III. Dans le cas où S est le demi-groupe multiplicatif des éléments non nuls d'un domaine d'intégrité $\mathfrak{O}$, nous dirons que a et b sont *premiers entre eux* (teilerfremd) s'il existe, dans S , deux éléments u, v tels que l'on ait

$$ua + vb = e \quad (\text{relation de Bezout}).$$

La propriété II entraîne la propriété I : b étant premier à a , si a et b ont un diviseur commun c , on a :

$$a = a'c, \quad b = b'c, \quad \text{d'où} \quad ab' = a'b;$$

a divise donc $a'b$ et, par conséquent, a' ; a et a' sont associés, c est une unité.

(1) *Abstrakter Aufbau der Idealtheorie* (*Math. Ann.*, t. 96, 1927, p. 26).

La propriété III (si $S = \mathfrak{o} - \{0\}$) entraîne la propriété II (et, par conséquent, la propriété I). Soit, en effet, $a \mid bx$, c'est-à-dire $bx = ra$; on en tire, d'après III,

$$x = ex = a(ux + vr), \quad \text{donc} \quad a \mid x.$$

Remarque. — Si $\mathfrak{o}$ est l'anneau C des entiers, on sait (d'après la théorie élémentaire du plus grand commun diviseur) que les propriétés I, II, III sont équivalentes.

D'une façon générale, soient a et b deux éléments du semi-groupe S : si un de leurs diviseurs communs d est divisé par tout autre diviseur commun à a et b , d est appelé *plus grand commun diviseur* (p. g. c. d.) de a et b . Tout élément associé à d a la même propriété et, inversement, tous les p. g. c. d. de a et b , s'il en existe, sont associés deux à deux.

LEMME 1. — *Pour que d soit un p. g. c. d. de a et b , il faut que l'on ait*

$$a = a'd, \quad b = b'd$$

et que a' , b' , soient sans diviseurs communs.

Soit, en effet, $a' = a''r$, $b' = b''r$; le produit rd divise a et b , donc leur p. g. c. d. d ; cela exige que r soit une unité.

LEMME 2. — *Pour qu'un diviseur commun d de a et de b soit un p. g. c. d., il suffit que le quotient b' de b par d soit premier au quotient a' de a par d .*

Soit, en effet, c un diviseur commun de a et de b . Nous avons

$$a = a'd = a''c, \quad b = b'd = b''c,$$

d'où

$$b'a'' = a'b''$$

et, par conséquent, $a' \mid b'a''$. Si b' est premier à a' , nous aurons $a' \mid a''$ et, par suite, $c \mid d$.

Un semi-groupe S sera dit *cohérent* si la propriété I entraîne la propriété II et, par conséquent, lui est équivalente. D'après les lemmes, nous avons la proposition suivante :

THÉORÈME 1. — *Dans un semi-groupe cohérent S , pour qu'un diviseur commun d de $a = a'd$ et de $b = b'd$ soit un p. g. c. d. de a et b , il faut et il suffit que a' et b' soient sans diviseurs communs.*

Une autre propriété importante est la suivante :

THÉOREME 2. — *Dans un semi-groupe cohérent, tout élément premier est premier au sens strict ⁽¹⁾.*

Soit p un élément premier. Supposons que l'on ait $p \mid xy$ et $p \nmid x$; p et x sont sans diviseurs communs, x est donc premier à p : nous avons alors $p \mid y$, p est bien premier au sens strict.

COROLLAIRE. — *Dans un semi-groupe cohérent, la décomposition d'un élément en produit d'éléments premiers, si elle existe, est « unique » (c'est-à-dire, le nombre de facteurs premiers est déterminé, et les facteurs eux-mêmes le sont à des unités près).*

Il suffit de rapprocher le théorème 2 du théorème général d'unicité établi au chapitre IV (§ 14, B, th. 7, p. 218).

Dans un semi-groupe S , même cohérent, on n'est pas en mesure d'affirmer l'existence d'un p. g. c. d. pour un couple quelconque d'éléments a, b . Appelons *semi-groupe complet* ⁽²⁾ un semi-groupe abélien avec élément-unité dans lequel deux éléments a, b , ont toujours un p. g. c. d. Soit $\mathcal{R}$ la relation d'équivalence définie par $x \equiv y (\mathcal{R})$ si $x \mid y$ et $y \mid x$ (cf. chap. IV, § 14, B, p. 209). Dans l'holoïde $\bar{S} = S/\mathcal{R}$, dont les éléments $\bar{a}, \dots$ sont les idéaux principaux $\langle a \rangle, \dots$ ⁽³⁾, la relation-image de $a \mid b$ est la relation d'inclusion inversée $\langle a \rangle \supseteq \langle b \rangle$. Le fait que S est *complet*, autrement dit l'existence du p. g. c. d. dans S , signifie qu'il existe un idéal principal minimum $\langle d \rangle$ contenant à la fois $\langle a \rangle$ et $\langle b \rangle$, donc que l'ensemble des idéaux principaux, partiellement ordonné par inclusion, est un *demi-treillis*.

Dans un semi-groupe complet, deux éléments sans diviseurs communs ont pour p. g. c. d. l'élément-unité e et les unités $\varepsilon, \dots$.

THÉOREME 3. — *Dans un semi-groupe complet S , on a, quels que soient $a, b, r \in S$:*

$$(1) \quad \text{p. g. c. d.}(ra, rb) = r \text{ p. g. c. d.}(a, b).$$

⁽¹⁾ Cf. chap. IV, § 14, B, p. 214.

⁽²⁾ Pour les domaines d'intégrité, cette notion se trouve dans J. KÖNIG, *Einleitung in die allgemeine Theorie der algebraischen Grössen* (p. 13). Nous conservons ici cette dénomination bien qu'elle ne soit pas en accord avec l'emploi actuel du mot « complet » dans la Théorie des Treillis.

⁽³⁾ S et le demi-groupe des idéaux principaux sont isomorphes, et il est commode d'identifier $\bar{a}$ et $\langle a \rangle$.

L'élément r divise ra et rb , donc aussi tout p. g. c. d., d_1 , de ra et rb . Posons donc $d_1 = r d_2$; d_2 divise a , et de même divise b , donc d_2 divise tout p. g. c. d. d de a et b . Inversement, rd divise ra et rb , donc aussi $d_1 = r d_2$: par conséquent, d divise d_2 ; d_2 et d sont associés, d_2 est donc un p. g. c. d. de a et b et l'égalité $d_1 = r d_2$ s'écrit sous la forme (1).

COROLLAIRE. — *Tout semi-groupe complet S est cohérent.* Soient, en effet, a et b deux éléments sans diviseurs communs : nous avons $e = \text{p. g. c. d.}(a, b)$, d'où, quel que soit $x \in S$, $x = \text{p. g. c. d.}(ax, bx)$. Si donc $a | bx$, comme $a | ax$ nous aurons $a | x$; b est donc premier à a (de même, a est premier à b).

Un domaine d'intégrité σ est dit *cohérent (complet)* si le semi-groupe multiplicatif $S = \sigma - \{0\}$ est *cohérent (complet)*. L'anneau $\mathbb{C}$ des entiers a ces deux propriétés. En anticipant un peu, donnons un exemple d'anneau qui n'est ni complet, ni même cohérent.

Exemple. — Considérons l'anneau A des nombres (complexes) de la forme $a + b\sqrt{-5}$, où a et b sont des entiers de signe quelconque ($a, b \in \mathbb{C}$). A est bien un domaine d'intégrité, puisqu'il est contenu dans le corps des nombres $\alpha + \beta\sqrt{-5}$, où α, β décrivent le corps des nombres rationnels Γ (ou dans le corps Ω de tous les nombres complexes). A possède un élément-unité 1.

Pour que $u + v\sqrt{-5}$ divise $a + b\sqrt{-5}$, c'est-à-dire

$$a + b\sqrt{-5} = (u + v\sqrt{-5})(x + y\sqrt{-5}),$$

il faut et il suffit que l'on ait

$$(2) \quad \begin{cases} ux - 5vy = a, \\ vx + uy = b, \end{cases}$$

d'où

$$a - b\sqrt{-5} = (u - v\sqrt{-5})(x - y\sqrt{-5})$$

et

$$a^2 + 5b^2 = (u^2 + 5v^2)(x^2 + 5y^2).$$

Le nombre naturel

$$(3) \quad d = u^2 + 5v^2$$

est donc un diviseur de $a^2 + 5b^2$, d'où seulement un nombre fini de valeurs possibles pour d ; pour chacune de ces valeurs, l'équation (3) ne peut avoir qu'un nombre fini de solutions entières u, v , à chacune desquelles ne correspond d'ailleurs un diviseur $u + v\sqrt{-5}$ de $a + b\sqrt{-5}$ que si le système (2) a des solutions entières x, y . Un élément donné $a + b\sqrt{-5}$ de A a donc un *nombre fini de diviseurs* et la méthode précédente permet de les déterminer.

L'équation

$$u^2 + 5v^2 = 1$$

n'ayant pas d'autres solutions que $u = \pm 1, v = 0$, les unités de A sont $+1$ et -1 .

On vérifie sans peine les résultats suivants. Les éléments $3, 1 - 2\sqrt{-5}, 2 - \sqrt{-5}$ n'ont pas de diviseurs véritables; ils sont *premiers*. Le nombre 9 a les diviseurs $3, 2 + \sqrt{-5}, 2 - \sqrt{-5}$; le nombre $3(1 - 2\sqrt{-5})$ a les diviseurs $3, 1 - 2\sqrt{-5}, 2 - \sqrt{-5}, 4 - \sqrt{-5}$.

L'élément *premier* $2 - \sqrt{-5}$ divise $3^2 = 9$ sans diviser 3 : *il n'est donc pas premier au sens strict, et A n'est pas cohérent; A n'est donc pas non plus un anneau complet*. D'ailleurs, 9 et $3(1 - 2\sqrt{-5})$ n'ont pas de p. g. c. d., car ils ont les deux diviseurs communs 3 et $2 - \sqrt{-5}$ dont aucun ne divise l'autre.

Enfin, le nombre 9 a deux décompositions distinctes en facteurs premiers :

$$9 = 3.3 = (2 + \sqrt{-5})(2 - \sqrt{-5});$$

on a, de même,

$$6 = 2.3 = (1 + \sqrt{-5})(1 - \sqrt{-5});$$

$$21 = 3.7 = (1 + 2\sqrt{-5})(1 - 2\sqrt{-5}).$$

Après avoir donné cet exemple, dans le XI^e supplément aux *Leçons sur la Théorie des Nombres de Dirichlet*, Dedekind le commente ainsi (*Œuvres*, t. 3, p. 19) : « Le même phénomène apparaît dans une infinité d'autres domaines.... C'est sans doute une entreprise parfaitement désespérée de vouloir ramener à des lois simples la décomposition et la divisibilité des nombres. Mais, comme cela s'est produit déjà plus d'une fois dans des circonstances analogues au cours du développement des Sciences Mathématiques, cette difficulté ... est devenue ... l'origine d'une découverte vraiment considérable.... Kummer, dans l'étude des domaines de nombres auxquels conduit le problème de la division du cercle, a découvert que les vieilles lois euclidiennes de la divisibilité retrouvent, même dans ces domaines, leur entière validité, dès que ces domaines sont complétés par l'introduction de nombres nouveaux, qu'il a appelés les nombres idéaux... ».

2. Semi-groupes à factorisation unique; anneaux à factorisation unique. — Un semi-groupe abélien S , ayant un élément-unité e , est un *semi-groupe à factorisation unique* si :

1° *Tout élément a de S , n'appartenant pas au groupe E des unités, est le produit d'un nombre fini d'éléments premiers :*

$$(1) \quad a = p_1 p_2 \dots p_r \quad (r \geq 1).$$

2° *La décomposition (1) est unique (au sens déjà précisé : r est déterminé; les p_i , distincts ou non, sont déterminés à des facteurs-unités près).*

Tout élément de S peut s'écrire sous la forme

$$a = \varepsilon p_1^{\alpha_1} \dots p_n^{\alpha_n} \quad (n \geq 0, \alpha_i > 0),$$

où ε est une unité et où deux facteurs premiers p_i, p_j ($i \neq j$) ne sont pas associés.

Supposons a décomposable et soit c un véritable diviseur de a :

$$a = cc' \quad (c, c' \notin E).$$

La décomposition (1) de a étant, par hypothèse, unique, chaque facteur premier q de c est associé à un facteur premier p de a et figure dans c avec un exposant γ au plus égal à l'exposant α avec lequel p figure dans a ; la différence $\alpha - \gamma$ est l'exposant avec lequel le même facteur (ou un facteur associé) figure dans c' . Convenons de ne pas regarder comme diviseurs distincts deux diviseurs associés : nous voyons qu'un élément a quelconque de S n'a qu'un nombre fini de diviseurs distincts. Il en résulte immédiatement que le semi-groupe Π des idéaux principaux vérifie la condition de chaîne ascendante (ou la condition maximale).

Considérons maintenant deux éléments a, b de S : il est commode de les écrire

$$a = \varepsilon p_1^{\alpha_1} \dots p_k^{\alpha_k}, \quad b = \varepsilon' p_1^{\beta_1} \dots p_k^{\beta_k},$$

où $\varepsilon, \varepsilon'$ sont des unités, $p_1, \dots, p_k$ les facteurs premiers figurant dans l'une au moins des décompositions de a et de b , α_i et β_j des entiers positifs ou nuls.

Un diviseur commun à a et b est de la forme

$$c = \varepsilon'' p_1^{\gamma_1} \dots p_k^{\gamma_k} \quad (\varepsilon'' \in E),$$

avec

$$0 \leq \gamma_i \leq \mu_i = \min(\alpha_i, \beta_i) \quad (i = 1, \dots, k).$$

Tous ces diviseurs divisent l'un deux

$$d = p_1^{\mu_1} \dots p_k^{\mu_k}$$

qui est donc p. g. c. d. de a et b , ainsi d'ailleurs que les éléments associés.

Un semi-groupe S à factorisation unique est donc complet et, par suite, cohérent.

Pour que deux éléments a, b de S soient sans diviseurs communs, ou premiers l'un à l'autre, il faut et il suffit qu'ils n'aient aucun facteur premier commun, c'est-à-dire

$$\mu_i = 0 \quad (i = 1, \dots, k).$$

Dans un semi-groupe abélien à factorisation unique, tout élément premier est premier au sens strict, tout élément qui n'est pas une unité est le produit d'éléments premiers au sens strict. Inversement,

d'ailleurs, si, dans un semi-groupe abélien S , tout élément a qui n'est pas une unité est un produit d'éléments premiers au sens strict, S est un semi-groupe à factorisation unique : on a, en effet, une décomposition de a en facteurs premiers, et cette décomposition est unique, d'après le théorème général d'unicité établi plus haut (chap. IV, § 14, B, th. 7, p. 218).

Les résultats précédents s'appliquent, en particulier, à un domaine d'intégrité F ayant un élément-unité e , et dont le semi-groupe multiplicatif $S = F - \{0\}$ est à factorisation unique : on donne alors à F le nom d'*anneau à factorisation unique*. W. Krull a donné une intéressante condition nécessaire et suffisante pour qu'un domaine d'intégrité avec élément-unité F soit un anneau à factorisation unique⁽¹⁾.

Pour arriver à la condition de Krull (en tant que condition nécessaire), considérons un domaine d'intégrité F à factorisation unique, et associons à tout élément non nul

$$a = p_1^{\alpha_1} \dots p_k^{\alpha_k}$$

le nombre entier

$$\lambda(a) = \alpha_1 + \dots + \alpha_k \geq 0.$$

Cette fonction λ , définie sur $F - \{0\}$, prend des valeurs réelles, positives ou nulles, entières, donc s'accumulant au plus à l'infini⁽²⁾. Si $b|a$, on a $\lambda(b) \leq \lambda(a)$, avec l'inégalité stricte si b est véritable diviseur de a . De plus, on a $\lambda(\varepsilon) = 0$ pour toute unité ε .

La fonction λ a, en outre, une propriété moins évidente, appelée par Krull *condition de réduction*.

Considérons deux éléments $a, b (\neq 0)$ dont aucun n'est multiple de l'autre; soit $d = \text{p. g. c. d.}(a, b)$; posons

$$a = a_1 d, \quad b = b_1 d.$$

Par hypothèse, d est un diviseur véritable de a et de b , d'où

$$\lambda(d) < \text{Min} [\lambda(a), \lambda(b)];$$

a_1 et b_1 sont sans diviseurs communs, par conséquent, un facteur

(1) W. KRULL, *Über die Zerlegung der Hauptideale in allgemeinen Ringen* (Math. Ann., t. 105, 1931, p. 1). Voir aussi H. HASSE, *Über eindeutige Zerlegung in Prim-elemente oder in Primhauptideale in Integritätsbereichen* (J. Ang. Math., t. 159, 1928, p. 3); R. DEDEKIND, *Charakteristische Eigenschaft einklassiger Körper* (Nachlass. Ges. Werke, t. 2, XXXVIII, p. 373).

(2) Cette expression signifie qu'il est impossible d'extraire de l'ensemble des valeurs $\lambda(a)$ une suite de nombres distincts qui converge vers une limite finie.

premier p_i de a ne figure pas à la fois dans a_1 et b_1 : appelons c_i un des éléments a_1, b_1 qui ne soit pas multiple de p_i , et considérons l'élément

$$r = \sum_{i=1}^k p_1 \dots p_{i-1} c_i p_{i+1} \dots p_k.$$

Puisque $c_i = a_1$ ou b_1 , r est de la forme $r = ua_1 + vb_1$; de plus, comme r n'est multiple d'aucun p_i , r est premier à a . Nous avons donc

$$(2) \quad rd = ua + vb,$$

avec

$$(3) \quad \lambda(d) < \text{Min}[\lambda(a), \lambda(b)] \quad \text{et} \quad r \text{ premier à } a.$$

C'est précisément la *condition de réduction de Krull* : il existe, pour chaque couple d'éléments non nuls a, b , dont aucun n'est multiple de l'autre, un élément d (qu'on ne supposera pas, a priori, p. g. c. d. de a et b) et un élément r premier à a vérifiant les relations (2) et (3).

En résumé, pour que le domaine d'intégrité F avec élément-unité soit un anneau à factorisation unique, il faut qu'on puisse définir sur $F - \{0\}$ une fonction λ prenant des valeurs $\lambda(a)$ positives ou nulles, s'accumulant au plus à l'infini, vérifiant

$$(4) \quad \lambda(a) \geq \lambda(b) \quad \text{si} \quad b \mid a$$

avec l'inégalité ou l'égalité suivant que b n'est pas ou est associé à a [$\lambda(e) = \lambda(\varepsilon)$ est la plus petite valeur de λ , on convient de la prendre nulle], et satisfaisant à la *condition de réduction*.

Montrons maintenant que cette condition est *suffisante*. Nous établirons un résultat un peu plus général, utile pour certaines applications. Soit F_1 un sous-ensemble non vide et multiplicativement fermé de $F - \{0\}$, contenant de plus, en même temps qu'un élément a , tout diviseur de a (en particulier, F_1 contient le groupe des unités E). Si un élément x de F_1 est multiple, dans F , d'un élément y de F_1 : $x = ry$, où $r \in F$, r est un diviseur de x , donc $r \in F_1$ et x est aussi multiple de y dans F_1 ⁽¹⁾.

Nous supposons qu'il existe une fonction λ , définie sur F_1 , prenant des valeurs réelles $\lambda(a) \geq 0$, qui s'accumulent au plus à l'infini, vérifiant, d'autre part, la condition (4), et la *condition de réduction sous la*

(1) On peut encore dire que, du point de vue multiplicatif, F_1 est un sous-demi-groupe unitaire de F .

forme suivante : si a et b sont deux éléments de F_1 , dont aucun n'est multiple de l'autre, il existe deux éléments u, v de F tels que l'on ait

$$(2) \quad ua + vb = rd$$

et

$$(3) \quad \lambda(d) < \text{Min}[\lambda(a), \lambda(b)],$$

où d appartient à F_1 , et où r est un élément de F premier à a . Nous allons montrer que, dans F_1 , tout élément a est le produit d'un nombre fini d'éléments premiers au sens strict, et d'abord que a est ou bien premier au sens strict, ou bien décomposable d'une façon non banale.

Pour l'élément considéré, a , de F_1 , nous avons les deux possibilités suivantes, qui s'excluent l'une l'autre :

α . Pour tout élément b de F_1 , non multiple de a , on peut trouver $u, v \in F$ tels que

$$ua + vb = r \quad (r \in F)$$

soit premier à a . Alors, si a divise bx , il divise rx , donc x : tout élément b de F_1 non multiple de a est premier à a ; par conséquent, a est premier au sens strict (dans F_1).

β . Il existe au moins un élément b de F_1 , non multiple de a , tel que, dans toute égalité de la forme

$$(2) \quad ua + vb = rd,$$

où $d \in F_1$ et où $r (\in F)$ est premier à a , on ait $d \notin E$, c'est-à-dire $\lambda(d) > 0$. Alors, cet élément b ne peut pas être une unité, car, pour une unité ε , si nous posons

$$ua + \varepsilon^{-1} \cdot \varepsilon = r,$$

nous avons une relation de la forme (2), avec $d = e \in E$, et où r est bien un élément premier à a ($-ua + er = e$).

Puisque b n'est pas une unité, si b divise a , a est décomposable (dans F_1). Si b ne divise pas a , nous avons l'égalité (2), avec (3), donc avec

$$(3') \quad 0 < \lambda(d) < \lambda(a);$$

Si plusieurs choix de u, v, r, d sont possibles, nous ferons en sorte que $\lambda(d)$ soit *minimum*. D'après (3'), d n'est pas multiple de a ; si a n'était pas multiple de d , nous pourrions, en appliquant la condition de réduction à a et d , trouver $u', v' (\in F)$ tels que

$$u'a + v'd = r'd',$$

où $r' (\in F)$ serait premier à a et où nous aurions

$$(5) \quad \lambda(d') < \lambda(d) \quad (d' \in F_1).$$

Il en résulterait

$$(v'u + ru')a + vv'.b = rr'.d',$$

où rr' est premier à a : d'après (5), cette égalité de la forme (2) est impossible, puisque $\lambda(d)$ est, par hypothèse, minimum.

Nous voyons donc, en tenant compte encore de (3'), que d est un véritable diviseur de a : a est bien décomposable dans F_1 .

Tout élément a qui n'est pas premier au sens strict étant indécomposable, et les facteurs de la décomposition donnant à la fonction λ des valeurs inférieures à $\lambda(a)$, on voit, puisque les valeurs de λ s'accumulent au plus à l'infini, que tout élément de F_1 est le produit d'un nombre fini d'éléments premiers au sens strict.

Pour $F_1 = F - \{0\}$, nous obtenons exactement la réciproque de la première partie.

3. Anneaux à idéaux principaux; anneaux euclidiens. — En modifiant convenablement la *condition de réduction*, on peut caractériser d'une façon analogue deux types plus particuliers de domaines d'intégrité : ceux où tout idéal est principal, et les anneaux euclidiens.

LEMME 1. — *Un domaine d'intégrité $\mathcal{J}$, possédant un élément unité e , et dans lequel tout idéal est principal, est un anneau complet.*

Deux éléments a, b de $\mathcal{J} - \{0\}$ engendrent un idéal (a, b) qui est principal,

$$(a, b) = (d)$$

(où d est défini à un facteur unité près). Nous avons donc

$$(1) \quad d = ua + vb \quad (u, v \in \mathcal{J})$$

et

$$(2) \quad a = a'd, \quad b = b'd.$$

D'après (1) et (2), tout diviseur commun à a et b divise d et tout diviseur de d divise à la fois a et b ; $d = ua + vb$ est donc un p. g. c. d. de a et b .

Étant complet, l'anneau $\mathcal{J}$ est cohérent : tout élément premier est premier au sens strict, et si un élément de $\mathcal{J} - \{0\}$ est décomposable

en un produit d'éléments premiers, la décomposition est unique (§ 1, th. 2 et cor., p. 309).

Remarque. — D'après le lemme 1, si deux éléments a, b de $\mathcal{J} - \{0\}$ sont sans diviseurs communs, leur p. g. c. d. d est nécessairement une unité et ils sont, d'après l'égalité (1), premiers entre eux : la propriété I entraîne la propriété III et, par conséquent, les propriétés I, II et III sont équivalentes (cf. § 1, p. 308).

LEMME 2. — *Un domaine d'intégrité $\mathcal{J}$, possédant un élément unité e , et dans lequel tout idéal est principal, est un anneau à factorisation unique; si l'on associe à l'élément*

$$a = \varepsilon p_1^{\alpha_1} \dots p_n^{\alpha_n} \quad (\neq 0)$$

le nombre

$$\lambda(a) = \alpha_1 + \dots + \alpha_n,$$

la fonction λ vérifie la condition de réduction sous la forme suivante : si a n'est pas multiple de b , ni b multiple de a , on peut trouver u, v tels que l'on ait

$$(3) \quad \lambda(ua + vb) < \text{Min}[\lambda(a), \lambda(b)] \quad (ua + vb \neq 0).$$

L'axiome de la base finie, vérifié dans $\mathcal{J}$ puisque tout idéal de $\mathcal{J}$ est principal, entraîne la *condition maximale* ⁽¹⁾ dans l'ensemble des idéaux de $\mathcal{J}$, qui coïncide ici avec l'ensemble Π des idéaux principaux. Puisque Π vérifie la condition maximale, tout élément de $\mathcal{J} - \{0\}$ qui n'est pas une unité est le produit d'un nombre fini d'éléments premiers (chap. IV, § 14, th. 6, p. 217) : $\mathcal{J}$ est donc bien un *anneau à factorisation unique*.

Si a n'est pas multiple de b , ni b multiple de a , le p. g. c. d. d de a et b est un diviseur véritable de a et de b , et nous avons, d'après la définition de la fonction λ ,

$$\lambda(d) < \text{Min}[\lambda(a), \lambda(b)],$$

d'où la condition de réduction (3) en tenant compte de la forme (1) du p. g. c. d.

LEMME 3. — *Si la fonction λ associée à un domaine à factorisation unique $\mathcal{J}$ vérifie la condition de réduction (3), $\mathcal{J}$ est un anneau à idéaux principaux.*

⁽¹⁾ Cf. chap. IV, § 13, p. 205; chap. I, § 11, p. 50. Rappelons que la démonstration de ce résultat fait intervenir l'axiome du choix.

Remarquons d'abord que la forme (3) de la condition de réduction se déduit de la forme générale (§ 2) en remplaçant l'élément r par e .

L'idéal (o) étant principal, considérons un idéal $\mathfrak{m} \neq (o)$ et soit a un élément non nul de $\mathfrak{m}$, choisi de façon que $\lambda(a)$ soit *minimum* : si $b \in \mathfrak{m}$ et $b \neq o$, nous avons $\lambda(b) \geq \lambda(a)$.

Si a est multiple de b , nous avons

$$\lambda(b) \leq \lambda(a), \quad \text{d'où} \quad \lambda(a) = \lambda(b),$$

ce qui, d'après l'une des propriétés de la fonction λ , entraîne que a et b sont associés : *b est donc multiple de a .*

Si a n'est pas multiple de b , b est encore multiple de a : dans le cas contraire, en effet, nous pourrions trouver u, v tels que l'on ait

$$\lambda(ua + vb) < \lambda(a) \quad (ua + vb \neq o),$$

ce qui est impossible.

L'idéal $\mathfrak{m} = (a)$ est donc principal.

En réunissant les lemmes 2 et 3, nous pouvons énoncer le théorème suivant :

THÉOREME 1. — *Pour qu'un domaine d'intégrité $\mathcal{J}$, possédant un élément-unité e , soit un anneau à idéaux principaux, il faut et il suffit qu'on puisse définir sur $\mathcal{J} - \{o\}$ une fonction λ à valeurs réelles positives ou nulles, s'accumulant au plus à l'infini, vérifiant $\lambda(a) \geq \lambda(b)$ si $b \mid a$ (l'égalité n'ayant lieu que si a et b sont associés), et satisfaisant à la condition de réduction (3) indiquée ci-dessus.*

Dans un tel domaine $\mathcal{J}$, les idéaux premiers différents de l'idéal (o) et de l'idéal-unité $(e) = \mathcal{J}$ sont les idéaux engendrés par un élément premier; montrons qu'un tel idéal (p) est sans diviseurs ⁽¹⁾. La relation d'inclusion stricte

$$(p) \subset \mathfrak{m} = (m)$$

exige que le générateur m de $\mathfrak{m}$ soit un diviseur de p non associé à p , donc une unité, d'où $\mathfrak{m} = \mathcal{J}$.

On donne le nom d'*anneau euclidien* à tout domaine d'intégrité R ne se réduisant pas à l'élément zéro et possédant les deux propriétés suivantes :

⁽¹⁾ Inversement, dans $\mathcal{J}$, tout idéal sans diviseurs est premier (chap. IV, § 12, p. 199).

1° A tout élément non nul $a \in R$ est associé un entier $g(a) \geq 0$, la fonction g étant telle que

$$g(ab) \geq g(a) \quad (b \neq 0);$$

2° Si a est différent de zéro, on peut trouver, pour tout $x \in E$, au moins un couple d'éléments q, r de E tels que

$$(4) \quad x = aq + r, \quad \text{avec} \quad \begin{cases} \text{ou bien } r = 0, \\ \text{ou bien } g(r) < g(a). \end{cases}$$

Les éléments r et q sont respectivement un *reste* et un *quotient* de la *division* de x par a ; la *division avec reste* dont il s'agit ici ne doit pas être confondue avec la *division exacte*, opération inverse de la multiplication, qui en est un cas particulier ($r = 0$), mais n'est pas toujours possible à moins que l'anneau euclidien ne soit un corps.

Exemple. — L'anneau C des entiers est un anneau euclidien : la division avec reste y est définie par l'égalité (4) et la double inégalité

$$(5) \quad 0 \leq r < |a|.$$

Si l'on définit la fonction g en posant

$$g(x) = |x|,$$

les conditions 1° et 2° sont bien vérifiées. On voit aisément que le quotient q et le reste r sont uniques.

La définition d'un anneau euclidien a été prise sous une forme aussi générale que possible : elle ne postule explicitement ni l'existence d'un élément-unité, ni le fait qu'on a l'inégalité stricte $g(ab) > g(a)$ si b n'est pas une unité. Ces deux propriétés, comme nous allons le montrer, résultent de la définition.

THEOREME 2. — *Dans un anneau euclidien R , tout idéal $\mathfrak{a}$ est principal :*

$$(6) \quad \mathfrak{a} = (a) = Ra$$

et R possède un élément-unité e .

L'idéal (0) étant principal, supposons $\mathfrak{a} \neq (0)$ et soit a un des éléments non nuls de $\mathfrak{a}$ pour lesquels $g(a)$ est *minimum*. Si x est un élément quelconque de $\mathfrak{a}$, l'élément r de la relation (4) appartient à l'idéal $\mathfrak{a}$: si donc r n'était pas nul, nous aurions $g(r) \geq g(a)$, ce qui est impossible. Nous avons donc

$$r = 0, \quad x = qa \in Ra$$

et, par suite,

$$a \subseteq Ra.$$

Or, nous avons évidemment

$$Ra \subseteq (a) \subseteq a,$$

d'où les égalités (6).

L'idéal R lui-même est engendré par un élément m :

$$R = (m) = Rm.$$

En particulier, l'élément m de R vérifie une égalité de la forme

$$(7) \quad m = em, \quad \text{avec } e \in R.$$

Puisque R ne se réduit pas à l'élément zéro, nous avons $m \neq 0$, $e \neq 0$ et, dans le *semi-groupe* $R \rightarrow \{0\}$, l'égalité (7) entraîne que e est élément-unité bilatère ⁽¹⁾.

D'après le lemme 1 et le théorème 2, les notions d'éléments sans diviseurs communs, premiers l'un à l'autre et premiers entre eux, se confondent dans un anneau euclidien; tout élément premier est premier au sens strict. Pour tout élément x de e , nous avons

$$g(x) = g(ex) \geq g(e).$$

THÉORÈME 3. — *Pour qu'un élément non nul, ε , de R , soit une unité, il faut et il suffit que l'on ait*

$$(8) \quad g(e) = g(\varepsilon).$$

Si ε est une unité, nous avons

$$g(\varepsilon\varepsilon^{-1}) = g(e) \geq g(\varepsilon) \geq g(e),$$

d'où l'égalité (8).

Si $\varepsilon (\neq 0)$ vérifie l'égalité (8), considérons le reste r de la division de e par ε :

$$e = q\varepsilon + r.$$

Si r n'était pas nul, nous aurions

$$g(r) < g(\varepsilon) = g(e),$$

ce qui est impossible. Nous avons donc $r = 0$, et ε est une unité ($\varepsilon^{-1} = q$).

⁽¹⁾ Directement, on peut remarquer que, tout élément x de R étant de la forme $x = mq$, on a

$$ex = e.mq = em.q = mq = x.$$

THÉORÈME 4. — Si b est un diviseur de a , $a = bc$ ($a \neq 0$) on a

$$(9) \quad g(b) \leq g(a),$$

l'égalité ayant lieu si et seulement si b et a sont associés.

L'inégalité (9) résulte de la première condition imposée à la fonction g :

$$g(a) = g(bc) \geq g(b).$$

Si c est une unité ε , les relations $a = b\varepsilon$, $b = a\varepsilon^{-1}$ entraînent

$$g(a) \geq g(b) \geq g(a),$$

d'où l'égalité.

Supposons, au contraire, que b soit un véritable diviseur de a ; nous avons

$$b = aq + r, \quad \text{avec } r \neq 0, \quad \text{donc } g(r) < g(a).$$

Mais l'égalité $a = bc$ donne

$$r = b(e - qc), \quad \text{donc } g(r) \geq g(b),$$

d'où enfin

$$g(b) < g(a).$$

D'après le théorème 4, la fonction $g(a)$ définie sur $R - \{0\}$ a les propriétés de la fonction $\lambda(a)$ considérée dans l'étude des anneaux à idéaux principaux. La condition de réduction, en particulier, est vérifiée : si a n'est pas multiple de b , ni b multiple de a , nous avons

$$a = bq + r, \quad \text{avec } r \neq 0, \quad \text{donc } g(r) < g(b);$$

$$b = aq' + r', \quad \text{avec } r' \neq 0, \quad \text{donc } g(r') < g(a).$$

Celui des deux nombres r , r' pour lequel g a la plus petite valeur est de la forme $ua + vb$ ($\neq 0$) et vérifie

$$g(ua + vb) < \text{Min}[g(a), g(b)].$$

Une autre conséquence du théorème 4 est que, dans un anneau euclidien, le plus grand commun diviseur de deux éléments a_1 , a_2 s'obtient par le procédé connu sous le nom d'*algorithme d'Euclide* (ce qui est précisément la raison pour laquelle un tel anneau est appelé euclidien). Si a_1 et a_2 sont associés, nous avons comme p. g. c. d. a_2 (ou tout élément associé). Dans le cas contraire, et si l'on a par exemple $g(a_1) \geq g(a_2)$, posons

$$a_1 = q_1 a_2 + a_3, \quad \text{avec } g(a_3) < g(a_2)$$

si a_3 n'est pas nul, puis

$$a_2 = q_2 a_3 + a_4, \quad \text{avec } g(a_4) < g(a_3)$$

si a_i n'est pas nul, etc. Comme l'ensemble des diviseurs communs à a_i et a_{i+1} coïncide avec l'ensemble des diviseurs communs à a_{i+1} et a_{i+2} , nous voyons que, si a_{n+2} est nul, les diviseurs communs à a_1 et a_2 sont les diviseurs de a_{n+1} qui est, par suite, un p. g. c. d. de a_1 et a_2 . Or, les nombres $g(a_i)$ vont en diminuant : nous obtenons donc bien, au bout d'un nombre fini n de divisions, une division exacte

$$a_n = q_n a_{n+1}.$$

D'après le théorème 2, tout anneau euclidien R est un anneau à idéaux principaux, donc un *anneau à factorisation unique* : il n'est pas sans intérêt d'en donner une démonstration directe, ne faisant pas intervenir l'axiome du choix.

Soit n_0 le minimum de $g(x)$ pour les éléments x de R qui ne sont égaux ni à zéro, ni à une unité, $n_0 > g(e)$. Tout élément p pour lequel on a $g(p) = n_0$ est premier.

Soient maintenant n un entier supérieur à n_0 et x un élément de R pour lequel $g(x) = n$. Supposons que tout élément a de R pour lequel $g(a)$ est inférieur à n , soit décomposable en un produit de facteurs premiers. Ou bien x est premier, ou bien il est décomposable en un produit aa' de diviseurs véritables : on a

$$g(a) < g(x), \quad g(a') < g(x);$$

a et a' sont décomposables en produits de facteurs premiers, et il en est de même de x . L'unicité de la décomposition, à des facteurs-unités près, est assurée d'après des propositions antérieures (§ 1, corollaires des théorèmes 2 et 3).

Nous avons ainsi étendu aux anneaux euclidiens les propositions fondamentales de l'arithmétique élémentaire et, en particulier, retrouvé ces propositions pour l'anneau des entiers, $\mathbb{C}$. Le fait qu'elles dérivent toutes de l'algorithme d'Euclide et, par conséquent, de la division avec reste, a été mis très nettement en évidence par Dirichlet (*Vorlesungen über Zahlentheorie*, 3^e éd., § 16, p. 30). Cependant, comme l'ont remarqué Kronecker (*Zahlentheorie*, p. 70-72) et Zermelo et comme nous l'avons vu plus haut, l'importante proposition de l'*unicité* de la décomposition en facteurs premiers peut être établie indépendamment de l'Algorithme d'Euclide. La théorie des anneaux euclidiens a été étendue au cas non abélien par J. H. M. Wedderburn, dans un Mémoire intitulé : *Non commutative domains of Integrity* (*J. f. Math.*, t. 167, 1932, p. 129-141). En ce qui concerne les *anneaux non commutatifs*, nous nous bornerons ici à établir le théorème suivant, trivial dans le cas abélien.

THÉOREME 5. — *Un anneau non commutatif $\mathcal{R}$, avec élément-unité e , sans véritables diviseurs de zéro, et dans lequel tout idéal à droite est principal, est régulier à droite.*

Nous devons montrer que deux éléments a, b non nuls de $\mathcal{R}$ ont au moins un multiple commun à droite non nul, m . L'idéal à droite $\{a, b\}$, ensemble des éléments de la forme $ar + bs$, où r et $s \in \mathcal{R}$, étant principal,

$$\{a, b\} = \{d\},$$

nous avons

$$a = da' \quad b = db' \quad \text{et} \quad d = au + bv,$$

où $a' \neq 0$, $b' \neq 0$ et où u et v ne sont pas tous les deux nuls : soit, par exemple, $u \neq 0$. Les relations précédentes entraînent

$$b(e - vb') = a \cdot ub' = m \neq 0,$$

ce qu'il fallait démontrer.

Exercices. — 1. Dans tout domaine d'intégrité avec élément-unité où la propriété :

I. x et y sont sans diviseurs communs,
entraîne la propriété :

II. y est premier à x ,
l'existence d'un p. g. c. d. d de deux éléments a, b entraîne celle d'un p. p. c. m. m et le produit dm est égal au produit ab .

2. Quel est le plus petit nombre naturel possédant 12 diviseurs distincts ?

3. Si la fonction $g(a)$ qui intervient dans la définition d'un anneau euclidien vérifie l'inégalité

$$g(x - y) \leq \text{Max}[g(x), g(y)] \quad (x, y \neq 0),$$

la division avec reste n'est possible que d'une manière.

4. Soit D un nombre naturel, non carré parfait. L'ensemble des nombres réels de la forme $x + y\sqrt{D}$, où x, y appartiennent à l'anneau des entiers $\mathbb{C}$, est un domaine d'intégrité $\mathcal{O}_1$. Pour que $x + y\sqrt{D}$ soit une unité de $\mathcal{O}_1$, il faut et il suffit que x et y vérifient l'équation de Pell ⁽¹⁾

$$x^2 - Dy^2 = \pm 1.$$

⁽¹⁾ La méthode suivante indiquée par Dedekind dans le Supplément VIII aux *Vorlesungen Über Zahlentheorie* de Dirichlet, fournit rapidement les principales propriétés des racines de l'équation de Pell et, par conséquent, des unités du domaine $\mathcal{O}_1$.

LEMME. — *Il existe une infinité de couples d'entiers X, Y vérifiant l'inégalité*

$$(1) \quad |X^2 - DY^2| < 1 + 2\sqrt{D}.$$

Pour établir cette proposition, choisissons un entier naturel m , et attribuons à y successivement les valeurs $0, 1, \dots, m-1, m$. A chacune de ces valeurs, nous pouvons

associer une valeur de x et une seule telle que l'on ait

$$0 \leq x - y\sqrt{D} < 1.$$

Si nous décomposons l'intervalle $(0, 1)$ en m intervalles partiels $\left(\frac{k}{m}, \frac{k+1}{m}\right)$ ($k = 0, 1, \dots, m-1$), deux au moins des $m+1$ nombres $x - y\sqrt{D}$ appartiennent au même intervalle partiel : si nous désignons ces deux nombres par $x' - y'\sqrt{D}$ et $x'' - y''\sqrt{D}$ ($y' > y''$), nous avons, en posant $X = x' - x''$, $Y = y' - y'' (> 0)$,

$$(2) \quad |X - Y\sqrt{D}| < \frac{1}{m}, \quad Y \leq m, \quad Y \neq 0;$$

d'où, *a fortiori*,

$$|X - Y\sqrt{D}| < \frac{1}{Y}.$$

Posons donc

$$X - Y\sqrt{D} = \frac{\delta}{Y}.$$

Nous avons $-1 < \delta < +1$ et $\delta \neq 0$, puisque $\sqrt{D}$ n'est pas rationnel. Il en résulte

$$X + Y\sqrt{D} = \frac{\delta}{Y} + 2Y\sqrt{D}$$

et

$$X^2 - DY^2 = \frac{\delta^2}{Y^2} + 2\delta\sqrt{D},$$

d'où, puisque δ est compris entre -1 et $+1$,

$$|X^2 - DY^2| < 1 + 2\sqrt{D}.$$

Nous avons ainsi trouvé un couple X, Y vérifiant l'inégalité (1). Supposons, d'une manière générale, que nous en ayons obtenu un nombre fini, et montrons qu'il est possible d'en trouver encore un autre. Nous pouvons choisir l'entier m assez grand pour que $\frac{1}{m}$ soit inférieur à chacune des quantités $|X - Y\sqrt{D}|$ correspondant aux couples déjà obtenus. Le couple X, Y fourni, pour cette valeur de m , par le procédé précédent, est nécessairement différent, d'après (2), des couples déjà obtenus, et le lemme est démontré.

Nous allons en déduire que l'équation de Pell admet toujours des solutions entières ξ, η dans lesquelles η est différent de zéro.

Comme il n'y a qu'un nombre fini d'entiers dont la valeur absolue est inférieure à $1 + 2\sqrt{D}$, il existe au moins un tel entier k , non nul, tel que l'on ait

$$X^2 - DY^2 = k$$

pour une infinité de couples X, Y . Comme il n'y a, d'autre part, qu'un nombre fini, k^2 , de systèmes de restes modulo k pour X et Y , nous avons au moins un système m, n de restes pour lequel il existe une infinité de couples X, Y vérifiant simultanément

$$(3) \quad X^2 - DY^2 = k,$$

$$(3') \quad X \equiv m \pmod{k}, \quad Y \equiv n \pmod{k}.$$

Soient X', Y', X'', Y'' deux tels couples. Nous avons

$$X'X'' - DY'Y'' \equiv X'^2 - DY'^2 \equiv 0 \pmod{k},$$

$$X'Y'' - Y'X'' \equiv 0 \pmod{k},$$

d'où

$$(X' - Y'\sqrt{D})(X'' + Y''\sqrt{D}) = k(\xi + \eta\sqrt{D}) \quad (\xi, \eta \text{ entiers}).$$

On a, de même,

$$(X' + Y' \sqrt{D})(X'' - Y'' \sqrt{D}) = k(\xi - \eta \sqrt{D}),$$

d'où, en multipliant membre à membre,

$$\xi^2 - D\eta^2 = 1,$$

Si η était nul, donc ξ égal à ± 1 , on aurait

$$(X' - Y' \sqrt{D})(X'' + Y'' \sqrt{D}) = \pm k,$$

donc, puisque X'', Y'' vérifient (3);

$$X' - Y' \sqrt{D} = \pm (X'' - Y'' \sqrt{D}).$$

Or, parmi l'infinité de couples X, Y vérifiant (3) et (3'), nous pouvons toujours choisir X', Y' et X'', Y'' de manière que X' soit différent de $\pm X''$ et Y' différent de $\pm Y''$. Il existe donc bien au moins une solution entière ξ, η dans laquelle η n'est pas nul.

D'ailleurs, pour des équations simples, telles que

$$x^2 - 2y^2 = \pm 1, \quad x^2 - 3y^2 = \pm 1, \quad x^2 - 5y^2 = \pm 1,$$

de telles solutions sont souvent évidentes :

$$x = 1, \quad y = 1; \quad x = 2, \quad y = 1; \quad x = 2, \quad y = 1.$$

[Pour une méthode permettant de trouver dans tous les cas la plus petite solution, voir par exemple SERRET (*Cours d'Algèbre supérieure*, t. I, p. 80-85); C. DIRICHLET, (*Vorlesungen über Zahlentheorie*, p. 208); E. CARMICHAEL (*Éléments de la théorie des Nombres*, chap. VI, p. 262).]

Pour déterminer maintenant toutes les solutions de l'équation de Pell ou, ce qui revient au même, toutes les unités de $\mathcal{O}_1$, nous remarquerons que puisque les unités forment un groupe, le produit et le quotient de deux quelconques d'entre elles est encore une unité,

D'autre part, si $\varepsilon = x + y \sqrt{D}$ est une unité, $x - y \sqrt{D} = \pm \varepsilon^{-1}$, $-x + y \sqrt{D} = \pm \varepsilon^{-1}$, $-x - y \sqrt{D} = -\varepsilon$ en sont aussi. Il suffit donc d'étudier les unités ε pour lesquelles on a $x > 0, y > 0$; ces unités sont supérieures à 1, et ce sont les seules qui le soient.

Soit $\varepsilon_0 = x_0 + y_0 \sqrt{D}$ ($x_0 > 0, y_0 > 0$) la plus petite d'entre elles. Pour toute unité $\varepsilon = x + y \sqrt{D}$, $x > 0, y > 0$, il existe un nombre naturel n tel que

$$\varepsilon_0^n \leq \varepsilon < \varepsilon_0^{n+1},$$

d'où

$$1 \leq \frac{\varepsilon}{\varepsilon_0^n} < \varepsilon_0.$$

Or $\frac{\varepsilon}{\varepsilon_0^n}$ est une unité : on a donc nécessairement $\frac{\varepsilon}{\varepsilon_0^n} = 1$ et, par suite,

$$\varepsilon = \varepsilon_0^n.$$

Il en résulte que toutes les unités du domaine $\mathcal{O}_1$ sont de la forme

$$\pm \varepsilon_0^v \quad (v \text{ entier relatif arbitraire})$$

ou encore

$$(-1)^{\mu} \varepsilon_0^v \quad (\mu, v \text{ entiers relatifs arbitraires}).$$

Par conséquent, le groupe multiplicatif E des unités admet les deux générateurs : -1 , d'ordre 2, et ε_0 , d'ordre infini. Il en résulte également que toutes les solutions de l'équation de Pell se déduisent de la solution particulière x_0, y_0 .

B. — ANNEAUX ET IDÉAUX DE POLYNOMES.

4. **Polynomes. Opérations entières.** — Considérons un *anneau commutatif* ⁽¹⁾ A et un demi-groupe cyclique infini, engendré par un élément x et possédant un élément-unité x^0

$$\Delta = \{x^0, x^1 = x, x^2, \dots, x^m, \dots\}.$$

On a $x^m \cdot x^n = x^{m+n}$ quels que soient $m, n \geq 0$. Les *polynomes* en x à coefficients dans A sont, par définition, les sommes formelles finies

$$f(x) = a_0 x^0 + a_1 x + \dots + a_n x^n = \sum_{i=0}^n a_i x^i, \quad \text{où } a_i \in A$$

soumises aux règles de calcul énoncées ci-dessous.

Si $a_n \neq 0$, $n \geq 0$, l'entier positif ou nul n s'appelle le *degré* du polynome $f(x)$; les éléments a_i sont ses *coefficients*; x est la *variable* ou l'*indéterminée* ⁽²⁾. Il est souvent commode de représenter le polynome $f(x)$ par la notation

$$f(x) = \sum_{i=0}^{\infty} a_i x^i = \sum a_i x^i$$

étant entendu que *parmi les coefficients a_i un nombre fini seulement sont différents de zéro*.

Un polynome est dit *nul* si tous ses coefficients sont nuls. Deux polynomes sont *égaux* ⁽³⁾ si leurs coefficients de même indice sont égaux.

La *somme* de deux polynomes

$$f(x) = \sum a_i x^i, \quad g(x) = \sum b_i x^i$$

⁽¹⁾ On supposera même en général que A est un *domaine d'intégrité* possédant un *élément-unité*. La définition des polynomes à coefficients dans A peut s'étendre au cas où A n'est pas commutatif, mais on voit alors apparaître certaines complications, notamment en ce qui concerne la *spécialisation* (voir p. 331).

⁽²⁾ On emploie fréquemment aussi, pour écrire un polynome de degré n , la notation

$$f(x) = a_0 x^n + a_1 x^{n-1} + \dots + a_n.$$

On dit alors que le polynome est ordonné suivant les puissances décroissantes de x .

⁽³⁾ En Algèbre élémentaire, on emploie l'expression : *identiques*. Nous verrons plus loin [p. 330, note ⁽¹⁾] que la chose essentielle est de distinguer entre le polynome formel $f(x)$, la fonction correspondante définie dans A et y prenant ses valeurs, et les valeurs de cette fonction, c'est-à-dire les expressions rationnelles entières.

est, par définition, le polynome

$$s(x) = \sum (a_i + b_i) x^i.$$

Son degré est égal au plus grand des degrés m , n de f et de g si m et n sont différents, au plus égal à leur valeur commune si m et n sont égaux. L'ensemble des polynomes

$$f(x) = \sum a_i x^i \quad (a_i \in \mathbf{A})$$

est un groupe abélien additif.

Le produit des polynomes $f(x)$, $g(x)$ est, par définition, le polynome

$$p(x) = \sum u_l x^l,$$

où

$$u_l = a_0 b_l + a_1 b_{l-1} + \dots + a_l b_0 = \sum_{i+j=l} a_i b_j.$$

Ce produit s'obtient donc en multipliant chaque terme (non nul) de f par chaque terme (non nul) de g , l'indéterminée étant regardée comme permutable avec les coefficients, puis en sommant. On a, en particulier, si f et g sont non nuls et de degrés respectifs m et n ,

$$u_{m+n} = a_m b_n, \quad u_{m+n+1} = u_{m+n+2} = \dots = 0.$$

Le degré du produit $p = fg$ est donc au plus égal à la somme des degrés de f et de g ; si $\mathbf{A}$ est un domaine d'intégrité, le degré de fg est égal à $m+n$ et le produit de deux polynomes non nuls est un polynome non nul. La multiplication des polynomes est visiblement commutative, et distributive par rapport à l'addition. Elle est aussi associative, car si nous considérons un troisième polynome

$$h(x) = \sum c_k x^k,$$

nous avons

$$f(x)g(x).h(x) = \sum v_l x^l, \quad f(x).g(x)h(x) = \sum v'_l x^l,$$

où

$$v_l = \sum_{i+j+k=l} a_i b_j c_k = v'_l.$$

L'ensemble des polynomes $f(x) = \sum a_i x^i (a_i \in \mathbf{A})$, est donc un

anneau commutatif, que l'on désigne par $A[x]$. Si A est un domaine d'intégrité, $A[x]$ en est un aussi, d'après ce qui a été vu plus haut. On peut alors former le corps des quotients de $A[x]$, dont les éléments sont, par définition, les *fractions rationnelles* $\frac{f(x)}{g(x)}$; on désigne ce corps par $A(x)$. On a $A(x) = K(x)$, K désignant le corps des quotients de A .

L'ensemble des polynômes de degré nul forme un sous-anneau $\bar{A}$ de $A[x]$, isomorphe à l'anneau A . $A[x]$ peut donc être regardé comme une *extension* de A . Il est d'usage d'identifier $\bar{A}$ avec A , donc de poser

$$a_0 x^0 = a_0 \quad \text{pour tout} \quad a_0 \in A.$$

Lorsque A possède un *élément-unité* e , on satisfait à la convention précédente en égalant e à l'élément-unité x^0 de Δ . On pose donc aussi $ex = x$, ce qui permet de regarder l'indéterminée x et, par suite, tous les éléments du demi-groupe Δ , comme des polynômes particuliers.

Remplaçons le demi-groupe cyclique $\Delta = \{x\}$ par un demi-groupe isomorphe $\Delta' = \{y\}$; nous obtenons un anneau de polynômes $A[y]$. La correspondance

$$f(x) = a_0 + a_1 x + \dots + a_n x^n \longleftrightarrow a_0 + a_1 y + \dots + a_n y^n = f(y)$$

entre $A[x]$ et $A[y]$ est un *isomorphisme* dans lequel *tout élément de A se correspond à lui-même* et, par conséquent, un *isomorphisme relatif par rapport à A* :

$$A[x] \underset{(A)}{\cong} A[y].$$

L'anneau des polynômes à une indéterminée sur un anneau donné A n'est défini qu'à un tel isomorphisme près.

Quand l'anneau A contient un *élément-unité* e , on peut construire l'anneau $A[x]$ en faisant intervenir seulement les éléments de A . Considérons, en effet, les suites

$$P = (a_0, a_1, \dots, a_n, \dots), \quad Q = (b_0, b_1, \dots, b_n, \dots), \quad \dots$$

d'éléments de A dans lesquelles tous les éléments sont *nuls à partir d'un certain rang*. Posons

$$\begin{aligned} P + Q &= (a_0 + b_0, \dots, a_n + b_n, \dots), \\ PQ &= (u_0, \dots, u_n, \dots), \end{aligned}$$

avec

$$u_l = a_0 b_l + a_1 b_{l-1} + \dots + a_l b_0;$$

l'ensemble des suites $P, Q, \dots$, est un *anneau* R . Posons

$$X = (0, e, 0, 0, \dots).$$

Nous avons

$$X^2 = (0, 0, e, 0, \dots), \quad \dots, \quad X^n = (0, 0, \dots, e, 0, \dots)$$

et, si nous convenons d'écrire

$$X^0 = (e, 0, 0, \dots),$$

$$P = (a_0, a_1, \dots, a_n, \dots) = \sum a_i X^i.$$

Si nous établissons la correspondance

$$X \leftrightarrow x, \quad P = \sum a_i X^i \leftrightarrow \sum a_i x^i,$$

les anneaux R et $A[x]$ sont isomorphes sur A , et R peut être regardé comme une *réalisation* de l'anneau $A[x]$.

En introduisant de nouvelles indéterminées $x_2, x_3, \dots, x_n$ que nous supposerons permutables entre elles et avec x_1 , nous pouvons construire, à partir de l'anneau $A[x_1]$, les anneaux

$$A[x_1][x_2], \quad \dots, \quad A[x_1][x_2] \dots [x_n].$$

Ce dernier est appelé *anneau des polynômes à n variables $x_1, x_2, \dots, x_n$ sur A* . Les n indéterminées jouant des rôles symétriques, puisqu'elles sont permutables entre elles, on désigne cet anneau par $A[x_1, x_2, \dots, x_n]$, il est l'ensemble des sommes, ou *polynômes*

$$f(x_1, x_2, \dots, x_n) = \sum a_{i_1, i_2, \dots, i_n} x_1^{i_1} x_2^{i_2} \dots x_n^{i_n},$$

où les coefficients $a_{i_1, i_2, \dots, i_n}$ appartiennent à A , un nombre fini seulement d'entre eux étant différents de zéro.

Le *degré* du *terme*, ou *monome*, $a_{i_1, i_2, \dots, i_n} x_1^{i_1} x_2^{i_2} \dots x_n^{i_n}$, supposé non nul, est par définition l'entier, positif ou nul, $i_1 + i_2 + \dots + i_n$. Le degré d'un polynôme non nul est le maximum des degrés de ses termes non nuls. On donne souvent le nom de *constantes* aux polynômes de degré nul. On appelle *forme* ou *polynôme homogène* un polynôme dont tous les termes ont le même degré. Le produit de deux formes (non nulles) est une forme; si A est un domaine d'intégrité, ce produit n'est pas nul et son degré est la somme des degrés des facteurs.

Un polynôme de degré n peut être décomposé en somme de parties homogènes de degrés respectifs $0, 1, \dots, n$: il en résulte que le produit

d'un polynôme de degré m par un polynôme de degré n est un polynôme de degré au plus égal à $m + n$, l'égalité ayant nécessairement lieu si l'anneau A des coefficients est un domaine d'intégrité. Dans ce cas, l'anneau $A[x_1, x_2, \dots, x_n]$ est aussi un domaine d'intégrité.

Considérons un anneau A' contenant A (et pouvant coïncider avec lui). Si, dans un polynôme

$$f(x) = a_0 + a_1x + \dots + a_nx^n \in A[x],$$

nous remplaçons x par un élément α de A' , nous obtenons une *expression rationnelle entière* (cf. chap. V, § 10, p. 305)

$$f(\alpha) = a_0 + a_1\alpha + \dots + a_n\alpha^n \in A',$$

appelée *valeur de $f(x)$ pour $x = \alpha$* . Si $g(x)$ est un autre polynôme de $A[x]$ et si l'on pose

$$(1) \quad f(x) + g(x) = s(x), \quad f(x)g(x) = p(x),$$

on a, d'après les règles fixées pour le calcul des polynômes,

$$(1') \quad f(\alpha) + g(\alpha) = s(\alpha), \quad f(\alpha)g(\alpha) = p(\alpha).$$

L'application $f(x) \rightarrow f(\alpha)$ de $A[x]$ dans A' est donc *régulière* par rapport à l'addition et à la multiplication.

Par conséquent, toute relation entre polynômes de $A[x]$ faisant intervenir l'égalité, la somme et le produit, reste vérifiée lorsqu'on y spécialise l'indéterminée x , c'est-à-dire lorsqu'on la remplace par un élément d'un anneau A' contenant A (principe de spécialisation).

Un polynôme $f(x)$ définit une *fonction* dans tout anneau $A' \supseteq A$ en particulier dans l'anneau lui-même. Cette fonction est dite *rationnelle et entière*, pour exprimer que le calcul de sa valeur comporte seulement des additions et des multiplications ⁽¹⁾. Le principe de spécialisation et

(1) En Analyse, on ne fait pas de distinction entre le polynôme et la fonction rationnelle entière correspondante. En Algèbre, au contraire, cette distinction s'impose pour les raisons suivantes.

D'après les formules (1) et (1'), la correspondance univoque

$$f(x) \rightarrow f(\alpha) \quad (\alpha \in A)$$

entre les polynômes de l'anneau $A[x]$ et les fonctions rationnelles entières $f(\alpha)$ définies dans A et y prenant leurs valeurs, respecte l'addition et la multiplication : c'est donc un homomorphisme, ou éventuellement un isomorphisme. Pour que ce soit un isomorphisme, il faut et il suffit qu'une même fonction ne soit pas l'image de deux polynômes différents, autrement dit que deux polynômes prenant des valeurs égales pour chaque valeur de x dans A , soient égaux (c'est-à-dire aient les mêmes coeffi-

la notion de fonction rationnelle entière s'étendent immédiatement au cas de plusieurs variables.

Si l'anneau A' n'est pas commutatif, on peut encore spécialiser dans A' à condition d'attribuer à x une valeur $\alpha \in A'$ permutable avec tout élément de l'anneau (commutatif) A : toute relation entre polynômes en x entraîne bien la relation correspondante entre expressions rationnelles entières en α . S'il s'agit de polynômes à plusieurs variables $x, y, \dots$, le principe de spécialisation subsiste également, à condition d'attribuer à $x, y, \dots$ des valeurs $\alpha, \beta, \dots \in A'$ permutable entre elles et avec tout élément de A .

Exercice. — Calculer le nombre $N(n, l)$ de termes distincts dans la forme la plus générale, à n variables, de degré l . Quel est le nombre de termes distincts dans le polynôme le plus général, à n variables, de degré l ?

3. Idéaux de polynômes. — A étant un anneau, nous nous proposons d'étudier quelques propriétés des idéaux de l'anneau $A[x]$. Nous avons en premier lieu la proposition suivante, connue sous le nom de *Théorème de la base finie*, ou de *Théorème de Hilbert* ⁽¹⁾.

THÉORÈME. — Si un anneau A , possédant un élément-unité, est noethérien ⁽²⁾, l'anneau $A[x]$ est, lui aussi, noethérien.

L'ensemble formé par zéro et par les coefficients $u_m, v_n, \dots$ de la plus haute puissance de x dans les polynômes

$$f(x) = u_0 + \dots + u_m x^m, \quad g(x) = v_0 + \dots + v_n x^n, \quad \dots$$

$$(u_m \neq 0, v_n \neq 0, \dots)$$

cients). Or, il existe des anneaux, importants du point de vue de l'Algèbre, dans lesquels cette condition n'est pas vérifiée. Par exemple, dans le corps $\{0, 1\}$ des classes résiduelles modulo 2, le polynôme $x^2 + x$ prend la valeur 0 pour toute valeur attribuée à x ; il est cependant distinct du polynôme 0. Plus généralement, soit $A = \{0, 1, a_3, \dots, a_N\}$ un anneau fini possédant un élément-unité 1 : le polynôme non nul

$$x(x-1) \dots (x-a_N) = x^N + \dots$$

prend la valeur zéro pour tout $\alpha \in A$. — Nous verrons ultérieurement (chap. VII, § 1, p. 359) que, dans le cas où A est un corps K , ou même un domaine d'intégrité, il est non seulement suffisant, mais nécessaire, que A soit fini pour qu'il existe dans $A[x]$ des polynômes non nuls prenant la valeur zéro pour toute valeur α attribuée à x dans A .

⁽¹⁾ D. HILBERT, *Über die Theorie der algebraischen Formen* (Math. Ann., t. 36, 1890, p. 473).

⁽²⁾ Rappelons qu'un anneau commutatif A est dit *noethérien* si tout idéal de A possède une base finie.

d'un idéal $\mathfrak{m}$, est un idéal $\mathfrak{a}$ dans A . En effet, en supposant par exemple, $m \geq n$, $u_m - v_n$ est, ou bien nul, ou bien égal au coefficient de la plus haute puissance de x dans le polynôme $f - x^{m-n} \cdot g$, qui appartient à $\mathfrak{m}$; (A ayant un élément-unité, x^{m-n} est un polynôme de $A[x]$ et, par conséquent, $x^{m-n} g \in \mathfrak{m}$). D'autre part, si r est un élément quelconque de A , le produit ru_m est ou bien nul, ou bien égal au coefficient de la plus haute puissance de x dans le polynôme $rf(x) \in \mathfrak{m}$, d'où $ru_m \in \mathfrak{a}$.

Par hypothèse, l'idéal $\mathfrak{a}$ admet une base finie :

$$\mathfrak{a} = (a_1, \dots, a_h),$$

où a_i est le coefficient de la plus haute puissance de x dans au moins un polynôme $\alpha_i(x)$ de l'idéal $\mathfrak{m}$, polynôme dont nous désignerons le degré par μ_i . Désignons par N le plus grand des μ_i . Soit

$$f(x) = u_0 + \dots + u_m x^m$$

un polynôme de l'idéal $\mathfrak{m}$ de degré $m \geq N$; on a

$$u_m \in \mathfrak{a}, \quad \text{d'où} \quad u_m = r_1 a_1 + \dots + r_h a_h \quad (r_i \in A)$$

et, par conséquent, le polynôme

$$f(x) - r_1 x^{m-\mu_1} \alpha_1(x) - \dots - r_h x^{m-\mu_h} \alpha_h(x)$$

est nul ou de degré au plus égal à $m-1$. En appliquant au besoin plusieurs fois le même procédé, on voit qu'on peut retrancher de f un polynôme appartenant à l'idéal

$$(\alpha_1(x), \dots, \alpha_h(x)) \subseteq \mathfrak{m}$$

et tel que la différence soit un polynôme $f_1(x) \in \mathfrak{m}$, nul ou de degré inférieur à N .

Si nous considérons maintenant les polynômes de degré $N-1$ qui appartiennent à l'idéal $\mathfrak{m}$, l'ensemble formé par zéro et par les coefficients de x^{N-1} dans ces différents polynômes est encore un idéal $\mathfrak{b}$ dans l'anneau A , et cet idéal (qui peut être nul) admet une base finie

$$\mathfrak{b} = (b_1, \dots, b_k),$$

où b_i est le coefficient de x^{N-1} dans un polynôme $\beta_i(x) \in \mathfrak{m}$. Si alors $f_1(x) = v_0 + \dots + v_{N-1} x^{N-1}$ est un polynôme de $\mathfrak{m}$ de degré $N-1$, on a

$$v_{N-1} = s_1 b_1 + \dots + s_k b_k \quad (s_i \in A)$$

et le polynôme

$$f_2(x) = f_1(x) - s_1 \beta_1(x) - \dots - s_k \beta_k(x)$$

est nul ou de degré inférieur à $N-1$.

Le raisonnement se poursuit de proche en proche. L'ensemble des constantes qui appartiennent à l'idéal $\mathfrak{m}$ est, dans A , un idéal, pouvant bien entendu se réduire à l'idéal zéro, mais qui admet dans tous les cas une base finie :

$$\mathfrak{d} = (d_1, \dots, d_l),$$

où d_i , considéré comme élément de $A[x]$, appartient à $\mathfrak{m}$.

Cela posé, si $f(x)$ est un polynôme quelconque de l'idéal $\mathfrak{m}$, nous avons :

$$f(x) \in (\alpha_1(x), \dots, \alpha_h(x), \beta_1(x), \dots, \beta_k(x), \dots, d_1, \dots, d_l),$$

donc, en désignant par $\mathfrak{m}'$ l'idéal du second membre :

$$\mathfrak{m} \subseteq \mathfrak{m}'.$$

Mais, comme chaque polynôme de base de $\mathfrak{m}'$ appartient à $\mathfrak{m}$, nous avons aussi

$$\mathfrak{m}' \subseteq \mathfrak{m},$$

d'où

$$\mathfrak{m} = \mathfrak{m}'$$

et, par conséquent, $\mathfrak{m}$ admet une base finie.

Remarque⁽¹⁾. — Inversement, si $A (\neq \{0\})$ est un domaine d'intégrité noethérien tel que l'anneau $A[x]$ soit, lui aussi, noethérien, A possède un élément-unité.

Soit a un élément non nul de A . Les polynômes

$$ax, ax^2, \dots, ax^n, \dots$$

engendrent un idéal $\mathfrak{m}$ qui possède une base finie, par conséquent les ax^n s'expriment sous forme de combinaisons d'un nombre fini d'entre eux, dont nous désignons par p le degré maximum : nous avons

$$ax^n = \sum_{i=1}^p [P_i(x) ax^i + n_i ax^i],$$

où $P_i(x) \in A[x]$ et $n_i \in \mathbb{C}$, $\mathbb{C}$ désignant l'anneau des entiers; il en résulte, en prenant $n > p$,

$$a = \sum_{i=1}^p r_i a, \quad (r_i \in A).$$

L'idéal principal (a) est donc contenu dans l'idéal Aa et, par conséquent, coïncide avec lui :

$$(a) = Aa,$$

⁽¹⁾ Communiquée par M. Kuntzmann.

ce qui entraîne une égalité de la forme

$$a = ea \quad (\neq 0) \quad (e \in A - \{0\}).$$

Puisque $A - \{0\}$ est un *semi-groupe* multiplicatif, e est élément-unité de $A - \{0\}$ et, par conséquent, de A .

Le théorème précédent s'applique de proche en proche aux anneaux

$$A[x_1], \quad A[x_1, x_2] = A[x_1][x_2], \quad \dots, \quad A[x_1, x_2, \dots, x_n].$$

Par conséquent, *si dans un anneau A possédant un élément-unité, tout idéal admet une base finie, tout idéal de l'anneau*

$$A[x_1, x_2, \dots, x_n]$$

admet également une base finie.

On en déduit aisément un énoncé un peu différent, qui est précisément celui de Hilbert : *dans tout sous-ensemble E de l'anneau*

$$R = A[x_1, x_2, \dots, x_n],$$

on peut trouver des éléments $\varphi_1, \varphi_2, \dots, \varphi_k$ tels que tout élément $f \in E$ puisse se mettre sous la forme

$$(1) \quad f = \lambda_1 \varphi_1 + \dots + \lambda_k \varphi_k, \quad \lambda_i \in R, \quad \varphi_i \in E.$$

Considérons, en effet, l'idéal $\mathfrak{m}$ engendré par l'ensemble E . Cet idéal admet, dans R , une base finie

$$\mathfrak{m} = (\psi_1, \dots, \psi_\mu)$$

et, d'après la définition de $\mathfrak{m}$, chaque élément de cette base, ψ_1 par exemple, est de la forme

$$\psi_1 = \gamma_1 \varphi_1 + \dots + \gamma_\nu \varphi_\nu, \quad \text{où } \gamma_i \in R, \quad \varphi_i \in E.$$

Si nous désignons par $\varphi_1, \dots, \varphi_\nu, \dots, \varphi_k$ l'ensemble des éléments de E ainsi introduits, nous avons, pour tout élément de $\mathfrak{m}$, donc en particulier pour tout élément de E , une représentation de la forme (1).

Les propositions précédentes s'appliquent notamment :

1° Au cas où A est l'anneau des entiers, puisque nous savons que, dans cet anneau, tout idéal est principal ;

2° Au cas où A est un corps quelconque K , puisque les seuls idéaux d'un corps sont (0) et (1) , c'est-à-dire deux idéaux principaux. En appliquant de proche en proche le théorème de la base finie, on voit que dans l'anneau $K[x_1, \dots, x_n]$ des polynômes à n variables sur un corps K , tout idéal admet une base finie.

Le théorème de Hilbert est ce qu'on appelle en Algèbre un *théorème de transfert*, c'est-à-dire une proposition permettant (avec, éventuellement, quelque condition supplémentaire, comme ici l'existence d'un élément-unité), d'affirmer qu'une propriété appartenant à un certain ensemble D appartient aussi à toute extension D' de D obtenue par un procédé déterminé.

La propriété d'être noethérien, pour un anneau A possédant un élément-unité, peut être transférée, non seulement aux anneaux de polynômes $A[x_1, \dots, x_n]$, mais aussi à l'anneau des séries entières formelles $A[[x_1, \dots, x_n]]$ ⁽¹⁾.

On appelle *série entière formelle* à n variables $x_1, \dots, x_n$ sur un anneau A toute somme formelle

$$F = \sum a_{\alpha_1, \dots, \alpha_n} x_1^{\alpha_1} \dots x_n^{\alpha_n}.$$

(où les α_i sont des entiers positifs ou nuls), dont les coefficients $a_{\alpha_1, \dots, \alpha_n}$ appartiennent à A : deux telles sommes F et F' sont égales si elles ont mêmes coefficients : $a_{\alpha_1, \dots, \alpha_n} = a'_{\alpha_1, \dots, \alpha_n}$, et seulement dans ce cas. Les séries entières formelles s'ajoutent terme à terme; le produit de deux d'entre elles s'obtient, de la façon habituelle, en multipliant chaque monome de l'une par chaque monome de l'autre et en ajoutant entre eux les monomes obtenus dans lesquels les exposants sont les mêmes. Avec ces règles de calcul, l'ensemble des séries entières formelles est un *anneau*, désigné par

$$A[[x_1, \dots, x_n]] = S.$$

Il contient comme sous-anneau l'anneau de polynomes

$$A[x_1, \dots, x_n] = R.$$

Considérons l'idéal $\mathfrak{X}$ engendré dans S par $x_1, \dots, x_n$. Les éléments de $\mathfrak{X}^m$ sont les séries entières qui ne contiennent aucun monome de degré $d = \alpha_1 + \dots + \alpha_n$ inférieur à m : nous avons donc

$$\bigcap_{m=1}^{\infty} \mathfrak{X}^m = \{0\}.$$

Si une série entière F non nulle appartient à $\mathfrak{X}^d$, mais non à $\mathfrak{X}^{d+1}$

(1) Cf. C. CHEVALLEY, *On the theory of local rings* [Annals of Math., t. 44, 1943, p. 696 (lemme 8)].

(avec la convention que $\mathfrak{X}^0$ est confondu avec S), il existe un polynome homogène F^* de degré d et un seul tel que

$$F - F^* \in \mathfrak{X}^{d+1}; \quad .$$

F^* est appelé *forme initiale* de F .

Cela posé, soit $\mathfrak{a}$ un idéal différent de (0) dans l'anneau S . Les formes initiales des éléments non nuls de $\mathfrak{a}$ engendrent un idéal homogène $\mathfrak{a}^*$ ⁽¹⁾ de l'anneau $R = A[x_1, \dots, x_n]$; R étant noethérien d'après le théorème de Hilbert, $\mathfrak{a}^*$ admet une base finie $(F_1^*, \dots, F_r^*)$; chaque F_i^* est la forme initiale, d'un certain degré d_i , d'une série $F_i \in \mathfrak{a}$. Une forme $F^* \neq 0$ de degré d dans $\mathfrak{a}^*$ vérifie une égalité

$$F^* = \sum_{i=1}^r M_i F_i^*,$$

où chaque M_i est une forme de degré $d - d_i$ ($M_i = 0$ si $d < d_i$): F^* est donc la forme initiale de la série

$$\sum_{i=1}^r M_i F_i \in \mathfrak{a}.$$

Soit G un élément quelconque de $\mathfrak{a}$. Définissons par induction r suites

$$\{G_{i,0}, G_{i,1}, \dots, G_{i,n}, \dots\} \quad (i = 1, \dots, r),$$

en posant d'abord $G_{i,0} = 0$, puis, les éléments $G_{i,k}$ étant supposés définis pour $k < m$, en formant l'élément

$$H_m = G - \sum_{k=0}^{m-1} \sum_{i=1}^r G_{i,k} F_i \in \mathfrak{a}, \quad (H_1 = G).$$

Si cet élément H_m est nul, nous posons

$$G_{i,m} = 0 \quad (i = 1, \dots, r).$$

Dans le cas contraire, H_m a une forme initiale de degré l_m que nous pouvons écrire

$$\sum_{i=1}^r G_{i,m} F_i^*,$$

(1) Un idéal de polynomes est dit *homogène* s'il contient, en même temps qu'un polynome $\varphi = \Phi_0 + \Phi_1 + \dots + \Phi_v + \dots$ chacune de ses parties homogènes, Φ_v , somme de tous les monomes de degré v figurant dans φ . Un idéal engendré par des formes a évidemment cette propriété.

où chaque $G_{i,m}$ est une forme de degré $l_m - d_i$ ($G_{i,m} = 0$ si $l_m < d_i$). S'il arrive, pour une valeur de m , que tous les $G_{i,m}$ soient nuls, G appartient à l'idéal engendré par $F_1, \dots, F_r$ dans S . Dans le cas contraire, nous avons

$$l_{m+1} > l_m$$

pour chaque valeur de m , d'où

$$\lim_{m \rightarrow \infty} l_m = \infty,$$

$\sum_{m=0}^{\infty} G_{i,m}$ est alors une série formelle G_i , et comme nous avons

$$G = \sum G_i F_i,$$

G appartient encore à l'idéal engendré par $F_1, \dots, F_r$ dans S : α se confond avec cet idéal, et l'anneau S est noethérien ⁽¹⁾.

Donnons maintenant un exemple d'anneau (commutatif) non noethérien. Considérons un corps K et un ensemble dénombrable de variables $x_1, \dots, x_n, \dots$. Soit A l'ensemble des polynômes par rapport à un nombre fini quelconque (changeant de l'un à l'autre) de variables prises parmi les x_i , ces polynômes ayant de plus leurs coefficients dans K . Deux de ces polynômes, P, Q , peuvent être ajoutés et multipliés comme dans l'anneau des polynômes dépendant des variables qui figurent dans P ou Q , et ayant leurs coefficients dans K . A est donc un anneau commutatif et même un domaine d'intégrité.

Les idéaux $(x_1), (x_1, x_2), \dots, (x_1, x_2, \dots, x_n), \dots$ forment une chaîne strictement croissante illimitée : A n'est donc pas noethérien. On notera que A contient les anneaux noethériens $K[x_1, \dots, x_n]$ et est contenu dans son corps des quotients, qui est aussi un anneau noethérien.

Considérons un anneau de polynômes à une seule variable $A[x]$, l'anneau A admettant un élément-unité. Quand A contient des diviseurs de zéro, des polynômes peuvent être inversibles dans $A[x]$. Si, par exemple, A est l'anneau des classes résiduelles modulo 4, on a

$$(2x + 1)^2 = 1.$$

(¹) Pour deux autres propriétés générales concernant les anneaux noethériens, voir chap. IV, § 13, exercice p. 208, et chap. V, § 7, p. 284.

Supposons, au contraire, que A soit un *domaine d'intégrité*. Alors, le degré $m(\alpha)$ du polynome α vérifie la relation

$$m(\alpha\beta) = m(\alpha) + m(\beta) \geq m(\alpha),$$

donc satisfait à la première condition imposée à la fonction g des anneaux euclidiens. D'après la même relation, les unités du domaine d'intégrité $A[x]$ sont nécessairement des constantes : ce sont donc les unités de A .

Un polynome est dit *irréductible sur A* s'il est un élément premier de $A[x]$, donc s'il est *indécomposable dans $A[x]$* et *non égal à une unité*. A étant un domaine d'intégrité, cette dernière condition est remplie d'elle-même pour tout polynome de degré non nul. Tout polynome du premier degré sur un corps est évidemment irréductible.

Exemple. — Γ désignant le corps des nombres rationnels, le polynome $x^2 - 2$ est irréductible sur Γ ; autrement, il existerait un nombre rationnel de carré égal à 2, ce qui est impossible. Mais le même polynome est réductible sur le corps $\mathbf{P}$ des nombres réels

$$x^2 - 2 = (x + \sqrt{2})(x - \sqrt{2}).$$

L'anneau A étant seulement assujéti à la condition d'avoir un *élément-unité*, considérons dans $A[x]$ deux polynomes

$$\alpha(x) = a_0x^m + \dots + a_m, \quad \beta(x) = b_0x^n + \dots + b_n \quad (a_0 \neq 0, b_0 \neq 0).$$

Si le coefficient b_0 de la plus haute puissance de x dans $\beta(x)$ est une unité de A , on peut trouver dans $A[x]$ deux polynomes $q(x)$ et $r(x)$ vérifiant l'égalité

$$\alpha(x) = \beta(x) \cdot q(x) + r(x), \quad \text{avec } \text{degré de } r < n$$

(*identité de la division*). Les polynomes $q(x)$, $r(x)$, appelés respectivement *quotient* et *reste*, sont déterminés d'une manière unique.

Si m est inférieur à n , il suffit de prendre $q = 0$, $r = \alpha$. Supposons donc $m \geq n$. Si nous posons $c_0 = a_0 b_0^{-1}$, le polynome

$$\alpha(x) - c_0 x^{m-n} \beta(x) = \alpha_1(x)$$

est de degré m_1 au plus égal à $m - 1$. En répétant l'application de ce procédé, on forme bien un polynome $q(x) = c_0 x^{m-n} + \dots$ tel que la différence $\alpha(x) - q(x) \beta(x) = r(x)$ ait un degré inférieur à n .

Soit q' , r' un autre système de polynomes vérifiant l'identité de la division. On a

$$\beta(q - q') = r' - r.$$

L'unité b_0 n'est pas diviseur de zéro; donc, si le premier membre n'est pas nul, son degré est égal à $n + \nu \geq n$, ν désignant le degré de $q - q'$. Mais le degré du second membre est certainement inférieur à n . Par conséquent, l'égalité précédente ne peut avoir lieu que si les deux membres sont nuls : $q = q'$, $r = r'$.

La division avec reste intervient notamment dans les deux cas suivants :

1° Le coefficient b_0 de la plus haute puissance de x dans le diviseur $\beta(x)$ est égal à 1. En particulier, $\beta(x)$ est de la forme $x - a$: dans ce dernier cas, le reste r est une constante, évidemment égale à $\alpha(a)$.

2° L'anneau A est un corps K . Tout élément non nul est alors une unité; par conséquent, la division avec reste est possible dès que le polynôme diviseur $\beta(x)$ n'est pas nul. Dans ces conditions, le degré $m(\alpha)$ est une fonction qui possède la deuxième propriété imposée à la fonction g des anneaux euclidiens. Comme nous avons vu qu'elle possède aussi la première, nous avons la proposition suivante :

THÉOREME. — L'anneau $K[x]$ des polynômes à une variable sur un corps K est un anneau euclidien.

COROLLAIRES. — 1. Dans l'anneau $K[x]$, tout idéal est principal.

2. Dans l'anneau $K[x]$, tout polynôme est le produit d'un nombre fini de polynômes irréductibles, définis à des unités, c'est-à-dire à des facteurs constants, près.

3. La condition nécessaire et suffisante pour que, dans l'anneau $R = K[x]$, un idéal (f) , non nul et différent de R , soit premier, est que le polynôme générateur f soit irréductible.

En outre, on peut définir dans $K[x]$, le p. g. c. d. de deux polynômes et le calculer par l'algorithme d'Euclide. Pour que deux polynômes $f(x)$ et $g(x)$ soient premiers entre eux, il faut et il suffit que l'on puisse déterminer deux polynômes $u(x)$, $v(x)$ de $K[x]$, tels que l'on ait l'identité de Bezout

$$u(x)f(x) + v(x)g(x) = 1.$$

D'après cette condition, deux polynômes de $K[x]$ premiers entre eux, restent premiers entre eux quand on les regarde comme polynômes de $\Omega[x]$, Ω étant un sur-corps quelconque de K .

Considérons maintenant un anneau de polynômes à n variables

$$R_n = A[x_1, x_2, \dots, x_n],$$

où A est un anneau commutatif possédant un élément-unité. Appelons point et désignons par $(a_1, a_2, \dots, a_n)$ un système de valeurs a_i appartenant à cet anneau ⁽¹⁾.

L'ensemble des polynômes $f(x_1, x_2, \dots, x_n)$ de R_n nuls en un point donné $(a_1, a_2, \dots, a_n)$,

$$f(a_1, a_2, \dots, a_n) = 0,$$

est visiblement un idéal α dans R_n .

Considérons, d'autre part, l'idéal

$$\alpha' = (x_1 - a_1, x_2 - a_2, \dots, x_n - a_n).$$

Puisque chaque polynôme de base de α' s'annule au point considéré, nous avons

$$(2) \quad \alpha' \subseteq \alpha.$$

Nous allons montrer que les idéaux α' et α coïncident.

La congruence modulo un idéal étant une équivalence régulière par rapport à l'addition et à la multiplication, les relations

$$x_i \equiv a_i \quad (\alpha') \quad (i = 1, 2, \dots, n)$$

entraînent, pour tout polynôme $f \in R_n$,

$$f(x_1, x_2, \dots, x_n) \equiv f(a_1, a_2, \dots, a_n) \quad (\alpha'),$$

c'est-à-dire

$$(3) \quad f(x_1, x_2, \dots, x_n) = (x_1 - a_1)f_1 + \dots + (x_n - a_n)f_n + f(a_1, a_2, \dots, a_n),$$

où les f_i sont des polynômes. Si f appartient à l'idéal α , on a

$$f(a_1, a_2, \dots, a_n) = 0$$

et, par conséquent,

$$f(x_1, x_2, \dots, x_n) \in \alpha', \quad \text{d'où} \quad \alpha \subseteq \alpha'$$

et, d'après (2),

$$\alpha = \alpha'.$$

Nous avons donc la proposition suivante :

⁽¹⁾ Voir Note IV, en particulier p. 446, note ⁽¹⁾.

THÉOREME. — Dans l'anneau $R_n = A[x_1, x_2, \dots, x_n]$, où A est un anneau possédant un élément-unité, l'idéal

$$(x_1 - a_1, x_2 - a_2, \dots, x_n - a_n) \quad (a_i \in A)$$

est l'ensemble de tous les polynômes nuls au point $(a_1, a_2, \dots, a_n)$.

COROLLAIRE. — Dans l'anneau $A[x]$, où A est un anneau possédant un élément-unité, l'ensemble de tous les polynômes nuls pour $x = a$ ($a \in A$), est l'idéal principal $(x - a)$.

Remarque. — Dans le cas des polynômes à une seule variable, l'égalité (3), qui s'écrit

$$(3') \quad f(x) = (x - a)f_1(x) + f(a)$$

est celle de la division avec reste de $f(x)$ par $x - a$: elle peut être écrite directement, et le corollaire en résulte.

Précisons maintenant la manière dont les propriétés de l'idéal $\mathfrak{a}$ dépendent de celles de l'anneau A .

La correspondance

$$f(x_1, x_2, \dots, x_n) \rightarrow f(a_1, a_2, \dots, a_n)$$

est une application univoque de R_n sur A , car un élément $c \in A$ est en particulier l'image du polynome $c \in R_n$. De plus, cette application est un homomorphisme : $R_n \sim A$. Or, l'ensemble des éléments de R_n auxquels correspond zéro dans A est, par définition, l'idéal $\mathfrak{a}$. Nous avons donc, d'après le théorème d'homomorphisme pour les anneaux, l'isomorphisme

$$R_n/\mathfrak{a} \simeq A.$$

Cet isomorphisme entraîne les deux propositions suivantes :

Si A est un domaine d'intégrité (possédant un élément-unité), l'idéal

$$\mathfrak{a} = (x_1 - a_1, x_2 - a_2, \dots, x_n - a_n)$$

dans l'anneau $A[x_1, x_2, \dots, x_n]$, est premier.

Dans l'anneau $K[x_1, x_2, \dots, x_n]$, où K désigne un corps, l'idéal

$$\mathfrak{a} = (x_1 - a_1, x_2 - a_2, \dots, x_n - a_n)$$

est un idéal sans diviseurs (et, par conséquent, premier).

Exemples. — 1. Si $A = C_i$, où C_i désigne l'anneau des classes résiduelles

modulo 4, l'idéal (x) , dans l'anneau $A[x]$, n'est pas premier. On a, par exemple,

$$2 \not\equiv 0 \pmod{(x)}, \quad x - 2 \not\equiv 0 \pmod{(x)} \quad \text{et} \quad 2(x - 2) = 2x \equiv 0 \pmod{(x)}.$$

2. Dans l'anneau $C[x, y]$, où C est l'anneau des entiers, l'idéal $\mathfrak{p} = (x, y)$ est *premier*; mais il admet, par exemple, comme diviseur véritable l'idéal $(3, x, y)$, ensemble des polynômes dont le terme constant est multiple de 3.

3. Dans l'anneau $\Gamma[x, y]$, où Γ désigne le corps des nombres rationnels, l'idéal $\mathfrak{p} = (x, y)$ est sans diviseurs.

4. Dans le même anneau $\Gamma[x, y]$, considérons l'idéal $\mathfrak{q} = (x^2, y)$. En posant $\mathfrak{p} = (x, y)$, nous avons

$$\mathfrak{p}^2 = (x^2, xy, y^2) \subset \mathfrak{q} \subset \mathfrak{p}.$$

Comme $\mathfrak{p}$ est sans diviseurs, l'idéal $\mathfrak{p}$ est *primaire* et appartient à $\mathfrak{p}$; mais $\mathfrak{q}$ n'est égal à aucune puissance de $\mathfrak{p}$. En outre, $\mathfrak{q}$ est *indécomposable*, c'est-à-dire n'est pas le produit de deux véritables diviseurs de $\mathfrak{q}$.

Plus généralement, dans l'anneau $K[x_1, x_2, \dots, x_n]$, où K est un corps quelconque, tout idéal $\mathfrak{q}$ vérifiant une relation de la forme

$$\mathfrak{a}^2 \subseteq \mathfrak{q} \subseteq \mathfrak{a}, \quad \text{où} \quad \mathfrak{a} = (x_1 - a_1, \dots, x_n - a_n)$$

est *primaire* et appartient à l'idéal *premier* $\mathfrak{a}$.

5. Il existe, dans certains anneaux de polynômes, des *puissances d'idéaux premiers qui ne sont pas primaires*. Dans l'anneau $R = C[x]$ des polynômes à coefficients entiers, considérons le sous-anneau S des polynômes de la forme

$$f(x) = a_0 + a_1 px + a_2 x^2 + \dots + a_n x^n \quad (a_i \in C),$$

p étant un nombre entier donné ($p \neq 1$). Modulo l'idéal

$$\mathfrak{p} = (px, x^2),$$

tout polynôme $f \in S$ est congru à son terme constant a_0 et, comme aucune constante non nulle n'appartient à $\mathfrak{p}$, nous avons l'isomorphisme d'anneaux ⁽¹⁾

$$S/\mathfrak{p} \simeq C.$$

L'idéal $\mathfrak{p}$ est donc *premier* dans S . Cela posé, nous avons

$$\mathfrak{p}^2 = (p^2 x^2, px^3, x^4),$$

donc

$$p^2 x^2 \equiv 0 \pmod{(\mathfrak{p}^2)}, \quad x^2 \not\equiv 0 \pmod{(\mathfrak{p}^2)}, \quad px^3 \not\equiv 0 \pmod{(\mathfrak{p}^2)}$$

quel que soit l'entier p ; l'idéal $\mathfrak{p}^2$ n'est donc pas *primaire*.

⁽¹⁾ Ou encore, l'application $f \rightarrow a_0$ est un homomorphisme d'anneaux

$$S \sim C$$

et l'ensemble des éléments de S ayant 0 pour image dans C est l'idéal $\mathfrak{p}$: on a donc, d'après le théorème d'homomorphisme,

$$S/\mathfrak{p} \simeq C.$$

Exercices. — 1. Γ désignant le corps des nombres rationnels et m étant un élément de Γ , de quelle forme sont les polynômes $\alpha(x)$ de l'anneau $\Gamma[x]$ tels que l'on ait $\alpha(+1) = m$, $\alpha(-1) = -m$?

2. Dans l'anneau $\Gamma[x, y]$, l'ensemble des polynômes nuls aux points A et A' de coordonnées $x = \pm 1$, $y = 0$, est un idéal α . Déterminer une base de α . Soit $\mathfrak{b}$ l'idéal des polynômes nuls aux points B et B' de coordonnées $x = 0$, $y = \pm 1$. Quel est l'idéal $\mathfrak{m}$ des polynômes nuls aux quatre points A, A', B, B' ? Déterminer une base de l'idéal $\mathfrak{m}$; montrer qu'on peut trouver pour cet idéal une base comprenant deux polynômes du second degré.

3. A étant l'anneau des classes résiduelles modulo 4, l'idéal (x) , dans l'anneau $R = A[x]$, est primaire.

4. Étant donné un corps K , on considère dans l'anneau $K[x]$ deux polynômes f et g de degrés m et n , premiers entre eux. Tous les polynômes $u, v \in K[x]$ et vérifiant l'identité de Bezout

$$uf + vg = 1$$

s'expriment en fonction de deux d'entre eux, u_0, v_0 , par les formules

$$u = u_0 + qg, \quad v = v_0 - qf, \quad q \in K[x].$$

En déduire qu'il existe un couple de polynômes u, v tel que u soit de degré $n-1$ au plus, v de degré $m-1$ au plus.

5. Dans l'anneau $\Gamma[x, y]$, où Γ désigne le corps des nombres rationnels, on considère les idéaux

$$\alpha = (x, y), \quad \mathfrak{m}_1 = (x^2, y^2), \quad \mathfrak{m}_2 = (xy).$$

Déterminer et comparer les idéaux

$$\alpha(\mathfrak{m}_1 \cap \mathfrak{m}_2) \quad \text{et} \quad (\alpha\mathfrak{m}_1) \cap (\alpha\mathfrak{m}_2)$$

(F. S. MACAULAY, *Alg. Theory of modular Systems*, Cambridge Tracts, 19, p. 31).

6. Décomposition des polynômes. — Soit $\mathfrak{o}$ un domaine d'intégrité possédant un élément-unité, et à factorisation unique. Nous nous proposons d'établir que le domaine d'intégrité $\mathfrak{o}[x]$ des polynômes en x à coefficients dans $\mathfrak{o}$ est également un domaine à factorisation unique ⁽¹⁾. Pour obtenir ce résultat, nous considérerons le corps des quotients, K , de $\mathfrak{o}$; le domaine d'intégrité $\mathfrak{o}[x]$ est contenu dans l'anneau $K[x]$ qui est euclidien, donc à factorisation unique; de la décomposition dans $K[x]$ d'un polynôme $f(x)$ de $\mathfrak{o}[x]$, nous passerons à sa décomposition dans $\mathfrak{o}[x]$. Rappelons que les unités de $K[x]$ sont celles de K , c'est-à-

⁽¹⁾ Cette proposition fondamentale constitue un *théorème de transfert*, qui justifie le fait qu'on regarde comme un *axiome* la propriété de factorisation unique.

dire tous les éléments $\frac{r}{s}$ non nuls de $K(r, s \in \mathfrak{o})$, et que les unités de $\mathfrak{o}[x]$ sont celles de $\mathfrak{o}$: nous les désignerons par $\varepsilon, \varepsilon', \dots$

Soit

$$f(x) = a_0 + a_1x + \dots + a_nx^n \quad (a_i \in \mathfrak{o})$$

un polynôme de $\mathfrak{o}[x]$. Nous appellerons *facteur constant* de ce polynôme un p. g. c. d. a de ses coefficients $a_0, a_1, \dots, a_n$. Si les coefficients a_i sont sans diviseurs communs, donc si $f(x)$ n'admet pas d'autres facteurs constants que les unités, le polynôme $f(x)$ est dit *primitif*. Nous désignerons les polynômes primitifs par $f^*, g^*, \dots$. Tout polynôme associé à un polynôme primitif est primitif; les polynômes primitifs de degré nul sont les unités.

Tout polynôme $f(x)$ est le produit d'un facteur constant par un polynôme primitif

$$(1) \quad f(x) = af^*(x) \quad (a \in \mathfrak{o})$$

et d'après la définition de a , cette décomposition est unique à des unités près. Une égalité de la forme

$$(2) \quad af^*(x) = bg^*(x), \quad \text{où } a, b \in \mathfrak{o}$$

entraîne donc

$$b = a\varepsilon \quad \text{et} \quad f^*(x) = \varepsilon g^*(x).$$

La décomposition (1) est *triviale* si a est une unité, donc si f est primitif, et seulement dans ce cas. Donc, pour qu'un polynôme de degré positif soit premier dans $\mathfrak{o}[x]$, une première condition nécessaire est qu'il soit primitif ⁽¹⁾.

*Le produit f^*g^* de deux polynômes primitifs — et par conséquent aussi le produit de r polynômes primitifs — est un polynôme primitif.* Supposons, en effet, que ce produit admette un facteur constant h non égal à une unité; $\mathfrak{o}$ étant un anneau à factorisation unique, h admet au moins un diviseur premier p ; tous les coefficients du produit f^*g^* seraient divisibles par p , tandis qu'au moins un coefficient de f^* et au moins un coefficient de g^* ne le seraient pas, puisque ces polynômes sont primitifs : cette circonstance est impossible, d'après le lemme suivant, qui nous sera encore utile ailleurs.

(1) Cette condition n'est évidemment pas suffisante : $x^2 - 1 = (x + 1)(x - 1)$ est primitif, mais non premier, dans $\mathbb{C}[x]$. Nous obtiendrons un peu plus loin la condition nécessaire et suffisante pour qu'un polynôme soit premier.

LEMME 1. — Soient

$$f(x) = a_0 + a_1x + \dots + a_mx^m, \quad g(x) = b_0 + b_1x + \dots + b_nx^n$$

deux polynomes de $\mathfrak{o}[x]$, et p un élément premier de $\mathfrak{o}$. Si p divise $a_0, \dots, a_{i-1}, b_0, \dots, b_{j-1}$ sans diviser a_i, b_j ($0 \leq i \leq m, 0 \leq j \leq n$), le coefficient c_{i+j} de x^{i+j} dans le produit $f(x)g(x)$ n'est pas divisible par p .

On a, en effet,

$$c_{i+j} = (a_0b_{i+j} + \dots + a_{i-1}b_{j+1}) + a_ib_j - (a_{i+1}b_{j-1} + \dots + a_{i+j}b_0),$$

et p divise chacune des deux parenthèses. S'il divisait c_{i+j} , il devrait diviser le produit a_ib_j , ce qui est impossible puisqu'il est premier et ne divise ni a_i ni b_j .

COROLLAIRE. — Tout élément premier p de $\mathfrak{o}$ est premier au sens strict dans $\mathfrak{o}[x]$.

Supposons que la constante p divise le produit fg , donc tous les c_i , et ne divise pas g . Soit b_j le premier coefficient de g non divisible par p : si les coefficients a_i de f n'étaient pas tous multiples de p , nous aurions, d'après le lemme 1, une contradiction.

Considérons maintenant un polynome non nul de $K[x]$

$$\Phi(x) = x_0 + x_1x + \dots + x_nx^n, \quad x_i = \frac{r_i}{s_i}, \quad r_i, s_i \in \mathfrak{o}.$$

En réduisant les x_i au même dénominateur, nous pouvons mettre $\Phi(x)$ sous la forme du quotient d'un polynome de $\mathfrak{o}[x]$ par un élément b de $\mathfrak{o}$. En mettant en évidence au numérateur le facteur constant et le polynome primitif, nous obtenons

$$(3) \quad \Phi(x) = \frac{a}{b} F^*(x),$$

où $F^* \in \mathfrak{o}[x]$ est de degré égal à celui de Φ .

Considérons un polynome $\Psi(x) = \frac{u}{v} \Phi(x)$, ($u, v \in \mathfrak{o}$) égal au produit de Φ par une unité de K , et soit

$$(3') \quad \Psi(x) = \frac{r}{s} G^*(x)$$

la décomposition analogue à celle de Φ . Nous avons

$$vbrG^*(x) = uasF^*(x),$$

d'où

$$F^*(x) = \varepsilon G^*(x),$$

où ε est une unité de $\mathfrak{o}$. Par conséquent, à tout polynôme $\Phi(x)$ de $K[x]$ correspond par la formule (3) un polynôme primitif $F^*(x) \in \mathfrak{o}[x]$ et si deux polynômes Φ, Ψ sont associés dans $K[x]$, les polynômes correspondants F^*, G^* sont associés dans $\mathfrak{o}[x]$. En particulier, dans (3), F^* est défini à une unité près.

Cela posé, considérons dans $\mathfrak{o}[x]$ un polynôme primitif $f^*(x)$ de degré positif, et supposons qu'il soit décomposable dans $K[x]$

$$(4) \quad f^*(x) = \Phi_1(x) \dots \Phi_r(x),$$

où $\Phi_1, \dots, \Phi_r$ sont des polynômes de degrés $n_1, \dots, n_r$ positifs.

LEMME 2. — *Le polynôme considéré f^* est décomposable dans $\mathfrak{o}[x]$ en un produit de r polynômes primitifs, de degrés $n_1, \dots, n_r$.*

Nous avons, en effet,

$$(5) \quad \Phi_i(x) = \frac{a_i}{b_i} F_i^*(x),$$

où $F_i^*(x) \in \mathfrak{o}[x]$ est de degré n_i et primitif. Il en résulte

$$b_1 \dots b_r f^*(x) = a_1 \dots a_r F_1^*(x) \dots F_r^*(x)$$

et, puisque le produit $F_1^* \dots F_r^*$ est primitif,

$$(6) \quad f^*(x) = F_1^*(x) \dots F_r^*(x)$$

(en faisant rentrer le facteur ε éventuel dans F_1^* , par exemple).

Une première conséquence de ce lemme est la proposition connue sous le nom de lemme ou théorème de Gauss.

THÉORÈME DE GAUSS. — *Si, pour un polynôme*

$$f(x) = a_0 + a_1 x + \dots + x^n$$

de l'anneau $\mathfrak{o}[x]$, dans lequel le coefficient de la plus haute puissance de x est égal à 1 (élément-unité de $\mathfrak{o}$), on a, dans $K[x]$, la décomposition

$$f(x) = \Phi_1(x) \Phi_2(x), \quad \text{où } \Phi_i(x) \in K[x]$$

et si, dans chacun des polynômes Φ_1, Φ_2 le coefficient de la plus haute puissance de x est égal à 1, les polynômes Φ_1, Φ_2 appartiennent à $\mathfrak{o}[x]$.

Le polynome f étant primitif, le lemme 2 est valable; nous avons, par conséquent, d'après (6),

$$(6') \quad f(x) = F_1^*(x) F_2^*(x)$$

et les coefficients $\varepsilon_1, \varepsilon_2$ de la plus haute puissance de x dans F_1^* et dans F_2^* sont des unités : $\varepsilon_1 \varepsilon_2 = 1$. Comme ces polynomes ne sont définis à partir de Φ_1 et Φ_2 qu'à des unités près, nous pouvons ramener le coefficient de la plus haute puissance de x à être égal, dans chacun d'eux, à 1. Nous avons alors, dans les relations (5),

$$\frac{a_1}{b_1} = 1, \quad \frac{a_2}{b_2} = 1,$$

d'où

$$\Phi_1(x) = F_1^*(x) \in \mathfrak{o}[x], \quad \Phi_2(x) = F_2^*(x) \in \mathfrak{o}[x],$$

ce qu'il fallait démontrer.

Pour qu'un polynome $f(x)$, de degré positif, soit *premier dans* $\mathfrak{o}[x]$, il faut qu'il soit, comme nous l'avons vu, *primitif*, et aussi, d'après le lemme 2, *premier dans* $K[x]$. Nous allons montrer que cette double condition est aussi *suffisante*.

Soit, en effet, $f^*(x)$ un polynome primitif de $\mathfrak{o}[x]$, premier dans $K[x]$, et de degré positif. Soit une décomposition de la forme

$$(7) \quad f^* = f_1 f_2, \quad f_i \in \mathfrak{o}[x] \subseteq K[x].$$

L'un des facteurs, f_1 par exemple, est une unité dans $K[x]$, c'est-à-dire un polynome de degré zéro; comme $f_1 \in \mathfrak{o}[x]$, f_1 est une constante a de $\mathfrak{o}$, et nous avons, en décomposant f_2 en facteur constant et polynome primitif

$$f^* = a f_2 = a \cdot a_2 f_2^*.$$

Par suite, $a \cdot a_2$ est une unité de $\mathfrak{o}$, $a = f_1$ et a_2 en sont également, et la décomposition (7) est bien triviale. Nous avons ainsi établi la proposition suivante :

THÉORÈME 1. — *Pour qu'un polynome $f(x)$, de degré positif, soit premier dans $\mathfrak{o}[x]$, il faut et il suffit qu'il soit primitif, et premier dans $K[x]$.*

Quant aux constantes, pour qu'un élément $a \in \mathfrak{o}$ soit premier dans $\mathfrak{o}[x]$, il faut et il suffit évidemment qu'il soit premier dans $\mathfrak{o}$.

COROLLAIRE. — Pour qu'un polynome $f \in \mathfrak{o}[x]$, de degré positif, ne soit pas le produit de deux polynomes de degrés positifs appartenant à $\mathfrak{o}[x]$, il faut [et il suffit ⁽¹⁾] qu'il soit irréductible sur K .

Soit, en effet, $f = af^*$, où f^* est primitif. Pour que f ne soit pas le produit de deux polynomes de degrés positifs, il faut et il suffit que f^* soit premier dans $\mathfrak{o}[x]$, donc dans $K[x]$, donc, puisque a est une unité dans K , que f soit premier dans $K[x]$, c'est-à-dire irréductible sur K .

Nous pouvons maintenant établir le théorème fondamental.

THÉORÈME 2. — L'anneau $\mathfrak{o}[x]$ est un domaine à factorisation unique ⁽²⁾.

Soit $f(x) \in \mathfrak{o}[x]$. Nous avons

$$f(x) = af^*(x),$$

où la constante a et le polynome primitif f ne sont définis qu'à des unités de $\mathfrak{o}$ près. Dans l'anneau euclidien $K[x]$, décomposons $f^*(x)$ en facteurs premiers dans $K[x]$

$$f^*(x) = \Phi_1(x) \dots \Phi_h(x).$$

Nous avons, d'après le lemme 2,

$$f^*(x) = F_1^*(x) \dots F_h^*(x),$$

où chaque polynome $F_i^*(x)$, défini par

$$\Phi_i(x) = \frac{a_i}{b_i} F_i^*(x),$$

est primitif, et premier dans $K[x]$ comme Φ_i auquel il est associé dans $K[x]$. Donc les $F_i^*(x)$ sont premiers dans $\mathfrak{o}[x]$. Ils sont, d'autre part, définis chacun à une unité de $\mathfrak{o}$ près, puisque les Φ_i sont définis à une unité de K près.

Si enfin nous décomposons dans $\mathfrak{o}$ le facteur constant a en facteurs premiers,

$$a = p_1 \dots p_k,$$

où les p_i sont également définis à des unités près, nous obtenons pour f

⁽¹⁾ Que la condition soit suffisante est évident *a priori*.

⁽²⁾ On trouvera une autre démonstration de ce théorème dans le Mémoire de K. HENSEL, *Ueber eindeutige Zerlegung in Primelemente* (J. f. Math., t. 158, 1923, p. 195-198).

la décomposition

$$f = p_1 \dots p_k F_1^{\alpha_1}(x) \dots F_h^{\alpha_h}(x),$$

où chaque facteur est premier dans $\mathfrak{o}[x]$ et défini à une unité près, ce qu'il fallait démontrer.

On peut également démontrer le théorème 2 en utilisant le *théorème de Krull* caractérisant les anneaux à factorisation unique au moyen d'une fonction λ vérifiant la *condition de réduction* (§ 2, p. 314).

L'ensemble $\mathfrak{T}_1$ des polynômes primitifs de l'anneau $\mathfrak{o}[x]$ est multiplicativement fermé, comme on l'a vu (p. 344), et il est évident que tout diviseur d'un polynôme primitif est lui-même primitif. Prenons comme fonction $\lambda(f)$ le *degré* du polynôme f : les valeurs (≥ 0) de cette fonction λ ne s'accumulent qu'à l'infini, et l'on a $\lambda(f) \geq \lambda(g)$ si $g \mid f$, avec l'inégalité ou l'égalité suivant que g n'est pas ou est associé à f .

Pour montrer que λ vérifie la condition de réduction, il suffit de remarquer que, si

$$f(x) = a_0 x^\alpha + \dots, \quad g(x) = b_0 x^\beta + \dots$$

sont des polynômes primitifs, avec par exemple $\alpha \leq \beta$, on a

$$b_0 x^{\beta-\alpha} f(x) - a_0 g(x) = g_1(x),$$

où g_1 est un polynôme de degré $\beta_1 < \beta$. En appliquant au besoin le même procédé à f et g_1 , ou à g_1 et f , etc., on arrivera à une identité de la forme

$$u(x)f(x) + v(x)g(x) = h(x),$$

où $u, v \in \mathfrak{o}[x]$ et où h est de degré inférieur à $\text{Min}(\alpha, \beta)$ et de la forme

$$h(x) = r d(x),$$

où $r \in \mathfrak{o}$, et $d(x) \in \mathfrak{T}_1$. Comme tout élément $r \in \mathfrak{R}$ est premier à tout polynôme primitif, et puisque nous avons

$$\lambda(d) \leq \text{Min}[\lambda(f), \lambda(g)],$$

la condition de réduction est remplie, ce qui établit la *factorisation dans $\mathfrak{T}_1$* (décomposition de tout élément de $\mathfrak{T}_1$ en produit d'un nombre fini d'éléments premiers au sens strict).

Puisque tout polynôme non primitif de $\mathfrak{o}[x]$ est le produit de son facteur constant par un polynôme primitif, et puisque la décomposition du facteur constant dans $\mathfrak{o}$ est encore une décomposition en produit d'éléments premiers au sens strict dans $\mathfrak{o}[x]$ (corollaire du lemme 1,

p. 345), tout élément de l'anneau $\mathfrak{o}[x]$ est le produit d'un nombre fini d'éléments premiers au sens strict : $\mathfrak{o}[x]$ est donc un anneau à factorisation unique (§ 2, p. 313; voir aussi chap IV, § 14, th. 7).

Étant donné un domaine d'intégrité $\mathfrak{o}$ à factorisation unique, nous pouvons appliquer de proche en proche le théorème précédent aux anneaux $\mathfrak{o}[x_1]$, $\mathfrak{o}[x_1, x_2] = \mathfrak{o}[x_1][x_2]$, ..., $\mathfrak{o}[x_1, x_2, \dots, x_n]$. Nous obtenons ainsi l'importante proposition suivante :

THÉORÈME. — *Si $\mathfrak{o}$ est un anneau à factorisation unique, l'anneau $\mathfrak{o}[x_1, x_2, \dots, x_n]$ des polynômes à n variables sur $\mathfrak{o}$ est un anneau à factorisation unique.*

En particulier, les anneaux $\mathbb{C}[x_1, x_2, \dots, x_n]$, où $\mathbb{C}$ est l'anneau des entiers, et $\mathbb{K}[x_1, x_2, \dots, x_n]$, où $\mathbb{K}$ désigne un corps quelconque, sont à factorisation unique.

On remarquera que, pour $n \geq 2$, l'anneau $\mathbb{K}[x_1, x_2, \dots, x_n]$ (ou $\mathbb{C}[x_1, x_2, \dots, x_n]$) n'est certainement pas euclidien ⁽¹⁾, puisqu'il y existe des idéaux non principaux, (x_1, x_2) par exemple. On peut encore le voir en remarquant que les propriétés :

- I. f et g sont sans diviseurs communs,
- II. f est premier à g ,

équivalentes dans cet anneau, ne sont pas équivalentes à la propriété :

- III. f et g sont premiers entre eux ⁽²⁾.

Par exemple, x_1 et x_2 sont sans diviseurs communs, tandis qu'une identité de la forme

$$ux_1 + vx_2 = 1$$

est impossible, car la spécialisation $x_1 = 0$, $x_2 = 0$ entraînerait une absurdité.

De nombreux critères ont été donnés pour reconnaître si un polynôme

$$\varphi(x) = c_0 + c_1x + \dots + c_r x^r \in \mathfrak{o}[x],$$

⁽¹⁾ Voir également l'exercice 1.

⁽²⁾ Du point de vue de la Géométrie analytique (où $\mathbb{K}$ est ordinairement le corps des nombres complexes), la condition I ou II exprime que les variétés $f = 0$, $g = 0$ sont sans partie commune, tandis que la condition III exige que $f = 0$, $g = 0$ n'aient aucun point commun (ce qui, pour $n > 1$, serait en contradiction avec le théorème de Bezout sur l'intersection des courbes, surfaces, ..., variétés algébriques).

où $\mathfrak{o}$ est un domaine à factorisation unique, est *irréductible* ou non. L'un des plus connus est celui d'*Eisenstein*.

THÉOREME D'EISENSTEIN. — *S'il existe dans $\mathfrak{o}$ un élément premier p tel que l'on ait*

$$c_r \not\equiv 0 \pmod{p},$$

$$c_i \equiv 0 \pmod{p} \quad \text{pour } i = 0, 1, \dots, r-1,$$

et

$$c_0 \not\equiv 0 \pmod{p^2},$$

le polynôme $\varphi(x) = c_0 + c_1 x + \dots + c_r x^r$ n'est pas le produit de deux polynômes de degrés positifs appartenant à $\mathfrak{o}[x]$ [donc il est irréductible sur K , où K désigne le corps des quotients de $\mathfrak{o}$ ⁽¹⁾].

Supposons, en effet, que l'on ait

$$\varphi(x) = f(x)g(x),$$

avec

$$f(x) = a_0 + \dots + a_m x^m, \quad g(x) = b_0 + \dots + b_n x^n.$$

Les relations

$$c_0 = a_0 b_0, \quad c_0 \equiv 0 \pmod{p}, \quad c_0 \not\equiv 0 \pmod{p^2}$$

exigent qu'un et un seul des éléments a_0, b_0 soit multiple de p ; soit, par exemple, $a_0 \equiv 0 \pmod{p}$, $b_0 \not\equiv 0 \pmod{p}$.

D'autre part, $c_r = a_m b_n$ ($r = m + n$) n'est pas multiple de p , donc a_m ne l'est pas non plus, et si a_i désigne le premier coefficient de $f(x)$ qui n'est pas multiple de p , nous avons

$$i \leq m < r.$$

Mais alors, d'après le lemme 1, $c_{i+0} = c_i$ n'est pas multiple de p , ce qui constitue bien une contradiction.

Exemples et remarques. — 1. Les polynômes

$$f = x^2 - 5, \quad g = 3x^4 - 4x + 2$$

sont irréductibles dans $\mathbb{C}[x]$, $\mathbb{C}$ désignant l'anneau des entiers. Ils sont, en effet, primitifs, et irréductibles sur K d'après le critère d'Eisenstein ($p = 5$ pour f , $p = 2$ pour g).

Le polynôme

$$f(x) = x^r + p$$

est irréductible dans $\mathbb{C}[x]$ quel que soit son degré r et le nombre premier p .

(1) Voir le corollaire du théorème 1, p. 348.

2. Le critère d'Eisenstein n'est pas toujours directement applicable à un polynome

$$\varphi(x) = c_0 + \dots + c_r x^r.$$

Il ne l'est certainement pas quand l'un des coefficients c_i d'indice inférieur à r est égal à l'élément-unité de $\mathfrak{o}$. Mais alors on peut remarquer que $\varphi(x)$ et $\varphi(x+a)$, où a est une constante quelconque de $\mathfrak{o}$, sont irréductibles sur K en même temps l'un que l'autre : il peut arriver qu'un choix simple de a permette d'appliquer à $\varphi(x+a)$ le critère d'Eisenstein.

Considérons, par exemple, les polynomes

$$\varphi(x) = x^2 + 1, \quad \psi(x) = x^2 - 3x + 4.$$

Nous avons

$$\varphi(x+1) = x^2 + 2x + 2, \quad \psi(x-2) = x^2 - 7x + 14.$$

Le critère d'Eisenstein s'applique dans les deux cas, et φ et ψ sont irréductibles sur Γ , corps des nombres rationnels.

3. Dans le cas où le domaine des coefficients est l'anneau C des entiers, un procédé très simple pour reconnaître si un polynome $f(x)$ est irréductible et, lorsqu'il ne l'est pas, pour faciliter la recherche de ses diviseurs, consiste à considérer le polynome $\bar{f}(x)$ dont les coefficients sont respectivement les restes de ceux de $f(x)$, modulo 2,

$$\bar{f}(x) \equiv f(x) \pmod{2}.$$

Une décomposition

$$(8) \quad f(x) = f_1(x)f_2(x)$$

dans $C[x]$ entraîne

$$(8') \quad \bar{f}(x) = \bar{f}_1(x)\bar{f}_2(x).$$

Or, dans l'anneau $C_2[x]$, où $C_2 = \{0, 1\}$ est le corps des classes résiduelles modulo 2, il y a seulement un nombre fini, 2^{s+1} , de polynomes d'un degré donné s . Un nombre fini d'essais, dans lesquels on donnera seulement à s des valeurs au plus égales à la moitié du degré de f , permet donc de reconnaître si la décomposition (8') est possible. *Si elle ne l'est pas, (8) ne l'est pas non plus et f est irréductible.*

Soit, par exemple,

$$f(x) = x^3 + 3x - 1.$$

On a

$$\bar{f}(x) = x^3 + x + 1.$$

Si f était réductible, il admettrait un diviseur du premier degré; les deux seuls polynomes du premier degré dans $C_2[x]$ sont x et $x+1$: aucun d'eux ne divisant $\bar{f}$, f est irréductible. On aurait la même conclusion, par exemple, pour le polynome

$$x^3 + 3x + 3 \equiv x^3 + x + 1 \pmod{2},$$

auquel le critère d'Eisenstein s'applique.

S'il existe une décomposition (8'), elle indique, pour la décomposition *éventuelle* (8) correspondante, les degrés ⁽¹⁾ des facteurs f_1, f_2 et les classes résiduelles modulo 2 auxquelles leurs coefficients appartiennent. On peut alors obtenir des renseignements complémentaires en remplaçant 2 par 3 ou par un entier quelconque (ne divisant pas le coefficient de la plus haute puissance de x dans f); et en appliquant le même procédé.

Exercices. — 1. *a.* C étant l'anneau des entiers, montrer que les polynômes de l'anneau $C[x]$ qui ont pour terme constant un nombre pair forment un idéal m ; déterminer une base de m ; montrer que m n'est pas un idéal principal.

b. Dans l'anneau $C[x]$, les polynômes x et 2 sont sans diviseurs communs; sont-ils premiers entre eux?

c. L'anneau $C[x]$ est-il euclidien?

2. Si p est premier, le polynôme

$$f(x) = x^{p-1} + x^{p-2} + \dots + 1$$

est irréductible dans $C[x]$, C désignant l'anneau des entiers.

(¹) A condition que le coefficient de la plus haute puissance de x dans f ne soit pas multiple de 2.



CHAPITRE VII.

ÉQUATIONS ALGÈBRIQUES.

A. — RACINES.

1. Propriétés générales. — Une équation algébrique sur un anneau $\mathfrak{O}$ (supposé commutatif) est une relation de la forme

$$(1) \quad f(\alpha) = 0,$$

où

$$f(x) = a_0 + a_1 x + \dots + a_m x^m \in \mathfrak{O}[x]$$

est un polynome dont les coefficients appartiennent à $\mathfrak{O}$. *Résoudre* cette équation, c'est déterminer, dans l'anneau $\mathfrak{O}$ lui-même ou dans une de ses extensions $\mathfrak{O}'$, les éléments α vérifiant la relation (1) : un élément de cette nature est par définition une *racine de l'équation* (1), ou un *zéro* du polynome $f(x)$.

Supposons que $\mathfrak{O}$ possède un *élément-unité*. D'après une proposition établie plus haut (chap. VI, § 3, corollaire, p. 341), *il faut et il suffit, pour qu'un élément $\alpha \in \mathfrak{O}' (\supseteq \mathfrak{O})$ soit une racine de l'équation (1), que le polynome $f(x)$ soit divisible par $x - \alpha$ ($x - \alpha \in \mathfrak{O}'[x]$)*.

Cela étant, supposons que $\mathfrak{O}'$ (donc aussi $\mathfrak{O}$) soit un *domaine d'intégrité*, $\mathfrak{O}' = \mathbf{I}$, et que l'équation (1) admette, dans $\mathbf{I}$, k *racines distinctes* $\alpha_1, \alpha_2, \dots, \alpha_k$; le polynome $f(x)$ est alors divisible par le produit $(x - \alpha_1) \dots (x - \alpha_k)$. Il est, en effet, divisible par $x - \alpha_1$. Supposons-le divisible par $(x - \alpha_1) \dots (x - \alpha_i)$ ($1 \leq i < k$)

$$f(x) = (x - \alpha_1) \dots (x - \alpha_i) g(x).$$

La spécialisation $x = \alpha_{i+1}$ donne

$$f(\alpha_{i+1}) = (\alpha_{i+1} - \alpha_1) \dots (\alpha_{i+1} - \alpha_i) g(\alpha_{i+1}) = 0,$$

d'où, puisque α_{i+1} n'est égal à aucun des éléments $\alpha_1, \dots, \alpha_i$ et que $\mathbf{I}$ est un domaine d'intégrité

$$g(\alpha_{i+1}) = 0.$$

Il en résulte

$$x - \alpha_{l+1} \mid g(x),$$

d'où

$$(x - \alpha_1) \dots (x - \alpha_l)(x - \alpha_{l+1}) \mid f(x)$$

et, par conséquent, la propriété est vraie pour un nombre quelconque k de zéros

$$f(x) = (x - \alpha_1) \dots (x - \alpha_k) q(x).$$

D'après cette égalité, dont le second membre a un degré au moins égal à k , le nombre k ne peut pas dépasser le degré m de $f(x)$, d'où l'importante proposition suivante :

THÉORÈME 1. — *Dans un domaine d'intégrité I, un polynome $f(x) \in I[x]$, de degré m , a au plus m zéros distincts.*

Remarques. — 1. Ce théorème est valable même si le domaine d'intégrité I ne possède pas d'élément-unité. Considérons, en effet, le corps des quotients, K, de I : $f(x)$ ayant au plus m zéros dans K, en a au plus m dans I.

2. Au contraire, dans un anneau ayant des diviseurs de zéro, le théorème précédent n'est plus vrai. Par exemple, dans l'anneau C_4 des classes résiduelles modulo 4, le polynome du premier degré $2x \in C_4[x]$ admet deux zéros distincts : 0 et 2.

Étant donné un domaine d'intégrité I, il existe, d'après le théorème 1, au plus un polynome $f(x) \in I[x]$, de degré inférieur ou égal à m , prenant $m+1$ valeurs données $\beta_0, \beta_1, \dots, \beta_m$ ($\beta_i \in I$) pour $m+1$ valeurs données de $x, \alpha_0, \alpha_1, \dots, \alpha_m$ ($\alpha_i \in I$)

$$f(\alpha_i) = \beta_i \quad (i = 0, 1, \dots, m).$$

Un tel polynome existe effectivement lorsque le domaine considéré est un corps K ; il est donné, d'une manière évidente, par la formule d'interpolation de Lagrange ⁽¹⁾

$$f(x) = \sum_{i=0}^m f(\alpha_i) \frac{(x - \alpha_0) \dots (x - \alpha_{i-1})(x - \alpha_{i+1}) \dots (x - \alpha_m)}{(\alpha_i - \alpha_0) \dots (\alpha_i - \alpha_{i-1})(\alpha_i - \alpha_{i+1}) \dots (\alpha_i - \alpha_m)}.$$

(1) Si l'on se place dans un domaine d'intégrité I ($\alpha_i \in I, \beta_i \in I$), il existe dans $K[x]$, en désignant par K le corps des quotients, un polynome de degré $\leq m$ vérifiant les $m+1$ relations $f(\alpha_i) = \beta_i$. Mais ce polynome n'appartient pas nécessairement à l'anneau $I[x]$. Par exemple, le polynome du premier degré égal à 0 pour $x = 0$ et à 1 pour $x = 2$ est $\frac{1}{2}x$, et n'appartient pas à $C[x]$.

On peut aussi obtenir ce polynome $f(x)$ par la méthode suivante, due à Newton ⁽¹⁾, et qui consiste à chercher ce polynome sous la forme

$$(2) \quad f(x) = q_0 + q_1(x - \alpha_0) + q_2(x - \alpha_0)(x - \alpha_1) + \dots + q_m(x - \alpha_0) \dots (x - \alpha_{m-1}).$$

On a

$$q_0 = f(\alpha_0),$$

d'où

$$(2') \quad \frac{f(x) - f(\alpha_0)}{x - \alpha_0} = q_1 + q_2(x - \alpha_1) + \dots + q_m(x - \alpha_1) \dots (x - \alpha_{m-1}).$$

Désignons par $f_1(\alpha_0, x)$ le premier membre qui est encore un polynome de $K[x]$, puisque $f(x) - f(\alpha_0)$, nul pour $x = \alpha_0$, est divisible par $x - \alpha_0$. La relation (2'), de même forme que (2), entraîne

$$q_1 = f_1(\alpha_0, \alpha_1) = \frac{f(\alpha_1) - f(\alpha_0)}{\alpha_1 - \alpha_0} = \frac{\beta_1 - \beta_0}{\alpha_1 - \alpha_0};$$

q_1 est donc la *pente* de la droite joignant dans le plan (α, β) les points (α_0, β_0) et (α_1, β_1) . Nous avons ensuite

$$(2'') \quad \frac{f_1(\alpha_0, x) - f_1(\alpha_0, \alpha_1)}{x - \alpha_1} = q_2 + q_3(x - \alpha_2) + \dots + q_m(x - \alpha_2) \dots (x - \alpha_m),$$

d'où, en désignant le premier membre par $f_2(\alpha_0, \alpha_1, x)$,

$$q_2 = f_2(\alpha_0, \alpha_1, \alpha_2).$$

On obtient d'ailleurs aisément

$$q_2 = - \frac{(\alpha_0 - \alpha_1)f(\alpha_2) + (\alpha_1 - \alpha_2)f(\alpha_0) + (\alpha_2 - \alpha_0)f(\alpha_1)}{(\alpha_1 - \alpha_2)(\alpha_2 - \alpha_0)(\alpha_0 - \alpha_1)}.$$

D'une façon générale, si nous définissons par récurrence le polynome $f_i(\alpha_0, \dots, \alpha_{i-1}, x)$ en posant

$$f_i(\alpha_0, \dots, \alpha_{i-1}, x) = \frac{f_{i-1}(\alpha_0, \dots, \alpha_{i-2}, x) - f_{i-1}(\alpha_0, \dots, \alpha_{i-2}, \alpha_{i-1})}{x - \alpha_{i-1}}$$

et, si nous supposons que l'on ait

$$f_i(\alpha_0, \dots, \alpha_{i-1}, x) = q_i + q_{i+1}(x - \alpha_i) + \dots,$$

nous en déduisons

$$q_i = f_i(\alpha_0, \dots, \alpha_{i-1}, \alpha_i) = \frac{f_{i-1}(\alpha_0, \dots, \alpha_{i-2}, \alpha_i) - f_{i-1}(\alpha_0, \dots, \alpha_{i-2}, \alpha_{i-1})}{\alpha_i - \alpha_{i-1}}.$$

⁽¹⁾ Nous suivons ici, dans ses grandes lignes, l'exposé de M. van der Waerden (*Moderne Algebra*, t. I, p. 70).

et

$$f_{i+1}(\alpha_0, \dots, \alpha_i, x) = q_{i+1} + q_{i+2}(x - \alpha_{i+1}) + \dots$$

La quantité q_i est appelée parfois *pente d'ordre i* correspondant aux $i+1$ points (α_ν, β_ν) ($\nu = 0, 1, \dots, i$). Le polynome $f(x)$ se trouve ainsi déterminé de proche en proche.

D'autre part, les q_i ayant les valeurs précédentes, le polynome

$$g_i(x) = q_0 + q_1(x - \alpha_0) + \dots + q_i(x - \alpha_0) \dots (x - \alpha_{i-1})$$

est le polynome, de degré inférieur ou égal à i , qui prend respectivement les valeurs β_ν aux points α_ν ($\nu = 0, 1, \dots, i$); comme il est unique et que le coefficient de son terme en x^i est précisément q_i , nous voyons que $q_i = f_i(\alpha_0, \dots, \alpha_i)$ dépend seulement des points (α_ν, β_ν) et non de l'ordre dans lequel on range ces points. C'est d'ailleurs ce qui apparaît pour q_0, q_1 et q_2 sur les formules explicites données plus haut. Il en résulte qu'on peut encore écrire, en permutant les α_ν dans l'expression de q_i

$$(3) \quad \left\{ \begin{aligned} q_i = f_i(\alpha_0, \alpha_1, \dots, \alpha_i) &= \frac{f_{i-1}(\alpha_1, \dots, \alpha_{i-1}, \alpha_i) - f_{i-1}(\alpha_1, \dots, \alpha_{i-1}, \alpha_0)}{\alpha_i - \alpha_0} \\ &= \frac{f_{i-1}(\alpha_1, \dots, \alpha_{i-1}, \alpha_i) - f_{i-1}(\alpha_0, \alpha_1, \dots, \alpha_{i-1})}{\alpha_i - \alpha_0}. \end{aligned} \right.$$

Pour calculer rapidement cette dernière expression, on utilise la disposition suivante, que nous figurerons pour $m = 2$,

$$\begin{array}{rcc} f(\alpha_0) & & \\ f(\alpha_1) & f_1(\alpha_0, \alpha_1) & f_2(\alpha_0, \alpha_1, \alpha_2). \\ f(\alpha_2) & f_1(\alpha_1, \alpha_2) & \end{array}$$

Le numérateur, mis sous la forme (3), d'un terme de ce tableau, est la différence des deux termes placés immédiatement à sa gauche.

Si l'on se donne un point supplémentaire $(\alpha_{m+1}, \beta_{m+1})$, le polynome de degré $m+1$ au plus prenant les valeurs β_ν aux points α_ν ($\nu = 0, 1, \dots, m+1$) se déduit de $f(x)$ par la simple addition du terme

$$q_{m+1}(x - \alpha_0) \dots (x - \alpha_m),$$

dont le calcul exige seulement qu'on inscrive un nombre au bas de chaque colonne du tableau et un nombre à la droite de ce tableau; cette possibilité de poursuivre facilement l'application du procédé est un avantage important de la méthode de Newton. Si l'on forme de la même manière un tableau illimité en inscrivant dans la première colonne, non plus des valeurs quelconques, mais celles que prend effectivement un

certain polynome $f(x)$ de degré m , tous les éléments obtenus dans la $(m+1)^{\text{ème}}$ colonne sont égaux [au coefficient q_m relatif à $f(x)$] et les colonnes suivantes se composent de zéros.

Un cas particulier important est celui où les α_i sont les nombres naturels consécutifs : $\alpha_i = i$. Il est alors commode de multiplier les éléments de la $(\nu+1)^{\text{ème}}$ colonne par $\nu!$, on obtient ainsi le tableau des différences

$$\begin{array}{ccccccc} & & & & & & \beta_0 \\ & & & & & & \Delta\beta_0 \\ & & & & & \beta_1 & \Delta^2\beta_0 \quad \dots, \\ & & & & & \Delta\beta_1 & \\ & & & & \beta_2 & \dots, \\ & & & & \dots & \dots & \end{array}$$

où

$$\begin{aligned} \Delta\beta_i &= \beta_{i+1} - \beta_i, \\ \Delta^2\beta_i &= \Delta(\Delta\beta_i) = \Delta\beta_{i+1} - \Delta\beta_i = \beta_{i+2} - 2\beta_{i+1} + \beta_i, \\ &\dots\dots\dots, \\ \Delta^\nu\beta_i &= \Delta(\Delta^{\nu-1}\beta_i) = \Delta^{\nu-1}\beta_{i+1} - \Delta^{\nu-1}\beta_i. \end{aligned}$$

Si l'on s'est donné $m+1$ points $(x_\nu = \nu, \beta_\nu)$, le polynome $f(x)$ correspondant est le polynome

$$(4) \quad f(x) = \beta_0 + \frac{\Delta\beta_0}{1}x + \dots + \frac{\Delta^m\beta_0}{m!}x(x-1)\dots(x-m+1).$$

Si, dans le tableau illimité des différences, les β_i sont les valeurs prises par un polynome donné de degré m , toutes les différences d'ordre m sont égales et les différences d'ordre supérieur sont nulles. Réciproquement, si une suite $\beta_0, \beta_1, \dots, \beta_\nu, \dots$ de nombres est telle que, dans le tableau des différences, toutes les différences soient nulles à partir de l'ordre $m+1$, les β_i sont les valeurs prises par un polynome de degré m . Pour le voir, considérons le polynome $f(x)$ de degré au plus égal à m , défini à partir des premiers éléments de chaque colonne par la formule (4), et formons le tableau des différences correspondant aux valeurs $\beta'_0 = \beta_0, \beta'_1, \beta'_2, \dots$ prises par ce polynome pour $x = 0, 1, 2, \dots$. Toutes les différences seront nulles à partir de l'ordre $m+1$, et nous aurons

$$\beta'_1 = \beta_0 + \Delta\beta_0 = \beta_1, \quad \Delta\beta'_1 = \Delta\beta_0 + \Delta^2\beta_0 = \Delta\beta_1, \quad \beta'_2 = \beta'_1 + \Delta\beta'_1 = \beta_2, \quad \dots;$$

ce tableau coïncide donc avec le tableau donné.

On appelle *progression arithmétique d'ordre nul* une suite de nombres tous égaux, *progression arithmétique d'ordre m* une suite $u_0, u_1, \dots, u_n, \dots$ telle que la suite des différences $\Delta u_i = u_{i+1} - u_i$

soit une progression arithmétique d'ordre $m - 1$. On voit, d'après ce qui précède, que *les valeurs prises par un polynôme de degré m pour $x = 0, 1, \dots, n, \dots$ forment une progression arithmétique d'ordre m ; et qu'inversement, toute progression arithmétique d'ordre m est la suite des valeurs prises par un polynôme de degré m au plus.*

Remarque. — On peut rattacher aux formules d'interpolation un procédé, dû à Kronecker, pour reconnaître, par un nombre fini d'opérations, si un polynôme $f(x)$ de $C[x]$, où C désigne l'anneau des entiers, est *réductible*, et pour obtenir, dans l'affirmative, sa décomposition en facteurs irréductibles. Remarquons d'abord que, si, dans $C[x]$, $g(x) | f(x)$, on aura, dans C , $g(\alpha) | f(\alpha)$ pour tout $\alpha \in C$. Pour examiner si f admet un diviseur g de degré $\leq n$, on se donnera $n + 1$ entiers $\alpha_0, \alpha_1, \dots, \alpha_n$ et l'on déterminera dans C les différents diviseurs $\delta_i, \delta'_i, \dots$, de $f(\alpha_i)$. On construira, de préférence par la méthode de Newton, les différents polynômes $g(x)$ prenant pour $x = \alpha_i$ une valeur β_i égale à l'un des nombres $\delta_i, \delta'_i, \dots$, et l'on examinera, pour chacun d'eux, s'il divise ou non $f(x)$. Pour opérer rapidement, il convient de choisir, autant que possible, les α_i de manière que les entiers $f(\alpha_i)$ soient premiers ou n'admettent qu'un très petit nombre de diviseurs. Si m désigne le degré de $f(x)$, on prend $n = \frac{m}{2}$ ou $\frac{m-1}{2}$ suivant que m est pair ou impair. On peut aussi pour opérer plus rapidement, combiner cette méthode avec les procédés indiqués plus haut (chap. VI, § 6, remarque 3, p. 352).

La méthode s'applique plus généralement dans un anneau $\mathfrak{o}[x]$, si $\mathfrak{o}$ est un *domaine à factorisation unique*, n'ayant qu'un nombre fini d'unités. Il est nécessaire de faire intervenir cette dernière condition, car des valeurs associées pour les β_i fournissent des polynômes $g(x)$ différents.

Du théorème 1, résulte qu'un polynôme $f(x)$, de degré m , de l'anneau $\mathfrak{o}[x]$, où $\mathfrak{o}$ désigne un domaine d'intégrité, est *nul* ⁽¹⁾, s'il admet dans un domaine d'intégrité $\mathfrak{o}'$ contenant $\mathfrak{o}$, plus de m zéros distincts. Par conséquent, *si $\mathfrak{o}'$ contient un ensemble infini E , et si $g(x)$ est un polynôme non nul de $\mathfrak{o}[x]$, on peut toujours trouver au moins une valeur $a \in E$ telle que $g(a)$ soit différent de zéro.*

Cette propriété s'étend immédiatement aux polynômes à plusieurs variables. Soit $g(x_1, x_2, \dots, x_n) \in \mathfrak{o}[x_1, x_2, \dots, x_n]$ un polynôme non nul. En regardant g comme un polynôme en x_n dont les coefficients appartiennent à $\mathfrak{o}[x_1, x_2, \dots, x_{n-1}]$, on peut trouver dans l'ensemble infini $E \subseteq \mathfrak{o}' \subseteq \mathfrak{o}'[x_1, x_2, \dots, x_{n-1}] = \mathfrak{o}'_{n-1}$ un élément a_n tel que $g(x_1, x_2, \dots, x_{n-1}, a_n)$ soit un élément non nul de $\mathfrak{o}'_{n-1}$. Cet élément peut être regardé à son tour comme un polynôme en x_{n-1} , non nul, dont les coefficients appartiennent à $\mathfrak{o}'_{n-2} = \mathfrak{o}'[x_1, x_2, \dots, x_{n-2}]$: on

(1) Voir p. 326.

peut trouver dans E un élément non nul, a_{n-1} , tel que

$$g(x_1, \dots, x_{n-2}, a_{n-1}, a_n)$$

soit différent de zéro, etc.

Si enfin nous nous donnons simultanément r polynômes non nuls $g_1(x_1, x_2, \dots, x_n), \dots, g_r(x_1, x_2, \dots, x_n)$ de $\mathfrak{O}[x_1, x_2, \dots, x_n]$, nous pouvons toujours trouver, dans le sous-ensemble infini E considéré du domaine d'intégrité $\mathfrak{O}'$ contenant $\mathfrak{O}$, un système de valeurs $a_1, a_2, \dots, a_n$ tel que l'on ait

$$g_1(a_1, \dots, a_n) \neq 0 \quad \dots, \quad g_r(a_1, \dots, a_n) \neq 0.$$

Il suffit d'appliquer ce qui précède au polynôme $g = g_1 g_2 \dots g_r$. De même, en considérant le produit $\prod_{\substack{\mu, \nu=1 \\ \mu < \nu}}^r (g_\mu - g_\nu)$, on voit qu'on peut trouver dans E au moins un système d'éléments $a_1, \dots, a_n$, pour lequel les polynômes g_i prennent des valeurs toutes différentes.

Considérons maintenant un corps K et l'anneau euclidien $K[x]$ des polynômes en x à coefficients dans K .

THÉORÈME 2. — *Deux polynômes de $K[x]$, $f(x)$, $g(x)$, premiers entre eux, n'ont aucun zéro commun dans K ou dans un sur-corps K' de K .*

En effet, si α était un zéro commun à $f(x)$ et $g(x)$, $x - \alpha$ diviserait, dans $K'[x]$, $f(x)$ et $g(x)$, ce qui est incompatible avec l'identité

$$u(x)f(x) + v(x)g(x) = 1 \quad (u, v \in K[x] \subseteq K'[x]).$$

Ce théorème s'applique en particulier à deux polynômes irréductibles sur K et distincts. Il entraîne, d'autre part, les conséquences suivantes.

COROLLAIRE 1. — *Si un polynôme $f(x) \in K[x]$, irréductible sur K , a un zéro commun, dans un sur-corps de K , avec un polynôme $\varphi(x) \in K[x]$, $f(x)$ divise $\varphi(x)$. En effet, dans $K[x]$, f et φ ne peuvent pas être premiers entre eux, d'après le théorème précédent. Comme f est irréductible, il divise φ .*

COROLLAIRE 2. — *Soient $f(x)$, $g(x)$ deux polynômes quelconques de $K[x]$. Leurs zéros communs (dans tel ou tel sur-corps de K), sont ceux des facteurs irréductibles communs qu'ils admettent lorsqu'on les décompose dans $K[x]$.*

Un élément α de K ou d'une extension K' de K est *racine d'ordre μ* de l'équation

$$f(x) = 0$$

ou *zéro d'ordre μ* du polynome $f(x)$, si l'on a

$$f(x) = (x - \alpha)^\mu q(x), \quad \text{avec } q(x) \neq 0.$$

Une racine d'ordre supérieur à l'unité est dite *multiple* ; si $\mu = 1$, la racine α est *simple*.

Considérons le polynome

$$\varphi_\alpha(x) = \frac{f(x)}{x - \alpha} = \frac{f(x) - f(\alpha)}{x - \alpha} = (x - \alpha)^{\mu-1} q(x);$$

la condition nécessaire et suffisante pour que α soit racine multiple s'écrit

$$(5) \quad \varphi_\alpha(x) = 0.$$

La notion de *dérivée*, que nous allons introduire, permet de donner à cette condition une forme plus remarquable et plus commode. Considérons la fonction rationnelle de deux variables x et y définie par la relation

$$(6) \quad F(x, y) = \frac{f(x) - f(y)}{x - y} \in K(x, y).$$

L'application

$$f(x) \rightarrow F(x, y)$$

de $K[x]$ dans $K(x, y)$, définie par (6), a les propriétés suivantes :

Elle est en premier lieu *régulière vis-à-vis de l'addition* ; autrement dit, d'après (6),

$$f_1 \rightarrow F_1, \quad f_2 \rightarrow F_2 \quad \text{entraînent} \quad f_1 + f_2 \rightarrow F_1 + F_2.$$

D'autre part, elle est *permise par rapport à K* , c'est-à-dire

$$f \rightarrow F \quad \text{entraîne} \quad af \rightarrow aF \quad \text{pour tout } a \in K.$$

Dans le cas particulier où $f(x) = x^m$, nous avons

$$F(x, y) = \frac{x^m - y^m}{x - y} = \frac{\left(\sum_{i=0}^{m-1} x^{m-i-1} y^i \right) (x - y)}{x - y} = \sum_{i=0}^{m-1} x^{m-i-1} y^i.$$

Si maintenant $f(x)$ est un polynome quelconque de $K[x]$,

$$f(x) = a_0 + a_1 x + \dots + a_m x^m \quad (a_i \in K),$$

nous avons, d'après les propriétés précédentes,

$$F(x, y) = a_1 + a_2(x + y) + \dots + a_m \sum_{i=0}^{m-1} x^{m-i-1} y^i$$

et, par conséquent, F est un polynôme en x et y :

$$F(x, y) \in K[x, y].$$

Nous définissons alors la *dérivée* $f'(x)$ de $f(x)$ en posant

$$f'(x) = F(x, x) = a_1 + 2a_2x + \dots + ma_mx^{m-1}.$$

Cette dérivée est un polynôme appartenant comme f à l'anneau $K[x]$; son degré est au plus égal à $m-1$; il est effectivement inférieur à $m-1$ si K a la caractéristique p et si m est multiple de p .

La dérivée d'une somme est visiblement la somme des dérivées. La dérivée d'un produit se calcule aisément; soit

$$f(x) = g(x)h(x).$$

Nous avons

$$\begin{aligned} F(x, y) &= \frac{g(x)h(x) - g(y)h(y)}{x - y} = \frac{g(x)[h(x) - h(y)] + h(y)[g(x) - g(y)]}{x - y} \\ &= g(x)H(x, y) + h(y)G(x, y), \end{aligned}$$

d'où, en remplaçant y par x ,

$$f'(x) = g(x)h'(x) + h(x)g'(x).$$

On en déduit immédiatement, pour un nombre quelconque, r , de facteurs, la formule de Leibnitz

$$(f_1 f_2 \dots f_r)' = \sum_{i=1}^r f_1 \dots f_{i-1} f'_i f_{i+1} \dots f_r,$$

d'où notamment

$$[g^r(x)]' = r g^{r-1}(x) g'(x).$$

On remarquera que, si K est un corps de caractéristique p , la dérivée de la puissance $p^{\text{ième}}$ d'un polynôme quelconque de $K(x)$, est un polynôme nul.

Cela posé, nous avons

$$\varphi_\alpha(x) = F(x, \alpha)$$

et la condition nécessaire et suffisante (5) pour que α soit zéro multiple de $f(x)$ s'écrit $F(\alpha, \alpha) = 0$, c'est-à-dire

$$(5') \quad f'(\alpha) = 0.$$

Nous avons, par conséquent, la proposition suivante :

THÉOREME 3. — *Pour qu'un zéro α de $f(x)$ soit multiple, il faut et il suffit qu'il annule la dérivée $f'(x)$.* En particulier, un zéro de f est simple dès qu'il n'annule pas f' : si donc f et f' sont premiers entre eux

$$uf + vf' = 1 \quad (u, v \in K[x]),$$

le polynome f n'a que des zéros simples.

Un cas particulièrement important est celui des *polynomes irréductibles* (sur K). Un polynome irréductible $f(x)$ est dit *inséparable* ou de *seconde espèce* s'il admet au moins un zéro multiple α (dans telle ou telle extension K' de K); dans le cas contraire, il est *séparable* ou de *première espèce*. Si tout polynome irréductible de $K[x]$ est séparable, le corps K est, par définition, *parfait*; s'il existe dans $K[x]$ des polynomes irréductibles inséparables (non nuls), K est *imparfait*.

Un polynome irréductible inséparable $f(x)$, à supposer qu'il en existe un, possède avec sa dérivée $f'(x)$ un zéro commun α ; d'après le corollaire I, il doit donc diviser $f'(x)$. Mais la dérivée $f'(x)$, ayant un degré inférieur à celui de $f(x)$, ne peut être divisible par f que si elle est un polynome nul. Donc,

THÉOREME 4. — *Si un polynome irréductible*

$$f(x) = a_0 + a_1x + \dots + a_mx^m$$

est inséparable, sa dérivée est un polynome nul

$$f'(x) = 0.$$

Pour appliquer ce théorème, nous distinguerons deux cas.

a. Le corps K est de caractéristique nulle.

La condition

$$f'(x) = 0, \quad \text{c'est-à-dire} \quad ka_k = 0 \quad (k = 1, \dots, m)$$

entraîne

$$a_k = 0 \quad (k = 1, \dots, m);$$

f est par suite une constante, qui n'admet de zéro que si elle est elle-même nulle. *Aucun polynome irréductible non nul ne peut donc être inséparable*, ce que nous pouvons encore énoncer de la manière suivante :

THÉOREME 4. — *Tout corps de caractéristique zéro est parfait.*

b. *Le corps K a la caractéristique p .*

Alors, la condition

$$f(x) = 0, \quad \text{c'est-à-dire} \quad ka_k = 0 \quad (k = 1, \dots, m)$$

n'entraîne $a_k = 0$ que si le nombre naturel k n'est pas multiple de p ; il existe donc des polynômes $f(x)$ de degré > 0 ayant une dérivée nulle : ils sont de la forme

$$(7) \quad f(x) = \sum_{\nu} a_{\nu p} x^{\nu p} \quad (\nu = 0, 1, \dots).$$

La question se pose alors de savoir si cette forme est compatible ou non avec l'irréductibilité du polynôme $f(x)$. Nous allons précisément voir qu'il existe aussi des corps parfaits parmi les corps de caractéristique p .

THÉOREME 5. — *Soit K un corps de caractéristique p . Si tout élément $a \in K$ possède, dans K , une racine $p^{\text{ième}}$, K est parfait.*

Si, en effet, un polynôme irréductible sur K , $f(x)$, possédait un zéro multiple, ce polynôme, ayant une dérivée nulle, serait de la forme (7) et nous aurions

$$f(x) = \sum_{\nu} (\sqrt[p]{a_{\nu p}} x^{\nu})^p = \left(\sum_{\nu} \sqrt[p]{a_{\nu p}} x^{\nu} \right)^p = [\varphi(x)]^p,$$

où $\varphi(x)$ appartient à $K[x]$, puisque $\sqrt[p]{a_{\nu p}} \in K$; cette conclusion est absurde, étant donné que f est irréductible sur K .

Indiquons maintenant un cas important dans lequel l'hypothèse du théorème 5 est vérifiée.

Dans un corps K de caractéristique p , l'application

$$x \rightarrow x^p$$

de K en lui-même est *biunivoque* ⁽¹⁾, car

$$x^p = y^p \quad \text{entraîne} \quad 0 = x^p - y^p = (x - y)^p, \quad \text{d'où} \quad x = y.$$

Par suite, si le corps K a un nombre fini d'éléments, tout élément de K est puissance $p^{\text{ième}}$, donc admet dans K une racine $p^{\text{ième}}$. Le corps K est parfait. Nous pouvons donc énoncer la proposition suivante :

(1) Il en résulte que, si un élément possède, dans un corps de caractéristique p , une racine $p^{\text{ième}}$, cette racine est unique.

THÉOREME 6. — *Tout champ de Galois est un corps parfait.*

En particulier, le corps C_p des classes résiduelles modulo p est un corps parfait (on remarquera que, d'après le théorème de Fermat, tout élément de C_p est sa propre racine $p^{\text{ième}}$).

K désignant un corps quelconque, soit α un zéro d'ordre μ d'un polynome $f(x) \in K[x]$

$$f(x) = (x - \alpha)^\mu g(x), \quad g(\alpha) \neq 0.$$

Nous obtenons en dérivant

$$f'(x) = (x - \alpha)^{\mu-1} [\mu g(x) + (x - \alpha) g'(x)].$$

Un zéro α d'ordre μ de $f(x)$ est donc, pour $f'(x)$, un zéro d'ordre $\mu - 1$ au moins : si K a la caractéristique p et si μ est multiple de p , α est, pour $f'(x)$, un zéro d'ordre μ au moins. Dans le cas d'un corps de caractéristique nulle, α est zéro d'ordre $\mu - 1$ exactement pour $f'(x)$. Alors, en considérant les dérivées successives de $f(x)$, $f''(x) = [f'(x)]'$, ..., on obtient immédiatement l'énoncé suivant :

Si K est un corps de caractéristique nulle, pour qu'un zéro α d'un polynome $f(x) \in K[x]$ soit d'ordre μ , il faut et il suffit que α annule les $\mu - 1$ premières dérivées de $f(x)$

$$f'(\alpha) = f''(\alpha) = \dots = f^{(\mu-1)}(\alpha) = 0.$$

Remarque. — Nous avons défini plus haut la dérivée $f'(x)$ d'un polynome $f(x) \in K[x]$. Considérons maintenant une fraction rationnelle

$$r(x) = \frac{f(x)}{g(x)} \in K(x)$$

et associons-lui la fraction

$$\begin{aligned} R(x, y) &= \frac{r(x) - r(y)}{x - y} = \frac{f(x)g(y) - f(y)g(x)}{(x - y)g(x)g(y)} \\ &= \frac{g(y)F(x, y) - f(y)G(x, y)}{g(x)g(y)} \in K(x, y). \end{aligned}$$

La fraction

$$R(x, x) = \frac{g(x)F(x, x) - f(x)G(x, x)}{g^2(x)} = \frac{f'(x)g(x) - f(x)g'(x)}{g^2(x)} \in K(x)$$

est, par définition, la dérivée $r'(x)$ de $r(x)$. On vérifie, comme pour les polynomes, les deux règles de calcul fondamentales

$$(8) \quad (r + s)' = r' + s',$$

$$(9) \quad (rs)' = r's + rs'.$$

Envisageons maintenant l'anneau $K[x_1, \dots, x_n]$ et le corps $K(x_1, \dots, x_n)$ et considérons particulièrement l'une des indéterminées, $x_1 (= x)$ par exemple. Désignons par Λ le corps $K(x_2, \dots, x_n)$ et regardons un polynôme $f(x_1, \dots, x_n)$ comme un élément $\varphi(x_1)$ de l'anneau $\Lambda[x_1]$, une fraction rationnelle $r(x_1, \dots, x_n)$ comme un élément $\varphi(x_1)$ du corps $\Lambda(x_1)$; les dérivées correspondantes $\varphi'(x_1)$, $\varphi''(x_1)$ sont appelées *dérivées partielles* de f ou de r par rapport à x_1 et désignées par f'_{x_1} , r'_{x_1} . On définit de même les dérivées partielles par rapport aux autres indéterminées. Toutes ces dérivations partielles vérifient les règles de calcul (8) et (9).

On appelle enfin, d'une façon tout à fait générale, *dérivation abstraite d'un corps* Σ quelconque une application $\alpha \rightarrow D\alpha$ de Σ dans lui-même vérifiant les deux règles fondamentales

$$(8') \quad D(\alpha + \beta) = D\alpha + D\beta,$$

$$(9') \quad D(\alpha\beta) = D\alpha \cdot \beta + \alpha \cdot D\beta.$$

On donne souvent le nom de *corps différentiel* à un corps muni de telles dérivations ⁽¹⁾.

Exercices. — 1. C_{12} désignant l'anneau des classes résiduelles modulo 12, combien le polynôme $3x^2 \in C_{12}[x]$ admet-il de zéros dans C_{12} ?

2. Quel est le degré du polynôme f de l'anneau $C[x]$ qui prend pour

$$x = -2, \quad -1, \quad 0, \quad +1, \quad +2$$

les valeurs

$$f(x) = 15, \quad 4, \quad 3, \quad 6, \quad 7.$$

Former ce polynôme; le décomposer en facteurs irréductibles dans $C[x]$.

3. On considère un nombre premier p et le corps C_p des classes résiduelles modulo p .

1° Les polynômes de $C_p[x]$, nuls pour toute valeur $a \in C_p$ attribuée à x , forment un idéal principal.

2° En désignant par $f(x)$ le polynôme de base de cet idéal, montrer qu'on a l'égalité

$$f(x) = f(x-1).$$

En déduire :

a. Les coefficients du polynôme $f(x)$;

b. Le théorème de Fermat

$$a^p \equiv a \pmod{p} \quad \text{pour tout } a \in C;$$

⁽¹⁾ On trouvera une étude systématique des corps différentiels dans l'Ouvrage de J. F. RITT, *Differential algebra* (Amer. Math. Soc., Coll. publ., t. 33, 1950) et l'on pourra consulter la bibliographie placée à la fin de ce volume. Voir également : A. WEIL, *Foundations of algebraic Geometry* (Amer. Math. Soc., Coll. publ., t. 29, p. 11; J. C. HERZ, *Contribution à la théorie algébrique des équations aux dérivées partielles* (Thèse, Paris, 1954; à paraître aux *Annales de l'École Normale*).

c. Le théorème de Wilson

$$(p-1)! \equiv -1 \pmod{p};$$

montrer qu'inversement, cette congruence entraîne : p est premier.

2. Extensions simples, adjonction symbolique. — Considérons un corps K et, dans un sur-corps Σ de K , un élément α *algébrique par rapport à K* (et n'appartenant pas à K). Nous nous proposons d'étudier l'extension algébrique simple $K(\alpha)$, obtenue à partir de K par l'*adjonction* de α .

Il existe par hypothèse des expressions rationnelles entières en α qui sont nulles

$$g(\alpha) = b_0 + b_1\alpha + \dots + b_n\alpha^n = 0 \quad (b_i \in K).$$

ou, ce qui revient au même, des polynomes $g(x) \in K[x]$ qui admettent, dans Σ , α pour zéro. Ces polynomes constituent, dans le domaine d'intégrité $I = K[x]$ un *idéal* $\mathfrak{a}$, qui est principal, puisque I est un anneau euclidien (chap. VI, § 5, p. 339)

$$\mathfrak{a} = (f).$$

Si m est le degré de f , tout polynome g appartenant à $\mathfrak{a}$ est d'un degré n au moins égal à m : il en résulte que f est *irréductible sur K* ; si l'on avait, en effet, $f = f_1 f_2$, f_1 et f_2 étant de véritables diviseurs de f , l'un au moins de ces facteurs admettrait α pour zéro dans Σ , donc appartiendrait à l'idéal $\mathfrak{a}$, ce qui est impossible. Le polynome de base f est défini à un facteur près, facteur égal à une unité de $K[x]$, c'est-à-dire à un élément de K : on peut donc prendre f de la forme

$$f(x) = a_0 + a_1x + \dots + x^m \quad (a_i \in K).$$

Ce polynome est appelé *polynome caractéristique* de l'élément α ou de l'extension algébrique simple $K(\alpha)$; son degré m est, par définition, le *degré de l'élément α* .

Un élément ξ quelconque de $K(\alpha)$ est une expression rationnelle en α

$$\xi = \frac{r(\alpha)}{s(\alpha)}, \quad \text{où } r(\alpha), s(\alpha) \in K[x], \quad \text{avec } s(\alpha) \neq 0;$$

$s(x)$ est *premier à f* , car, s'il ne l'était pas, le polynome irréductible $f(x)$ diviserait s et $s(\alpha)$ serait nul. Nous avons donc une identité de la forme

$$u(x)s(x) + v(x)f(x) = 1 \quad (u(x), v(x) \in K[x]),$$

d'où

$$u(\alpha)s(\alpha) = 1$$

et

$$\xi = r(\alpha) u(\alpha).$$

Tout élément ξ de $K(\alpha)$ peut donc se mettre sous forme entière

$$(1) \quad \xi = h(\alpha), \quad \text{où } h(x) \in K[x]$$

et nous avons

$$K(\alpha) = A,$$

où $A = \{h(\alpha)\}$ désigne l'anneau des expressions rationnelles entières en α (à coefficients dans K).

Si nous considérons, pour un même élément ξ , deux représentations différentes

$$\xi = h_1(\alpha) = h_2(\alpha) \quad (h_1, h_2 \in K[x]),$$

nous avons

$$h_1(x) - h_2(x) \in \mathfrak{a}, \quad \text{donc } h_1 - h_2 = qf.$$

Par suite, parmi toutes les représentations de ξ possibles, il en existe une et une seule

$$\xi = c(\alpha), \quad c(x) \in K[x]$$

dans laquelle $c(x)$ est un polynome de degré inférieur à m .

D'après ce qui précède, l'extension $K(\alpha)$ et l'anneau des classes résiduelles modulo $\mathfrak{a}$, $K[x]/(f(x)) = I/\mathfrak{a}$ se correspondent biunivoquement. D'après le principe de spécialisation, cette correspondance est un isomorphisme pour l'addition et la multiplication; elle est même un isomorphisme sur K , puisque les éléments de K se correspondent à eux-mêmes. Nous avons, par conséquent,

$$K(\alpha) \underset{(\bar{K})}{\cong} K[x]/(f(x)) = I/\mathfrak{a}.$$

De cette relation résulte que $K[x]/(f)$ est un corps, ce qu'on peut voir également en remarquant que l'idéal principal $\mathfrak{a}$, engendré par un élément premier f de I , est sans diviseurs (chap. VI, § 3, p. 318).

On peut obtenir les mêmes résultats par une méthode sensiblement différente, qui permet de traiter en même temps le cas où α est un élément transcendant par rapport à K .

L'extension simple $K(\alpha)$, où α est algébrique ou transcendant par rapport à K , contient l'anneau A des expressions rationnelles entières en α à coefficients dans K ; A est d'ailleurs un domaine d'intégrité, comme sous-anneau d'un corps. L'application

$$(2) \quad h(x) \rightarrow h(\alpha), \quad \text{où } h(x) \in K[x],$$

de $I = K[x]$ sur A est, d'après le principe de spécialisation, un homomorphisme : $K[x] \sim A$. En appliquant le théorème d'homomorphisme pour les anneaux, nous obtenons :

$$(3) \quad A \simeq K[x]/\mathfrak{a},$$

où $\mathfrak{a}$ est l'idéal des polynomes $h(x)$ de $K[x]$ auxquels l'application (2) fait correspondre l'élément zéro de A : $h(\alpha) = 0$. A étant un domaine d'intégrité, $K[x]/\mathfrak{a}$ en est un ; l'idéal $\mathfrak{a}$ est donc *premier*. Cet idéal est d'autre part *principal*, puisque l'anneau $K[x]$ est euclidien : soit $\mathfrak{a} = (f)$. Deux cas sont alors possibles. Ou bien le polynome $f(x)$ est nul, et alors il n'existe aucun polynome non nul de $K[x]$ prenant pour $x = \alpha$ la valeur zéro : α est donc *transcendant* par rapport à K . Ou bien le polynome f est différent de zéro, et alors α est *algébrique* par rapport à K . Étudions séparément ces deux cas.

1° $f(x) = 0$, α *transcendant*. — D'après (3), les domaines d'intégrité A et $K[x] = K[x]/(0)$ sont *isomorphes* ; leurs corps des quotients $K(\alpha)$ et $K(x)$ le sont aussi, et même sont *isomorphes sur K* , puisque, dans (2), les éléments de K se correspondent à eux-mêmes. Appelons *extensions équivalentes* des sur-corps de K qui sont isomorphes sur K , nous avons la proposition suivante :

THÉOREME 1. — *Toute extension transcendante simple de K est isomorphe sur K au corps des fractions rationnelles en x à coefficients dans K ; par conséquent, deux extensions transcendantes simples de K sont équivalentes.*

2° $f(x) \neq 0$, α *algébrique*. — Alors le polynome caractéristique f a un *degré positif*, sans quoi la constante non nulle $f \in K$ aurait pour image zéro dans l'application (2), ce qui est impossible puisque l'image d'une constante est cette constante elle-même ; f a même un degré supérieur à 1 si l'on suppose que α n'appartient pas à K , c'est-à-dire que l'on a $K(\alpha) \neq K$. De plus, f est *irréductible*, puisque l'idéal $\mathfrak{a}$ est premier (chap. VI, § 3, p. 318) ; mais alors l'idéal $\mathfrak{a}$ est non seulement premier, mais *sans diviseurs* (*ibid.*), donc $K[x]/\mathfrak{a}$ est un corps, et A également. Par suite, les relations $K \subseteq A$ et $\alpha \in A$ entraînent $K(\alpha) \subseteq A$; comme nous avons, d'autre part, $A \subseteq K(\alpha)$, il vient

$$A = K(\alpha), \quad \text{d'où} \quad K(\alpha) \simeq K[x]/\mathfrak{a}$$

et, puisque chaque élément de K se correspond à lui-même,

$$K(\alpha) \underset{(K)}{\simeq} K[x]/(f).$$

Nous pouvons donc énoncer le théorème suivant :

THÉORÈME 2. — *Toute extension algébrique simple $K(\alpha)$ d'un corps K est isomorphe sur K au corps des classes résiduelles $K[x]/(f)$, où $f(x)$ est un polynome non nul irréductible sur K [polynome caractéristique de α ou de $K(\alpha)$]. Par conséquent, deux extensions algébriques simples correspondant au même polynome caractéristique sont équivalentes.*

Décomposons le polynome caractéristique $f(x)$ en facteurs irréductibles dans l'anneau $\Sigma[x]$. Nous aurons au moins un facteur linéaire $x - \alpha$, de sorte que nous pouvons écrire, en mettant en évidence les facteurs linéaires et en posant, par raison de symétrie $\alpha = \alpha_1$,

$$(4) \quad f(x) = (x - \alpha_1) \dots (x - \alpha_\sigma) f_1(x) \dots f_v(x) \quad (\sigma \geq 1),$$

où les $f_i(x)$ sont des polynomes irréductibles sur Σ , de degré supérieur à l'unité. Il peut d'ailleurs arriver que ces polynomes n'existent pas. Les éléments $\alpha_1 = \alpha$, $\alpha_2, \dots, \alpha_\sigma$ qui sont les zéros, appartenant à Σ , d'un même polynome $f(x)$ irréductible sur K , sont dits *conjugués dans Σ par rapport à K* . Les extensions algébriques simples $K(\alpha_1), \dots, K(\alpha_\sigma)$, équivalentes d'après ce qui précède, sont dites elles-mêmes conjuguées.

Remarque et exemple. — Soit $\Sigma_0 = K(\alpha_1, \dots, \alpha_\sigma) \subseteq \Sigma$ le corps obtenu en adjoignant à K α_1 et les éléments conjugués $\alpha_2, \dots, \alpha_\sigma$. Le polynome $F = (x - \alpha_1) \dots (x - \alpha_\sigma)$ appartient à $\Sigma_0[x]$; f aussi; comme F divise f dans $\Sigma[x]$, il le divise également dans $\Sigma_0[x]$; nous avons donc

$$Q(x) = f_1(x) \dots f_v(x) \in \Sigma_0[x]$$

et

$$f(x) = (x - \alpha_1) \dots (x - \alpha_\sigma) Q(x).$$

Σ_0 est le plus petit sous-corps de Σ dans lequel f est divisible par les facteurs linéaires $(x - \alpha_1), \dots, (x - \alpha_\sigma)$.

Prenons, par exemple, comme corps K le corps Γ des nombres rationnels; comme sur-corps Σ le corps $\mathbf{P}$ des nombres réels, comme élément α le nombre algébrique $\sqrt[4]{2}$, dont le polynome caractéristique est $f(x) = x^4 - 2$. Les éléments conjugués sont, dans $\mathbf{P}$, $\alpha_1 = \sqrt[4]{2}$ et $\alpha_2 = -\sqrt[4]{2}$, et l'on a pour f la décomposition

$$x^4 - 2 = (x - \sqrt[4]{2}) (x + \sqrt[4]{2}) (x^2 + \sqrt{2}),$$

$x^2 + \sqrt{2}$ étant irréductible sur $\mathbf{P}$. Les extensions simples $\Gamma(\sqrt[4]{2})$, $\Gamma(-\sqrt[4]{2})$ sont ici, non seulement équivalentes, mais identiques et coïncident avec le plus petit sous-corps Σ_0 de $\mathbf{P}$ dans lequel la décomposition précédente a lieu.

Un problème différent de celui qui vient d'être traité, et même en quelque sorte opposé, consiste, étant donné un corps K et un polynome $f(x)$ irréductible sur K et de degré supérieur à 1, à *construire, par un procédé purement algébrique, un sur-corps de K dans lequel $f(x)$ admette un zéro* : il suffit évidemment de chercher une extension algébrique *simple* $K' = K(\alpha)$ de K telle que l'on ait $f(\alpha) = 0$ dans K' . Un tel corps K' est appelé *corps de rupture* du polynome $f(x)$. Ultérieurement, nous construirons, également par un procédé algébrique, un *corps de décomposition* de $f(x)$, c'est-à-dire un sur-corps Δ de K dans lequel f se décompose en facteurs tous linéaires, aucun corps compris strictement entre K et Δ n'ayant la même propriété.

La méthode pour construire un corps de rupture est suggérée par les résultats obtenus plus haut : l'anneau des classes résiduelles $K[x]/(f(x))$, parfaitement défini une fois K et f donnés, est un corps puisque, f étant irréductible sur K , l'idéal (f) est sans diviseurs; le corps $K(\alpha)$ cherché doit lui être isomorphe. Considérons donc, *a priori*, ce corps des classes résiduelles $K_1 = K[x]/(f(x))$. Les classes $\bar{a}$ contenant les éléments a de K correspondent biunivoquement à ces éléments, car deux éléments distincts de K ne peuvent pas être congrus modulo f ; par suite, ces classes constituent un corps K_1 isomorphe à K . Par le procédé indiqué précédemment (chap. III, § 8, p. 132), nous pouvons *identifier* la classe $\bar{a}$ et l'élément a , en d'autres termes former un corps K' isomorphe à K_1 et contenant K comme sous-corps.

Ce corps K' est l'extension cherchée. Soit, en effet, α l'élément de K' qui a pour image dans K_1 la classe $\bar{x}$ contenant le polynome x de $K[x]$. L'élément $f(\alpha)$ a pour image la classe contenant $f(x)$, c'est-à-dire la classe zéro. Mais l'élément zéro de K' a aussi pour image cette classe; nous avons donc, dans K'

$$f(\alpha) = 0,$$

ce qu'il fallait démontrer. On remarquera, en outre, que tous les éléments du corps K' peuvent, d'après la définition de ce corps, se mettre sous la forme d'expressions rationnelles entières en α , à coefficients dans K : nous avons donc $K' = K(\alpha) = K[\alpha]$; en d'autres termes, K' est bien une *extension algébrique simple* de K . On peut lui substituer, comme corps de rupture, toute extension équivalente.

Ce procédé de construction purement algébrique, du corps de rupture K' d'un polynome f irréductible sur K , est connu sous le nom d'*adjonction symbolique*. Donnons-en quelques applications.

1° THÉOREME 3. — *Tout corps Λ de caractéristique p dans lequel certains éléments n'ont pas de racine $p^{\text{lème}}$, est imparfait* ⁽¹⁾.

Soit, en effet, $a \in \Lambda$ un élément n'ayant pas de racine $p^{\text{lème}}$ dans Λ . Considérons le polynome

$$F(x) = x^p - a$$

et soit $f(x)$ un facteur irréductible de $F(x)$ dans $\Lambda[x]$: le degré de f est évidemment supérieur à 1. Si $\Lambda(\alpha) = \Lambda'$ désigne un corps de rupture de f , α est, dans Λ' , racine de l'équation $F(\alpha) = 0$, d'où

$$\alpha^p = a \quad \text{et} \quad F(x) = x^p - \alpha^p = (x - \alpha)^p,$$

ce qui entraîne

$$f(x) = (x - \alpha)^r, \quad \text{où} \quad 1 < r \leq p,$$

$f(x)$ est donc un polynome irréductible *inséparable* sur Λ et Λ est imparfait.

Remarque. — Le polynome irréductible $f(x)$, admettant un zéro multiple, a une dérivée nulle; par conséquent, son degré r est multiple de p : le raisonnement fait dans la démonstration entraîne donc $r = p$ et $F = f$; donc, si un élément a d'un corps Λ de caractéristique p n'admet pas de racine $p^{\text{lème}}$ dans ce corps, $x^p - a$ est irréductible sur Λ .

2° Tout nombre algébrique α peut être défini, à partir du corps Γ des nombres rationnels, par le procédé de l'adjonction symbolique. Celui-ci nous fournit donc, en premier lieu, une nouvelle définition des nombres algébriques *réels* tels que $\sqrt{2}$, $\sqrt{2} + \sqrt{3}$, ... On remarquera que les deux extensions $\Gamma(\sqrt{2})$, par exemple, définies l'une comme sous-corps du corps $\mathbf{P}$ des nombres réels, l'autre comme corps de rupture de $x^2 - 2$ sur le corps Γ des nombres rationnels, sont *équivalentes* (par rapport à Γ) et, par conséquent, jouent des rôles identiques, bien que les deux symboles $\sqrt{2}$ correspondants soient de natures bien différentes.

D'autre part, l'adjonction symbolique permet de construire pour *tout* polynome irréductible d'un corps $K[x]$, un élément α qui en soit un zéro : pour $K = \Gamma$, l'introduction des nombres réels n'avait permis de résoudre ce problème que pour des polynomes particuliers, par exemple pour $x^2 - 2$, mais non pour $x^2 + 1$, qui est irréductible sur $\mathbf{P}$ comme sur Γ .

(1) Donc, dans un corps de caractéristique p , l'existence d'une racine $p^{\text{ième}}$ pour tout élément du corps est une condition nécessaire et suffisante pour que le corps soit parfait (cf. § 1, th. 5, p. 364).

Dans ce qui suit, nous allons précisément étudier le corps de rupture Ω , sur $\mathbf{P}$, du polynome $x^2 + 1$; ce corps Ω , extension algébrique simple de $\mathbf{P}$, $\Omega = \mathbf{P}(i)$, est en même temps corps de décomposition de $x^2 + 1$, puisque ce polynome est du deuxième degré. L'élément conjugué de i est $-i$ et l'on a dans $\Omega[x]$ la décomposition

$$x^2 + 1 = (x + i)(x - i).$$

Les éléments de Ω sont appelés *nombre complexes* : tout nombre est une expression rationnelle entière en i de degré au plus égal à 1, de la forme

$$\alpha = a + a'i \quad (a, a' \in \mathbf{P}).$$

Cette représentation est unique

$$a + a'i = b + b'i \quad \text{entraîne} \quad a = b, \quad a' = b'.$$

Les règles de calcul sur les nombres complexes sont les mêmes que sur les classes résiduelles modulo $x^2 + 1$ ⁽¹⁾.

$$\begin{aligned} (a + a'i) + (b + b'i) &= (a + b) + (a' + b')i, \\ (a + a'i) \cdot (b + b'i) &= (ab - a'b') + (ab' + ba')i. \end{aligned}$$

Le nombre $\bar{\alpha} = a - a'i$ est dit *imaginaire conjugué* de $\alpha = a + a'i$. La somme $\alpha + \bar{\alpha} = 2a$ et le produit $\alpha\bar{\alpha} = a^2 + a'^2$ de deux nombres imaginaires conjugués sont réels.

De la relation $i^2 = -1$ résulte que le corps Ω des nombres complexes n'est pas un corps ordonné, puisqu'un carré peut y être négatif. Cependant en posant

$$|\alpha| = \sqrt{\alpha\bar{\alpha}} = \sqrt{a^2 + a'^2},$$

on définit une fonction $|\alpha|$, appelée *module* de α , coïncidant avec la valeur absolue de α lorsque α est réel, et ayant, dans le cas général, des propriétés analogues. On a, en effet,

$$\begin{aligned} |-\alpha| &= |\alpha|, \\ |\alpha\beta| &= \sqrt{\alpha\beta\bar{\alpha}\bar{\beta}} = \sqrt{\alpha\bar{\alpha}\beta\bar{\beta}} = \sqrt{\alpha\bar{\alpha}}\sqrt{\beta\bar{\beta}} = |\alpha| |\beta| \end{aligned}$$

et, en posant $\beta = b + b'i$,

$$|\alpha - \beta| = \sqrt{(a - b)^2 + (a' - b')^2} \leq \sqrt{a^2 + a'^2} + \sqrt{b^2 + b'^2} = |\alpha| + |\beta|$$

car la distance de deux points $A(a, a')$, $B(b, b')$ du plan est au plus

⁽¹⁾ Ce mode de définition des nombres complexes a été donné par Cauchy lui-même (*Exercices d'Analyse*, t. 4, 1847, p. 68).

égale à la somme des distances OA, OB ; en changeant β en $-\beta$, il vient

$$|\alpha + \beta| \leq |\alpha| + |\beta|.$$

Tout nombre complexe $\alpha = a + a'i$ est racine d'une équation du second degré sur $\mathbf{P}$, équation irréductible si α n'est pas réel : en effet, le polynome

$$f(x) = (x - \alpha)(x - \bar{\alpha}) = x^2 - 2ax + a^2 + a'^2$$

appartient à l'anneau $\mathbf{P}[x]$; et ses zéros sont α et $\bar{\alpha}$. Nous voyons de plus que deux imaginaires conjuguées α et $\bar{\alpha}$ sont *conjuguées par rapport à $\mathbf{P}$* , au sens donné à cette expression dans la théorie générale.

Inversement, tout polynome $f(x) = x^2 + px + q \in \mathbf{P}[x]$, du second degré et irréductible sur $\mathbf{P}$, admet deux zéros conjugués dans Ω . On a, en effet,

$$f(x) = x^2 + px + q = \left(x + \frac{p}{2}\right)^2 + q - \frac{p^2}{4},$$

d'où, f étant irréductible sur $\mathbf{P}$,

$$q - \frac{p^2}{4} > 0.$$

Le nombre $r = q - \frac{p^2}{4}$ admet une racine carrée positive $\sqrt{r} \in \mathbf{P}$, et nous avons, dans $\Omega[x]$,

$$f(x) = \left(x + \frac{p}{2} + i\sqrt{r}\right) \left(x + \frac{p}{2} - i\sqrt{r}\right),$$

d'où les deux zéros conjugués $-\frac{p}{2} \pm i\sqrt{r}$. Le corps des nombres complexes est donc corps de décomposition non seulement pour $x^2 + 1$, mais pour tout polynome du second degré à coefficients réels, irréductible sur $\mathbf{P}$. En fait, nous allons voir qu'il possède une propriété beaucoup plus forte.

Un corps $\mathbf{K}$ est dit *algébriquement fermé* si, dans l'anneau $\mathbf{K}[x]$, tout polynome se décompose en facteurs *linéaires*. Une condition équivalente est que tout polynome $f(x) \in \mathbf{K}[x]$ admette au moins un zéro dans $\mathbf{K}$: s'il en est ainsi, on a, en effet,

$$f(x) = (x - \alpha)f_1(x), \quad \text{avec } \alpha \in \mathbf{K}, \quad f_1(x) \in \mathbf{K}[x];$$

$f_1(x)$ admet à son tour un zéro dans $\mathbf{K}$, donc est divisible dans $\mathbf{K}[x]$ par un facteur linéaire, et l'on obtient ainsi, de proche en proche, une décomposition de f en facteurs linéaires dans $\mathbf{K}[x]$.

THÉORÈME. — *Le corps Ω des nombres complexes est algébriquement fermé.*

Cette importante propriété est connue sous le nom de *théorème fondamental de l'Algèbre*. On peut encore l'énoncer de la manière suivante :

THÉORÈME DE D'ALEMBERT. — *Tout polynome $f(x) \in \Omega[x]$, de degré ≥ 1 , admet au moins un zéro dans Ω .*

Ces deux énoncés sont des conséquences presque immédiates des propositions concernant les fonctions d'une variable complexe. Si le polynome $f(x)$ n'a aucun zéro dans le plan complexe, la fonction $\frac{1}{f(x)}$, régulière dans tout le plan et demeurant bornée quand x tend vers l'infini, est égale à une constante non nulle, d'après le *théorème de Liouville* ⁽¹⁾, et il en est de même de $f(x)$.

On peut encore déduire le théorème fondamental de l'Algèbre du *Théorème de Rouché* ⁽²⁾ : si l'on a, sur une circonférence C de centre O et de rayon R

$$(5) \quad |h(x)| < |g(x)|$$

et si les fonctions $g(x)$, $h(x)$ de la variable complexe x sont holomorphes dans et sur C , $g(x)$ et $f(x) = g(x) + h(x)$ ont le même nombre de zéros dans C . Cela étant, considérons un polynome

$$f(x) = a_0 + a_1 x + \dots + a_m x^m,$$

et posons $g(x) = a_m x^m$, $h(x) = a_0 + \dots + a_{m-1} x^{m-1}$. Nous avons, sur C

$$|g| = |a_m| R^m, \quad |h| \leq |a_0| + \dots + |a_{m-1}| R^{m-1},$$

d'où, si R est supérieur à 1,

$$|h| < (|a_0| + \dots + |a_{m-1}|) R^{m-1}.$$

⁽¹⁾ Voir, par exemple, GOURSAT, *Cours d'Analyse Mathématique*, t. 2, 4^e éd., p. 86; VALIRON, *Théorie des Fonctions*, p. 371.

⁽²⁾ Voir, par exemple, GOURSAT, *Cours d'Analyse Mathématique*, t. 2, 4^e éd., p. 114; VALIRON, *Théorie des Fonctions*, p. 391 ou TITCHMARSH, *Theory of Functions*, p. 116 (Oxford, 1932). — Au lieu d'utiliser le théorème de Rouché, on peut encore considérer l'intégrale

$$\frac{1}{2i\pi} \int \frac{f'(z)}{f(z)} dz$$

prise sur un cercle de rayon assez grand (cf. JORDAN, *Cours d'Analyse*, t. 2, 3^e éd., p. 355).

Si donc R est supérieur également à $\frac{|a_0| + \dots + |a_{m-1}|}{|a_m|}$, l'inégalité (5) sera vérifiée, et comme g possède, dans C , m zéros (confondus en 0), f admet également m zéros (1).

Considérons un polynôme à coefficients réels, $f(x) \in \mathbf{P}[x]$, de degré m supérieur à 1, et irréductible sur $\mathbf{P}$: $f(x)$ admet dans Ω m zéros non réels. Or, si α est zéro de f , $\bar{\alpha}$ l'est également : si, en effet, on remplace les termes d'une somme ou les facteurs d'un produit par des quantités conjuguées, le résultat est remplacé par la quantité conjuguée ; nous avons donc, puisque les coefficients de f sont réels

$$f(\bar{\alpha}) = \overline{f(\alpha)} = 0$$

et $f(x)$ est divisible par le polynôme $(x - \alpha)(x - \bar{\alpha})$, qui appartient à l'anneau $\mathbf{P}[x]$. Comme f est irréductible sur $\mathbf{P}$, il en résulte

$$f(x) = a(x - \alpha)(x - \bar{\alpha}) \quad (a \in \mathbf{P}),$$

d'où $m = 2$, et nous avons la proposition suivante :

THÉORÈME. — *Dans l'anneau $\mathbf{P}[x]$ des polynômes à coefficients réels, les seuls polynômes irréductibles sont, avec ceux du premier degré, les polynômes du second degré n'ayant pas leurs zéros réels.*

Une autre conséquence du théorème fondamental concerne l'équation binôme

$$x^m - a = 0 \quad (a \in \Omega);$$

cette équation a, dans Ω , m racines $\xi_1, \dots, \xi_m$, qui sont distinctes si a est différent de zéro, ce que nous supposons, et se déduisent toutes de l'une d'entre elles en la multipliant par les m racines $\xi_1, \dots, \xi_m$ de l'équation

$$z^m - 1 = 0.$$

$\xi_1, \dots, \xi_m$ sont appelées racines $m^{\text{ièmes}}$ de l'unité. Les racines $m^{\text{ièmes}}$ de l'unité forment par rapport à la multiplication un groupe abélien Γ_m d'ordre m , car les égalités $\xi^{mi} = \xi^{lm} = 1$ entraînent $(\xi \xi^{l-1})^m = 1$. On a, d'autre part,

$$|\xi|^m = 1, \quad \text{d'où} \quad |\xi| = 1;$$

(1) Pour une démonstration utilisant seulement les propriétés des fonctions continues, voir par exemple JORDAN, *Cours d'Analyse*, t. 1, 3^e éd., p. 203, ainsi que VALIRON, *Théorie des Fonctions*, p. 68.

le groupe Γ_m est donc un sous-groupe du groupe multiplicatif Γ des nombres complexes de module 1.

Cela posé, si l'on représente chaque nombre complexe $\xi = x + ix'$ par le point du plan dont les coordonnées cartésiennes sont x et x' , un nombre $\alpha = a + ia'$ de module 1 est représenté par le point du cercle-unité dont l'angle polaire φ , appelé *argument* de α , est donné par

$$a = \cos \varphi, \quad a' = \sin \varphi.$$

De la relation

$$(a + ia')(b + ib') = ab - a'b' + i(ab' + ba')$$

et des formules d'addition du cosinus et du sinus résulte que l'*argument d'un produit est la somme des arguments des facteurs* ⁽¹⁾: le groupe multiplicatif Γ des nombres complexes de module 1 est donc isomorphe au groupe des rotations de centre O, et l'on a la *formule de Moivre*

$$(\cos \varphi + i \sin \varphi)^m = \cos m\varphi + i \sin m\varphi.$$

D'après cette formule, les m racines $m^{\text{ièmes}}$ de l'unité sont les nombres

$$\zeta_k = \cos \frac{2k\pi}{m} + i \sin \frac{2k\pi}{m} \quad (k = 1, 2, \dots, m),$$

qui forment bien un groupe multiplicatif Γ_m , isomorphe au *groupe cyclique* des rotations de centre O et d'angle multiple de $\frac{2\pi}{m}$. Toute racine génératrice du groupe Γ_m est dite *primitive*: la racine ζ_1 l'est visiblement. Pour qu'une autre racine $\zeta_k = \zeta_1^k$ le soit, il faut et il suffit, d'après les propriétés générales des groupes cycliques (chap. IV, § 4, p. 156) que k soit premier à m .

Nous reviendrons ultérieurement (t. II) sur la théorie des équations algébriques, par des procédés qui nous donneront des résultats plus généraux et plus étendus.

Exercices 1. — On appelle *entiers de Gauss* les nombres complexes de la forme

$$\alpha = a + bi,$$

où a et b sont des entiers relatifs. Montrer que ces nombres forment un domaine d'intégrité G dont le corps des quotients est l'extension simple $\Gamma(i)$ du corps Γ des nombres rationnels. Déterminer les unités du domaine G . En prenant comme fonction $g(\alpha)$ la *norme* de α , c'est-à-dire la quantité $a^2 + b^2$, montrer que G est un anneau euclidien.

(1) A un multiple de 2π près.

2. Décomposer le polynome $x^4 + 1$ en facteurs irréductibles :

1° dans le corps $\Gamma(i)$;

2° dans le corps Ω des nombres complexes.

Quel est le plus petit sous-corps de Ω dans lequel $x^4 + 1$ se décompose en facteurs linéaires ?

3. **Applications géométriques; théorème de Noether.** — Soit Ω un corps algébriquement fermé, par exemple le corps des nombres complexes. Étudions les idéaux premiers de l'anneau $A = \Omega[x, y]$ des polynomes à deux variables x, y , à coefficients dans Ω .

THÉORÈME 1. — *Un idéal premier $\mathfrak{p}$ de l'anneau A , s'il n'est pas principal, est l'ensemble des polynomes nuls en un point :*

$$\mathfrak{p} = (x - \alpha, y - \beta) \quad (\alpha, \beta \in \Omega).$$

Montrons que l'idéal $\mathfrak{p}$ contient un polynome de la forme $x - \alpha$ ($\alpha \in \Omega$) ; il contiendra de même un polynome de la forme $y - \beta$ ($\beta \in \Omega$), d'où

$$(x - \alpha, y - \beta) \subseteq \mathfrak{p}.$$

Or, le premier membre est un idéal sans diviseurs (chap. VI, § 5) ; puisque $\mathfrak{p}$ est différent de l'idéal-unité A engendré par l'élément-unité de Ω , et par conséquent principal, nous avons bien

$$(x - \alpha, y - \beta) = \mathfrak{p}.$$

Pour établir que $\mathfrak{p}$ contient un polynome de la forme $x - \alpha$, il suffit de montrer qu'il existe dans $\mathfrak{p}$ un polynome non nul indépendant de y , $\varphi(x)$. S'il en est ainsi, en effet, $\varphi(x)$ qui ne peut pas se réduire à une constante ($\mathfrak{p} \neq A$), est de la forme

$$\varphi(x) = a(x - \alpha_1)^{\nu_1} \dots (x - \alpha_k)^{\nu_k} \quad (k \geq 1, \alpha_i \in \Omega, \alpha_i \neq \alpha_j, a \neq 0)$$

puisque Ω est algébriquement fermé. Le facteur constant a n'appartenant pas à $\mathfrak{p}$, un au moins des facteurs $x - \alpha_i$ doit appartenir à cet idéal, puisque $\mathfrak{p}$ est premier. On ne peut d'ailleurs pas avoir simultanément

$$x - \alpha_i \in \mathfrak{p}, \quad x - \alpha_j \in \mathfrak{p} \quad (i \neq j),$$

car il en résulterait

$$\alpha_i - \alpha_j \in \mathfrak{p} \quad \text{et} \quad \mathfrak{p} = A.$$

N'étant pas principal, l'idéal $\mathfrak{p}$ est différent de (0) . Ordonnons en y les polynomes non nuls de $\mathfrak{p}$ et soit n le minimum de leur degré en y : nous devons montrer que n est nul. *Supposons, au contraire, $n > 0$.*

Parmi les polynomes de $\mathfrak{p}$ qui sont de degré n en y , il en existe au moins un,

$$\varphi(x, y) = a_0(x)y^n + \dots + a_n(x) \quad (a_i \in \Omega[x]),$$

qui n'est divisible par aucun polynome en x seul (si en effet un tel facteur $\psi(x)$ existe, ψ n'appartient pas à $\mathfrak{p}$ puisque n est positif, et le quotient φ/ψ appartient à $\mathfrak{p}$).

Cela posé, soit

$$\psi(x, y) = b_0(x)y^m + \dots + b_m(x) \quad (b_i \in \Omega[x], m \geq n)$$

un polynome quelconque de $\mathfrak{p}$. Divisons le produit $\alpha_0^{m-n+1}(x)\psi(x, y)$ par $\varphi(x, y)$ suivant les puissances décroissantes de y :

$$\alpha_0^{m-n+1}\psi(x, y) = q(x, y)\varphi(x, y) + r(x, y)$$

où (à cause du facteur α_0^{m-n+1}) $q(x, y)$ et $r(x, y)$ sont certainement des polynomes de l'anneau $\mathbf{A}$. Nous avons $r \in \mathfrak{p}$; comme le degré de r en y est inférieur à n , r est nul. L'égalité

$$\alpha_0(x)^{m-n+1}\psi(x, y) = q(x, y)\varphi(x, y)$$

dans l'anneau à factorisation unique $\mathbf{A}$ exige, puisque $\varphi(x, y)$ n'est divisible par aucun polynome en x seul, que $\alpha_0(x)^{m-n+1}$ divise $q(x, y)$. Mais alors $\psi(x, y)$ est multiple de $\varphi(x, y)$ et nous avons $\mathfrak{p} = (\varphi)$, contrairement à l'hypothèse. Le degré n de φ est donc nécessairement nul, ce qui démontre le théorème.

Considérons deux courbes algébriques planes $f=0$, $g=0$, où f et g sont deux polynomes de l'anneau $\mathbf{A} = \Omega[x, y]$; nous supposons que f et g n'appartiennent pas à un même idéal principal. Pour obtenir le théorème de Noether concernant l'intersection de ces deux courbes, utilisons, en tenant compte du théorème précédent, la décomposition normée de l'idéal (f, g) en intersection d'idéaux premiers (chap. IV, § 14, p. 212) :

$$(f, g) = \mathfrak{m} = \mathfrak{q}_1 \cap \dots \cap \mathfrak{q}_r.$$

Désignons par $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ les idéaux premiers associés respectivement à $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ et appelés *idéaux premiers essentiels* de $\mathfrak{m}$; nous avons

$$f \in \mathfrak{m} \subseteq \mathfrak{q}_i \subseteq \mathfrak{p}_i, \quad g \in \mathfrak{m} \subseteq \mathfrak{q}_i \subseteq \mathfrak{p}_i.$$

De l'hypothèse faite sur f et g résulte que $\mathfrak{p}_i$ n'est pas principal; nous avons donc, d'après le théorème 1,

$$\mathfrak{p}_i = (x - \alpha_i, y - \beta_i) \quad (\alpha_i, \beta_i \in \Omega),$$

et le point M_i de coordonnées α_i, β_i appartient aux deux courbes $f = 0$, $g = 0$.

Inversement, tout point $M(\alpha, \beta)$, où $\alpha, \beta \in \Omega$, commun aux deux courbes $f = 0$, $g = 0$, figure parmi les points M_i . Posons, en effet,

$$p = (x - \alpha, y - \beta).$$

Nous avons par hypothèse $f \in p, g \in p$, donc

$$m = (f, g) \subseteq p,$$

d'où, en désignant par ρ_i l'exposant de l'idéal primaire q_i ,

$$p^{\rho_1} \dots p^{\rho_r} \subseteq q_1 \cap \dots \cap q_r = m \subseteq p,$$

ce qui exige qu'un au moins des idéaux essentiels p_i soit contenu dans l'idéal premier p :

$$p_\lambda \subseteq p, \quad \text{d'où} \quad p_\lambda = p,$$

puisque, comme chaque p_i, p_λ est un idéal sans diviseurs. M coïncide donc avec le point M_λ et il y a correspondance biunivoque entre les points communs aux deux courbes et les idéaux premiers essentiels de l'idéal $m = (f, g)$: il en résulte notamment que *les points d'intersection des deux courbes sont en nombre fini*.

Le fait que les idéaux premiers essentiels p_i de α sont sans diviseurs entraîne pour les composants primaires q_i une forme remarquable. Considérons l'un d'eux, q_1 par exemple que nous désignerons plus simplement par q ; soient p l'idéal premier associé, ρ l'exposant de q , σ un nombre naturel quelconque ; nous avons :

$$p^\sigma \subseteq m + p^\sigma \subseteq p;$$

par suite, puisque p est un idéal sans diviseurs, $m + p^\sigma = q'$ est un idéal primaire, appartenant à p . Nous avons, d'autre part,

$$(1) \quad qq_2 \dots q_r \subseteq q \cap q_2 \cap \dots \cap q_r = m \subseteq q'$$

et

$$(2) \quad q_2 \dots q_r \not\subseteq p,$$

car $q_i \subseteq p$ entraînerait $p_i^{\rho_i} \subseteq p$, donc $p_i \subseteq p$, ce qui n'est pas. De (1) et (2) résulte

$$q \subseteq q' \quad (\text{quel que soit } \sigma).$$

Si l'on prend $\sigma \geq \rho$, on a $p^\sigma \subseteq p^\rho \subseteq q$; puisque $m (= q \cap q_2 \cap \dots \cap q_r)$ est également contenu dans q , nous avons $q' \subseteq q$, d'où $q' = q$, et nous

pouvons écrire

$$(3) \quad \mathfrak{m} + \mathfrak{p}^\rho = \mathfrak{m} + \mathfrak{p}^{\rho+1} = \dots = \mathfrak{q}.$$

Quant à l'idéal $\mathfrak{m} + \mathfrak{p}^{\rho-1}$, défini seulement si ρ est supérieur à 1, il est *strictement* contenu dans $\mathfrak{q}$, car l'égalité $\mathfrak{m} + \mathfrak{p}^{\rho-1} = \mathfrak{q}$ entraînerait $\mathfrak{p}^{\rho-1} \subseteq \mathfrak{q}$, ce qui est contraire à la définition de l'exposant ρ .

Puisque $\mathfrak{p}$ est l'idéal des polynômes de Λ nuls en un point $M(\alpha, \beta)$, $\mathfrak{p}^\rho$ est l'ensemble des polynômes d'ordre supérieur ou égal à ρ en M , c'est-à-dire tels que, développés suivant les puissances croissantes de $x - \alpha$, $y - \beta$, ils commencent par des termes de degré ρ au moins. D'après (3), le composant primaire $\mathfrak{q}$ relatif au point M est l'ensemble des polynômes φ qui peuvent se mettre sous la forme

$$uf + v\psi + \psi \quad (u, v, \psi \in \Lambda),$$

ψ étant d'ordre au moins égal à ρ au point M .

En opérant de même pour les différents composant primaires $\mathfrak{q}_i$ et en revenant à la formule de décomposition

$$\mathfrak{m} = \mathfrak{q}_1 \cap \mathfrak{q}_2 \cap \dots \cap \mathfrak{q}_r,$$

nous obtenons l'importante proposition suivante :

THÉOREME 2 (THÉOREME DE NOETHER). — Ω désignant un corps algébriquement fermé, soient f, g deux polynômes de l'anneau $\Lambda = \Omega[x, y]$ qui n'appartiennent pas à un même idéal principal. Pour qu'un polynôme $\varphi \in \Lambda$ appartienne à l'idéal $\mathfrak{m} = (f, g)$, il faut et il suffit qu'en chaque point $M_i(\alpha_i, \beta_i)$ commun aux courbes $f = 0, g = 0$, on puisse trouver des polynômes u_i, v_i , tels que la différence $\varphi - u_i f - v_i g$ soit d'ordre suffisamment élevé. D'une façon précise, cet ordre doit être au moins égal à l'entier ρ_i , exposant du composant primaire $\mathfrak{q}_i$, appelé en Géométrie multiplicité de Noether.

Remarque. — Il est évident que la condition énoncée dans le théorème 2 est nécessaire; soit en effet $\varphi = af + bg$ ($a, b \in \Lambda$); en prenant $u_i = a, v_i = b$ quel que soit i , on obtient des différences $\varphi - u_i f - v_i g$ identiquement nulles, c'est-à-dire d'ordre infini. L'importance de la condition vient de ce qu'elle est suffisante. Souvent d'ailleurs, dans les applications, on peut se contenter de conditions suffisantes plus restrictives, généralement plus faciles à établir. Par exemple, la relation immédiate

$$\mathfrak{p}_1^{\rho_1} \cap \dots \cap \mathfrak{p}_r^{\rho_r} \subseteq \mathfrak{m} = (f, g)$$

permet d'affirmer que tout polynôme d'ordre au moins égal à ρ_i en chaque point M_i appartient à l'idéal (f, g) , ce qui résulte aussi, bien entendu, de l'énoncé général : on a ici $u_i = v_i = 0$ pour tout i .

Prenons l'un des points d'intersection M_i comme origine des coordonnées, désignons par $\mathfrak{p}$ l'idéal (x, y) et étudions le composant primaire $\mathfrak{q}$ correspondant de l'idéal $\mathfrak{m} = (f, g)$.

LEMME. — *L'idéal $\mathfrak{q}$ est l'ensemble des polynômes q de l'anneau $\mathbb{A}$ auxquels on peut associer un polynôme h de $\mathbb{A}$ ne s'annulant pas à l'origine, $h \notin \mathfrak{p}$, tel que qh appartienne à $\mathfrak{m}$.*

1° Si $q \in \mathfrak{q}$, soit h un polynôme appartenant aux autres composants primaires $\mathfrak{q}_i$ de $\mathfrak{m}$ et ne s'annulant pas en O , un tel polynôme existe bien car, dans le cas contraire, nous aurions $\mathfrak{q}_2 \cap \dots \cap \mathfrak{q}_r \subseteq \mathfrak{p}$, d'où $\mathfrak{p}_2^{\alpha_2} \dots \mathfrak{p}_r^{\alpha_r} \subseteq \mathfrak{p}$ et, pour au moins une valeur de i , $\mathfrak{p}_i \subseteq \mathfrak{p}$. Le produit qh appartient à tous les composants primaires de $\mathfrak{m}$, donc aussi à $\mathfrak{m}$.

2° Soit $qh \in \mathfrak{m}$, donc $qh \in \mathfrak{q}$. Si $h \notin \mathfrak{p}$, on a $q \in \mathfrak{q}$.

Cela posé, écrivons

$$(4) \quad f = \alpha x + \beta y + f_2, \quad g = \alpha' x + \beta' y + g_2,$$

où $\alpha, \alpha', \beta, \beta' \in \Omega$ et $f_2, g_2 \in \mathfrak{p}^2$. Désignons respectivement par r, s les ordres respectifs de f et g en O : on a, par exemple, $r > 1$ si $\alpha = \beta = 0$ et seulement dans ce cas. Si $r = 1$, on dit que O est *point simple* pour la courbe $f = 0$, et que $\alpha x + \beta y = 0$ est la *tangente* en O à cette courbe.

THÉORÈME 3. — *Pour que la multiplicité de Noether de l'idéal (f, g) au point O soit égale à 1, en d'autres termes pour que l'on ait $\mathfrak{q} = \mathfrak{p}$, il faut et il suffit que les courbes $f = 0, g = 0$ admettent O comme point simple et que leurs tangentes en O soient distinctes, ce qui s'exprime par l'unique condition*

$$\alpha\beta' - \beta\alpha' \neq 0.$$

1° *La condition est nécessaire.* — Si $\mathfrak{q} = \mathfrak{p}$, toute forme linéaire $\lambda x + \mu y$ ($\lambda, \mu \in \Omega$) appartient à $\mathfrak{q}$, donc vérifie, d'après le lemme, une égalité de la forme

$$(\lambda x + \mu y)h = af + bg, \quad (a, b \in \mathbb{A}, h \notin \mathfrak{p}).$$

Le terme constant du polynôme h n'étant pas nul, cette égalité ne peut avoir lieu pour toutes les valeurs de λ et μ que si les termes du premier ordre existent effectivement dans f et g et n'y sont pas proportionnels, donc si $\alpha\beta' - \beta\alpha' \neq 0$.

2° *La condition est suffisante.* — On tire des équations (4)

$$(\alpha'\beta' - \beta\alpha')x = \beta'f - \beta g + t_2, \quad (t_2 \in \mathfrak{p}^2).$$

La condition $\alpha\beta' - \beta\alpha' \neq 0$ entraîne donc

$$x \in (f, g, \mathfrak{p}^2) \quad \text{et, de même,} \quad y \in (f, g, \mathfrak{p}^2),$$

donc

$$\mathfrak{p} \subseteq \mathfrak{m} + \mathfrak{p}^2,$$

d'où

$$\mathfrak{p}^\nu \subseteq \mathfrak{m}\mathfrak{p}^{\nu-1} + \mathfrak{p}^{\nu+1} \subseteq \mathfrak{m} + \mathfrak{p}^{\nu+1},$$

donc, pour tout nombre naturel σ ,

$$\mathfrak{m} + \mathfrak{p}^\sigma \subseteq \mathfrak{m} + \mathfrak{p}^{\sigma+1},$$

d'où l'égalité puisque $\mathfrak{p}^{\sigma+1}$ est contenu dans $\mathfrak{p}^\sigma$.

Ainsi, nous avons

$$\mathfrak{m} + \mathfrak{p} = \mathfrak{m} + \mathfrak{p}^2 = \mathfrak{m} + \mathfrak{p}^3 = \dots,$$

ce qui entraîne $\rho = 1$, $\eta = \mathfrak{p}$.

Les théorèmes 2 et 3 fournissent l'équation générale des courbes algébriques passant par les différents points d'intersection M_i des deux courbes données $f=0$, $g=0$ lorsque ces points sont simples pour les deux courbes et que celles-ci n'y présentent aucun contact. Cette équation s'écrit

$$af + bg = 0 \quad (a, b \in \Lambda).$$

Il s'agit, dans tout ce qui précède, uniquement des points d'intersection « à distance finie ». Passons au plan projectif dans lequel un point est l'ensemble de trois éléments X, Y, Z de Ω , non tous nuls, définis à un facteur de proportionnalité près (voir Note IV). Soient $F=0$, $G=0$ les courbes du plan projectif correspondant aux courbes $f=0$, $g=0$ considérées plus haut; nous avons, par exemple,

$$f(x, y) = F(x, y, 1)$$

et la forme $F(X, Y, Z)$ est supposée ne pas contenir Z en facteur.

Les résultats obtenus plus haut pour les polynômes f, g, φ sont valables même si, dans le plan projectif, les courbes $F=0$, $G=0$ ont en commun des points « à l'infini » ($Z=0$) ne comptant pas parmi les points M_i . Par exemple, si $f=x$, $g=y-x^2$ et $\varphi=y$, nous avons

$$(f, g) = (x, y - x^2) = (x, y), \\ \varphi \in (f, g) \quad \text{ou} \quad y = x \cdot x + 1(y - x^2).$$

Maïs, si nous passons aux formes correspondantes, $F = X$, $G = YZ - X^2$, $\Phi = Y$, nous obtenons

$$YZ = X \cdot X + 1(YZ - X^2).$$

La relation $\Phi \notin (F, G)$ est d'ailleurs évidente *a priori* puisque Φ ne s'annule pas au point $(0, 1, 0)$ commun à la droite $X = 0$ et à la parabole $YZ - X^2 = 0$.

Montrons que, si les courbes $F = 0$, $G = 0$ n'ont pas de points communs à l'infini, donc si $F = F(X, Y, 0)$ et $G = G(X, Y, 0)$ sont sans diviseurs communs, l'identité

$$(5) \quad \varphi = af + bg$$

entraîne

$$(6) \quad \Phi = AF + BG,$$

où A, B sont des formes.

En posant, dans (5), $x = \frac{X}{Z}$, $y = \frac{Y}{Z}$, nous obtenons

$$(7) \quad Z^v \Phi = UF + VG,$$

où U, V sont des formes. Si v n'est pas nul, la spécialisation $Z = 0$ donne

$$0 = \bar{U} \cdot \bar{F} + \bar{V} \cdot \bar{G},$$

d'où, en raison de l'hypothèse,

$$\bar{U} = P(X, Y) \bar{G}, \quad \bar{V} = -P(X, Y) \bar{F}$$

et, par conséquent,

$$U = PG + ZU_1, \quad V = -PF + ZV_1,$$

d'où, en portant dans (7),

$$Z^{v-1} \Phi = U_1 F + V_1 G.$$

En répétant l'application de ce procédé, on arrive finalement à la relation (6).

Nous nous bornerons ici à ces indications sur le théorème de Noether. Une autre méthode de démonstration repose sur la considération des polynômes de l'idéal $m = (f, g)$ qui dépendent *seulement* de x . Ces polynômes forment dans l'anneau euclidien $\Omega[x]$ un idéal *principal* dont le générateur est appelé *sous-résultant* des polynômes f, g (parce qu'il peut très bien être un diviseur véritable du *résultant* considéré dans la théorie de l'élimination et intervenant dans

le théorème de Bezout). Avec les notations employées plus haut, en supposant Ω de caractéristique nulle et moyennant un choix convenable des coordonnées, on montre que l'ordre de multiplicité d'un zéro α_i du sous-résultant est égal à l'exposant ρ_i du composant primaire q_i relatif au point d'intersection $M_i(\alpha_i, \beta_i)$. Ce fait sert de point de départ pour la détermination de la multiplicité de Noether à partir des caractères géométriques ⁽¹⁾.

Exercices. — 1. a. Soit A un anneau noethérien ayant un élément-unité. Un idéal de A contenu dans un seul idéal premier $\mathfrak{p} \neq A$ est dit *uniforme*. Montrer que tout idéal uniforme est primaire. Quelle condition doit vérifier un idéal premier $\mathfrak{p}_1$ pour qu'un idéal primaire $\mathfrak{q}_1$ appartenant à $\mathfrak{p}_1$ soit uniforme?

b. On considère dans A un idéal $m = q_1 \cap q_2 \cap \dots \cap q_r$ dont tout idéal premier essentiel p_i est maximal (c'est-à-dire distinct de A et n'ayant pas d'autre diviseur que A). De quelle forme sont les composantes primaires q_i de m ?

2. Ω désignant le corps des nombres complexes, déterminer la multiplicité de Noether à l'origine pour les deux courbes $f = 0$, $g = 0$ lorsqu'on prend

$$f = x \in \Omega[x, y], \quad g = \lambda x + y^n \in \Omega[x, y].$$

B. — FONCTIONS SYMÉTRIQUES.

4. **Théorème fondamental; méthode de Waring.** — Considérons un anneau commutatif $\mathbf{A}$ possédant un élément-unité, et l'anneau $\mathbf{R}_n = \mathbf{A}[x_1, \dots, x_n]$ des polynômes en $x_1, \dots, x_n$ à coefficients dans $\mathbf{A}$. Un polynôme de $\mathbf{R}_n$ est dit *symétrique* s'il est invariant par toute substitution effectuée sur $x_1, \dots, x_n$. Par exemple, les polynômes

$$\text{(I)} \quad \begin{cases} \sigma_1 = x_1 + x_2 + \dots + x_n = \Sigma x_i \\ \sigma_2 = x_1x_2 + \dots + x_1x_n + x_2x_3 + \dots + x_{n-1}x_n = \Sigma x_ix_j \\ \vdots \\ \sigma_n = x_1x_2\dots x_n \end{cases}$$

sont symétriques : on les désigne sous le nom de *fonctions symétriques élémentaires* des n variables $x_1, x_2, \dots, x_n$. Si $P(u)$ désigne le polynôme de l'anneau $\mathbf{R}_n[u]$ qui admet $x_1, \dots, x_n$ pour zéros, nous avons l'identité

$$(I') \quad F(u) = (u - x_1)(u - x_2) \dots (u - x_n) = u^n - \sigma_1 u^{n-1} + \sigma_2 u^{n-2} - \dots + (-1)^n \sigma_n,$$

(¹) Cf. P. DUBREIL, *Recherches sur la valeur des exposants...* (*J. Math. pures et appl.*, 9^e s., t. 9, 1930, p. 231); *Remarques sur le théorème de Noether* (*Bull. Soc. Math. de France*, t. 64, 1936, p. 99); B. L. VAN DER WAERDEN, *Einführung in die algebraische Geometrie* (*Grundl. Math. Wiss.*, t. 51, Springer, Berlin, 1933, chap. VIII).

Les sommes de puissances semblables des x_i ,

$$\begin{aligned} s_1 &= x_1 + x_2 + \dots + x_n = \sigma_1, \\ s_2 &= x_1^2 + x_2^2 + \dots + x_n^2 = \sigma_1^2 - 2\sigma_2, \\ &\dots\dots\dots, \\ s_h &= x_1^h + x_2^h + \dots + x_n^h, \end{aligned}$$

sont également des polynômes symétriques.

D'une façon générale, un polynôme symétrique contient, en même temps qu'un monome $ax_1^{\alpha_1} \dots x_n^{\alpha_n}$ ($\alpha_i \geq 0$), tous les monomes $ax_{i_1}^{\alpha_1} \dots x_{i_n}^{\alpha_n}$, où $\{i_1, \dots, i_n\}$ est une permutation quelconque des indices $1, \dots, n$: la somme de ces différents termes est, par définition, le polynôme symétrique *engendré* par le monome $ax_1^{\alpha_1} \dots x_n^{\alpha_n}$.

La somme, la différence, le produit de deux polynômes symétriques sont des polynômes symétriques : les polynômes symétriques de $\mathbf{R}_n$ forment donc un sous-anneau $\mathbf{S}_n$ de $\mathbf{R}_n$. D'après les expressions (1), tout produit $P = a\sigma_1^{\gamma_1} \dots \sigma_n^{\gamma_n}$ est égal à un *polynôme symétrique et homogène* en $x_1, \dots, x_n$, de degré

$$k = \gamma_1 + 2\gamma_2 + \dots + n\gamma_n.$$

Le nombre entier k est appelé *poids* du produit P . Un polynôme en $\sigma_1, \dots, \sigma_n$, $\varphi(\sigma_1, \dots, \sigma_n)$, est dit *isobare* si tous ses termes $a\sigma_1^{\gamma_1} \dots \sigma_n^{\gamma_n}$ ont le même poids k : on a alors

$$\varphi(\sigma_1, \dots, \sigma_n) = f(x_1, \dots, x_n)$$

où le polynôme $f(x_1, \dots, x_n)$, s'il n'est pas nul, est homogène et de degré k en $x_1, \dots, x_n$. Le poids k d'un polynôme $\varphi(\sigma_1, \dots, \sigma_n)$ quelconque est par définition le poids maximum de ses différents termes : le polynôme correspondant $f(x_1, \dots, x_n)$ a un *degré au plus égal à k* . Les polynômes symétriques $f(x_1, \dots, x_n) = \varphi(\sigma_1, \dots, \sigma_n)$ ainsi obtenus à partir de polynômes en $\sigma_1, \dots, \sigma_n$, forment évidemment un sous-anneau Σ_n de $\mathbf{S}_n$: $\Sigma_n \subseteq \mathbf{S}_n$.

Le résultat fondamental de la théorie des fonctions symétriques est précisément que *l'anneau Σ_n coïncide avec $\mathbf{S}_n$* .

$$\Sigma_n = \mathbf{S}_n.$$

En d'autres termes, tout polynôme de $\mathbf{R}_n$ symétrique en $x_1, x_2, \dots, x_n$ et de degré k , s'exprime au moyen des fonctions symétriques élémentaires sous forme d'un polynôme $\varphi(\sigma_1, \sigma_2, \dots, \sigma_n)$ de poids égal à k .

Ce théorème est évident pour $n = 1$, puisqu'on a alors une seule fonction symétrique élémentaire $\sigma_1 = x_1$: tout polynome $f(x_1) \in \mathbf{R}_1$ est symétrique et peut s'écrire sous la forme $f(\sigma_1)$. Supposons donc le théorème vrai pour tout polynome symétrique à $n - 1$ variables $x_1, \dots, x_{n-1}$ et démontrons-le pour les polynomes symétriques à n variables $x_1, \dots, x_{n-1}, x_n$.

Soit $f(x_1, \dots, x_n)$ un tel polynome, de degré k . Si k est égal à zéro, f est une constante et le théorème est évident. Supposons donc le théorème vrai pour les polynomes symétriques en $x_1, \dots, x_n$ de degré inférieur à k . Posons

$$f_0 = f(x_1, \dots, x_{n-1}, 0).$$

et, en particulier,

$$\begin{aligned} \sigma_{1,0} &= x_1 + \dots + x_{n-1}, \\ &\dots\dots\dots, \\ \sigma_{n-1,0} &= x_1 \dots x_{n-1} \quad (\sigma_{n,0} = 0); \end{aligned}$$

$\sigma_{1,0}, \dots, \sigma_{n-1,0}$ sont les fonctions symétriques élémentaires de $x_1, \dots, x_{n-1}$. Comme f_0 est évidemment symétrique en $x_1, \dots, x_{n-1}$, nous avons

$$(2) \quad f_0 = \varphi_0(\sigma_{1,0}, \dots, \sigma_{n-1,0}),$$

où φ_0 est un polynome de poids k par rapport aux $n - 1$ variables qui y figurent. La différence

$$d = f(x_1, \dots, x_n) - \varphi_0(\sigma_1, \dots, \sigma_{n-1})$$

est un polynome symétrique en $x_1, \dots, x_n$, dont le degré est au plus égal à k . D'après (2), ce polynome est nul pour $x_n = 0$: par suite, il contient x_n en facteur, donc aussi $x_1, \dots, x_{n-1}$ et par conséquent le produit $\sigma_n = x_1 \dots x_n$,

$$d = \sigma_n f_1(x_1, \dots, x_n).$$

Dans cette égalité, f_1 est évidemment un polynome symétrique, dont le degré k_1 est au plus égal à $k - n$. Si k est inférieur à n , ce polynome est identiquement nul et le théorème est démontré. Sinon, nous avons

$$f_1(x_1, \dots, x_n) = \varphi_1(\sigma_1, \dots, \sigma_{n-1}, \sigma_n),$$

où φ_1 est un polynome de poids k_1 , et nous pouvons écrire

$$f(x_1, \dots, x_n) = \varphi_0(\sigma_1, \dots, \sigma_{n-1}) + \sigma_n \varphi_1(\sigma_1, \dots, \sigma_{n-1}, \sigma_n).$$

Le second membre est bien un polynome en $\sigma_1, \dots, \sigma_n$, $\varphi(\sigma_1, \dots, \sigma_n)$, somme de deux termes dont les poids respectifs sont k et $k_1 + n \leq k$:

son poids est donc au plus égal à k . Mais si ce poids était inférieur à k , f serait de degré inférieur à k , ce qui est contraire à l'hypothèse. Nous avons donc bien

$$(3) \quad f(x_1, \dots, x_n) = \varphi(\sigma_1, \dots, \sigma_n).$$

où φ est un polynôme de poids k exactement.

Le théorème précédent admet un complément important : la représentation (3) est possible d'une seule manière. En d'autres termes, deux polynômes distincts $\varphi(s_1, \dots, s_n)$, $\psi(s_1, \dots, s_n)$, où $s_1, \dots, s_n$ désignent des indéterminées, ne peuvent pas fournir, par la spécialisation $s_i = \sigma_i$, le même polynôme $\varphi(\sigma_1, \dots, \sigma_n) = f(x_1, \dots, x_n)$. Il suffit évidemment de montrer qu'un polynôme $\varphi(s_1, \dots, s_n)$ non nul ne peut pas donner, par la spécialisation considérée, un polynôme $f(x_1, \dots, x_n) = 0$. Cette proposition est évidente pour $n = 1$, car on a $\sigma_1 = x_1$, et le polynôme $f(x_1)$ qui se déduit de $\varphi(s_1)$ par la spécialisation $s_1 = \sigma_1 = x_1$ a les mêmes coefficients que φ . Considérons donc le résultat comme établi pour un nombre de variables inférieur à n , et supposons qu'il existe un polynôme $\varphi(s_1, \dots, s_n)$ non nul et tel que le polynôme $f(x_1, \dots, x_n)$ correspondant soit nul. Nous pouvons supposer en outre que, parmi les polynômes ayant cette propriété, φ a été choisi de degré minimum, h , par rapport à s_n . Posons

$$\varphi(s_1, \dots, s_n) = \lambda_0(s_1, \dots, s_{n-1}) + \lambda_1(s_1, \dots, s_{n-1})s_n + \dots + \lambda_h(s_1, \dots, s_{n-1})s_n^h \neq 0.$$

Nous avons par hypothèse

$$\begin{aligned} \varphi(\sigma_1, \dots, \sigma_n) &= \lambda_0(\sigma_1, \dots, \sigma_{n-1}) + \lambda_1(\sigma_1, \dots, \sigma_{n-1})\sigma_n \\ &\quad + \dots + \lambda_h(\sigma_1, \dots, \sigma_{n-1})\sigma_n^h = f(x_1, \dots, x_n) = 0. \end{aligned}$$

Si nous remplaçons x_n par zéro dans cette relation, nous obtenons

$$\lambda_0(\sigma_{1,0}, \dots, \sigma_{n-1,0}) = 0;$$

$\sigma_{1,0}, \dots, \sigma_{n-1,0}$ étant les fonctions symétriques élémentaires de $x_1, \dots, x_{n-1}$, et le théorème étant supposé vrai pour $n-1$ variables, il en résulte

$$\lambda_0(s_1, \dots, s_{n-1}) = 0,$$

ce qui démontre le théorème si $h = 0$. Dans le cas général, on a

$$\varphi(s_1, \dots, s_n) = s_n \psi(s_1, \dots, s_n),$$

où le polynôme $\psi(s_1, \dots, s_n)$ n'est pas nul, et

$$\varphi(\sigma_1, \dots, \sigma_n) = x_1 \dots x_n \psi(\sigma_1, \dots, \sigma_n) = 0,$$

d'où

$$\psi(\sigma_1, \dots, \sigma_n) = 0.$$

Comme ψ est de degré $h - 1$ par rapport à s_n , il en résulte

$$\psi(s_1, \dots, s_n) = 0,$$

ce qui est absurde

Une autre méthode pour établir le théorème fondamental et pour calculer effectivement le polynome $\varphi(\sigma_1, \dots, \sigma_n)$ auquel un polynome symétrique donné $f(x_1, \dots, x_n)$ est égal, est la *méthode de Waring*, dont le principe consiste à ordonner alphabétiquement les monômes en $x_1, x_2, \dots, x_n$. Un monome $M = ax_1^{\alpha_1} \dots x_n^{\alpha_n}$ est dit *plus haut* qu'un monome $N = bx_1^{\beta_1} \dots x_n^{\beta_n}$ si la première des différences $\alpha_i - \beta_i$ qui n'est pas nulle, est positive. Cette propriété est visiblement transitive. Dans tout polynome (réduit), il y a un monome et un seul plus haut que tous les autres. Si le polynome considéré $f(x_1, \dots, x_n)$ est *symétrique* et si $M = ax_1^{\alpha_1} \dots x_n^{\alpha_n}$ est son monome le plus haut, on a nécessairement

$$\alpha_1 \geq \alpha_2 \geq \dots \geq \alpha_n,$$

car de l'inégalité $\alpha_i < \alpha_j$ ($i < j$) résulterait que le monome de f qui se déduit de M par l'échange de x_i et de x_j serait plus haut que M . De même, si $N = bx_1^{\beta_1} \dots x_n^{\beta_n}$ est un monome quelconque du polynome *symétrique* f , aucun des exposant β_i ne peut dépasser α_i .

Si un monome M est plus haut qu'un monome M' et un monome M_1 plus haut qu'un monome M'_1 , le produit MM_1 est plus haut que $M'M'_1$ ⁽¹⁾; de même, P étant un monome quelconque, MP est plus haut que $M'P$. Il en résulte que, *dans le produit de deux polynomes f et g , le monome le plus haut est le produit des monomes les plus hauts de f et g .*

Or, dans les fonctions symétriques élémentaires $\sigma_1, \sigma_2, \dots, \sigma_n$ les monomes les plus hauts sont respectivement $x_1, x_1x_2, \dots, x_1x_2 \dots x_n$. Étant donné un monome

$$M = ax_1^{\alpha_1} \dots x_n^{\alpha_n} \quad (\alpha_1 \geq \alpha_2 \geq \dots \geq \alpha_n, a \in \mathbf{A}),$$

le polynome symétrique

$$a\sigma_n^{\alpha_n}\sigma_{n-1}^{\alpha_{n-1}-\alpha_n}\dots\sigma_2^{\alpha_2-\alpha_3}\sigma_1^{\alpha_1-\alpha_2}$$

a, comme monome le plus haut

$$a(x_1 \dots x_n)^{\alpha_n}(x_1 \dots x_{n-1})^{\alpha_{n-1}-\alpha_n} \dots (x_1x_2)^{\alpha_2-\alpha_3}x_1^{\alpha_1-\alpha_2},$$

c'est-à-dire précisément M .

(1) Nous supposons ici que les coefficients a, a' des monomes considérés ne sont pas diviseurs de zéro. Il en est certainement ainsi quand $\mathbf{A}$ est un domaine d'intégrité.

Cela posé, étant donné un polynôme symétrique $f(x_1, \dots, x_n)$, la méthode de Waring consiste à déterminer son monome le plus haut, $M = ax_1^{\alpha_1} \dots x_n^{\alpha_n}$, puis à retrancher de f le polynôme $a\sigma_n^{\alpha_n} \dots \sigma_1^{\alpha_1 - \alpha_n}$. La différence

$$f_1 = f - a\sigma_n^{\alpha_n} \dots \sigma_1^{\alpha_1 - \alpha_n},$$

est un polynôme symétrique, dont le monome le plus haut, $N = bx_1^{\beta_1} \dots x_n^{\beta_n}$, est nécessairement moins haut que M : chacun des exposants β_i est donc au plus égal à α_i . Si la différence f_1 n'est pas identiquement nulle, on répète le raisonnement, et il est clair qu'au bout d'un nombre fini d'opérations, on obtient l'expression de f sous forme d'un polynôme $\varphi(\sigma_1, \dots, \sigma_n)$ en $\sigma_1, \sigma_2, \dots, \sigma_n$. Il importe de remarquer que les coefficients de ce polynôme appartiennent à l'anneau $\mathbf{A}$ comme ceux du polynôme f : en particulier, *tout polynôme symétrique $f(x_1, \dots, x_n)$ à coefficients entiers est égal à un polynôme $\varphi(\sigma_1, \dots, \sigma_n)$ lui aussi à coefficients entiers.*

Exemples. — Soit d'abord $f = \Sigma x_i^2 x_j$ ($n \geq 3$). Le monome le plus haut est

$$M = x_1^2 x_2 \quad (\alpha_1 = 2, \alpha_2 = 1).$$

On a

$$f - \sigma_1 \sigma_2 = \Sigma x_i^2 x_j - (\Sigma x_i) (\Sigma x_i x_j) = -3 \Sigma x_i x_j x_k = -3 \sigma_3,$$

d'où

$$f = \sigma_1 \sigma_2 - 3 \sigma_3.$$

Soit maintenant $g = \Sigma x_i^3$ ($n \geq 3$). Nous avons $M = x_1^3$ ($\alpha_1 = 3, \alpha_2 = \dots = 0$). Or

$$\Sigma x_i^3 - \sigma_1^3 = -3 \Sigma x_i^2 x_j - 6 \Sigma x_i x_j x_k = -3(\sigma_1 \sigma_2 - 3 \sigma_3) - 6 \sigma_3,$$

d'où

$$\Sigma x_i^3 = \sigma_1^3 - 3 \sigma_1 \sigma_2 + 3 \sigma_3.$$

5. Méthodes de Newton et de Cauchy. Applications. — La méthode de Newton permet de calculer directement, par des formules simples, les sommes $s_h = \Sigma x_i^h$ de puissances semblables des x_i . Nous avons, d'après l'équation (1') de la section précédente,

$$F'(u) = nu^{n-1} - (n-1)\sigma_1 u^{n-2} + \dots + (-1)^h (n-h)\sigma_h u^{n-h-1} + \dots$$

et, d'autre part,

$$F'(u) = \sum \frac{F(u)}{u - x_i}.$$

Or

$$\frac{F(u)}{u - x_i} = u^{n-1} + (x_i - \sigma_1)u^{n-2} + \dots + [x_i^h - \sigma_1 x_i^{h-1} + \dots + (-1)^h \sigma_h] u^{n-h-1} + \dots,$$

d'où

$$F'(u) = nu^{n-1} + (s_1 - n\sigma_1)u^{n-2} + \dots + [s_h - \sigma_1 s_{h-1} + \dots + (-1)^h n\sigma_h]u^{n-h-1} + \dots$$

En égalant les deux expressions de $F'(u)$, nous obtenons les *formules de Newton*

$$s_h - \sigma_1 s_{h-1} + \dots + (-1)^h h\sigma_h = 0 \quad (h = 1, 2, \dots, n-1).$$

La somme s_n est donnée à son tour par la relation

$$s_n - \sigma_1 s_{n-1} + \dots + (-1)^n n\sigma_n = 0,$$

conséquence immédiate des relations $F(x_i) = 0$. Pour $h > n$, nous avons, en ajoutant terme à terme les relations $x_i^{h-n} F(x_i) = 0$,

$$s_h - \sigma_1 s_{h-1} + \dots + (-1)^n n\sigma_n s_{h-n} = 0.$$

Ces formules donnent en particulier

$$\begin{aligned} s_1 &= \sigma_1, \\ s_2 &= \sigma_1 s_1 - 2\sigma_2 = \sigma_1^2 - 2\sigma_2 \quad (n \geq 2), \quad s_2 = \sigma_1^2 \quad (n = 1), \\ s_3 &= \sigma_1 s_2 - \sigma_2 s_1 + 3\sigma_3 = \sigma_1^3 - 3\sigma_1 \sigma_2 + 3\sigma_3 \quad (n \geq 3), \\ s_3 &= \sigma_1^3 - 3\sigma_1 \sigma_2 \quad (n = 2), \quad s_3 = \sigma_1^3 \quad (n = 1). \end{aligned}$$

D'une manière générale, pour h positif ou nul, les sommes s_h sont des polynômes à coefficients entiers en $\sigma_1, \sigma_2, \dots, \sigma_n$. Conformément au théorème général, s_h est un polynôme isobare et de poids h en $\sigma_1, \sigma_2, \dots, \sigma_h$ ($h \leq n$) ou $\sigma_1, \sigma_2, \dots, \sigma_n$ ($h > n$).

A partir des expressions des sommes de puissances semblables, on peut obtenir directement, par le procédé suivant, l'expression d'un polynôme symétrique quelconque. Nous pouvons évidemment nous borner au cas d'un polynôme symétrique engendré par un seul monome, c'est-à-dire de la forme

$$f(x_1, \dots, x_n) = \Sigma x_i^\alpha x_j^\beta \dots x_l^\lambda \quad (\alpha > 0, \dots, \lambda > 0).$$

L'ordre d'un tel polynôme est, par définition, le nombre des lettres distinctes $x_i, x_j, \dots, x_l$ figurant effectivement dans le monome générateur. Les sommes de puissances semblables s_h sont les polynômes symétriques d'ordre égal à 1.

Si nous considérons un polynôme d'ordre 2, $f = \Sigma x_i^\alpha x_j^\beta$, nous avons, en supposant d'abord $\alpha \neq \beta$

$$s_\alpha s_\beta = \Sigma x_i^\alpha x_j^\beta + \Sigma x_i^{\alpha+\beta},$$

d'où

$$\Sigma x_i^\alpha x_j^\beta = s_\alpha s_\beta - s_{\alpha+\beta}$$

et, par conséquent, $\Sigma x_i^\alpha x_j^\beta$ est un polynôme à coefficients entiers en $\sigma_1, \sigma_2, \dots, \sigma_n$, polynôme isobare et de poids $\alpha + \beta$.

Si maintenant β est égal à α , nous avons,

$$s_\alpha^2 = 2 \Sigma x_i^\alpha x_j^\alpha + \Sigma x_i^{2\alpha},$$

d'où

$$\Sigma x_i^\alpha x_j^\alpha = \frac{1}{2} (s_\alpha^2 - s_{2\alpha}).$$

Il n'est plus évident sur cette expression que le premier membre est un polynôme à coefficients entiers en $\sigma_1, \dots, \sigma_n$; cette propriété est cependant encore vérifiée, d'après les résultats obtenus par la méthode de Waring.

On calculera de même un polynôme symétrique du troisième ordre $\Sigma x_j^\alpha x_i^\beta x_k^\gamma$ à partir du produit $s_\alpha s_\beta s_\gamma$. Il y aura lieu de distinguer le cas où deux des exposants sont égaux et celui où les trois exposants le sont.

Signalons encore une méthode intéressante, due à Cauchy, pour le calcul des fonctions symétriques. Nous supposons ici que l'anneau $\mathbf{A}$ des coefficients est un *domaine d'intégrité*. Comme nous l'avons vu, $x_1, x_2, \dots, x_n$ sont les racines de l'équation

$$F(u) = (u - x_1) \dots (u - x_n) = u^n - \sigma_1 u^{n-1} + \sigma_2 u^{n-2} - \dots + (-1)^n \sigma_n = 0,$$

où $F(u) \in \mathbf{A}[\sigma_1, \dots, \sigma_n][u]$ ⁽¹⁾. De même, $x_2, \dots, x_n$ sont les racines de l'équation

$$F_1(u) = \frac{F(u)}{u - x_1} = u^{n-1} + (x_1 - \sigma_1) u^{n-2} + (x_1^2 - \sigma_1 x_1 + \sigma_2) u^{n-3} + \dots = 0,$$

dont le premier membre appartient à l'anneau $\mathbf{A}[\sigma_1, \dots, \sigma_{n-1}, x_1][u]$, puisque σ_n n'intervient pas dans le calcul du quotient. Posons, de proche en proche,

$$F_k(u) = \frac{F_{k-1}(u)}{u - x_k}.$$

Ce polynôme, qui est de degré $n - k$, appartient à l'anneau $\mathbf{A}[\sigma_1, \dots, \sigma_{n-k}, x_1, \dots, x_k][u]$ et admet pour zéros $x_{k+1}, \dots, x_n$. On a enfin

$$F_{n-1}(u) = \frac{F_{n-2}(u)}{u - x_{n-1}}$$

⁽¹⁾ $\sigma_1, \sigma_2, \dots, \sigma_n$ étant les polynômes en $x_1, \dots, x_n$ définis par les relations (1) du paragraphe 3, les anneaux $\mathbf{A}[\sigma_1, \dots, \sigma_n], \dots, \mathbf{A}[\sigma_1, \dots, \sigma_{n-k}, x_1, \dots, x_k], \dots$ sont des sous-anneaux du domaine d'intégrité $\mathbf{R}_n = \mathbf{A}[x_1, \dots, x_n]$.

et le zéro x_n de ce polynome appartient au même anneau que ses coefficients

$$(1) \quad x_n \in \mathbf{A}[\sigma_1, x_1, \dots, x_{n-1}].$$

On a d'ailleurs évidemment

$$(1') \quad x_n = \sigma_1 - x_1 - \dots - x_{n-1}.$$

Cela posé, un polynome symétrique $f(x_1, x_2, \dots, x_n)$ peut, en tenant compte de la relation (1) ou (1'), se mettre sous la forme

$$f = f_1(\sigma_1, x_1, x_2, \dots, x_{n-1}).$$

Or, x_{n-1} étant un zéro du polynome du second degré $F_{n-2}(u)$, f_1 , considéré comme polynome en x_{n-1} , peut être remplacé par son reste r_1 modulo F_{n-2} , reste qui est du premier degré en x_{n-1} . Nous avons donc

$$(2) \quad f(x_1, \dots, x_n) = r_1 = f_2 + \lambda_1 x_{n-1} \quad \text{avec} \quad f_2, \lambda_1 \in \mathbf{A}[\sigma_1, \sigma_2, x_1, \dots, x_{n-2}].$$

Si maintenant nous intervertissons dans ce qui précède x_{n-1} et x_n , nous obtenons la relation analogue

$$(2') \quad f = f_2 + \lambda_1 x_n,$$

où f_2 et λ_1 sont évidemment *les mêmes que dans (2)*. La comparaison de (2) et (2') entraîne

$$\lambda_1 = 0,$$

d'où

$$f = f_2(\sigma_1, \sigma_2, x_1, \dots, x_{n-2}).$$

Le raisonnement se poursuit de proche en proche : on peut remplacer f_2 , considéré comme polynome en x_{n-2} , par son reste modulo F_{n-3} , reste qui est du second degré en x_{n-2} ; on obtient ainsi une égalité de la forme

$$f = \lambda_2 x_{n-2}^2 + \mu_2 x_{n-2} + f_3, \quad \text{avec} \quad \lambda_2, \mu_2, f_3 \in \mathbf{A}[\sigma_1, \sigma_2, \sigma_3, x_1, \dots, x_{n-3}],$$

qui subsiste lorsqu'on y remplace x_{n-2} par x_{n-1} ou x_n . Le polynome $H(u) = \lambda_2 u^2 + \mu_2 u + f_3 - f \in \mathbf{R}_n[u]$, sur le domaine d'intégrité $\mathbf{R}_n = \mathbf{A}[x_1, \dots, x_n]$, s'annule pour $u = x_{n-2}$, x_{n-1} et x_n , nous avons donc

$$\lambda_2 = \mu_2 = 0, \quad f = f_3,$$

ce qui fournit une expression de f ne contenant plus que $\sigma_1, \dots, \sigma_3, x_1, \dots, x_{n-3}$. Finalement, on arrive, par une simple succession de divisions, à une expression de f ne contenant plus que les fonctions

symétriques élémentaires, et qui est par conséquent l'expression cherchée

$$f(x_1, \dots, x_n) = \varphi(\sigma_1, \dots, \sigma_n).$$

Exemple. — Pour trois variables x_1, x_2, x_3 , calculons $f = \Sigma x_i^3$. On a

$$\begin{aligned} f(x_1, x_2, x_3) &= f_1(\sigma_1, x_1, x_2) = x_1^3 + x_2^3 + (\sigma_1 - x_1 - x_2)^3 \\ &= 2x_1^2 - 2(\sigma_1 - x_1)x_2 + \sigma_1^3 - 2\sigma_1 x_1 + 2x_1^2. \end{aligned}$$

Or, x_2 est racine de

$$F_1(x) = \frac{x^3 - \sigma_1 x^2 + \sigma_2 x - \sigma_3}{x - x_1} = x^2 + (x_1 - \sigma_1)x + x_1^2 - \sigma_1 x_1 + \sigma_2 = 0,$$

d'où

$$\begin{aligned} f &= 2(\sigma_1 - x_1)x_2 - 2(\sigma_1 - x_1)x_2 - 2(x_1^2 - \sigma_1 x_1 + \sigma_2) + \sigma_1^3 - 2\sigma_1 x_1 + 2x_1^2 \\ &= \sigma_1^3 - 2\sigma_2. \end{aligned}$$

Une *fraction rationnelle* $R(x_1, x_2, \dots, x_n)$ appartenant au corps des quotients $\mathbf{K}_n$ de l'anneau $\mathbf{R}_n$, est *symétrique* si elle est invariante par toute substitution effectuée sur les x_i . Par exemple, les fractions

$$\frac{x_1^2 + x_2^2}{x_1 x_2}, \quad \frac{x_1^3 - x_2^3}{x_1^2 - x_2^2}$$

sont symétriques. On peut toujours écrire une fraction rationnelle symétrique sous forme du quotient de deux polynômes symétriques. Si, en effet, le dénominateur D n'est pas symétrique, on multipliera les deux termes de la fraction par les polynômes distincts qui se déduisent de D en permutant les x_i de toutes les manières possibles. On obtient ainsi au dénominateur un polynôme symétrique et le numérateur correspondant est évidemment symétrique lui aussi. On a, par exemple,

$$\frac{x_1^3 - x_2^3}{x_1^2 - x_2^2} = \frac{(x_1^3 - x_2^3)(x_2^2 - x_1^2)}{(x_1^2 - x_2^2)(x_2^2 - x_1^2)} = \frac{x_1^2 x_2^2 (x_1 + x_2) - (x_1^5 + x_2^5)}{2x_1^2 x_2^2 - (x_1^4 + x_2^4)}.$$

Supposons de plus, ici, que l'anneau $\mathbf{A}$ des coefficients soit un anneau à factorisation unique, ce qui entraîne la même propriété pour $\mathbf{R}_n$, et montrons que toute fraction symétrique irréductible $R(x_1, \dots, x_n)$ a un numérateur et un dénominateur symétriques. A cet effet, remarquons d'abord que, si un polynôme symétrique $f(x_1, \dots, x_n)$ admet un diviseur non symétrique $m(x_1, \dots, x_n) \in \mathbf{R}_n$, f est multiple de chacun des polynômes qui se déduisent de m par une substitution effectuée sur les x_i , donc du p. p. c. m. ⁽¹⁾ $\mu(x_1, \dots, x_n)$ de ces poly-

⁽¹⁾ Au sens de la Théorie des anneaux à factorisation unique.

nomes, lequel est évidemment symétrique. Si, en particulier, m est le p. g. c. d. δ de f et d'un autre polynome symétrique g , on a nécessairement $\mu = \delta$ et, par suite, δ est symétrique. Soit alors R une fraction rationnelle symétrique, quotient de deux polynomes symétriques f et g , on la met sous forme irréductible en divisant f et g par leur p. g. c. d. ; celui-ci étant symétrique, le numérateur et le dénominateur ainsi obtenus le sont également. Par exemple, la fraction irréductible $\frac{x_1^2 + x_1x_2 + x_2^2}{x_1 + x_2}$, égale à la fraction symétrique $\frac{x_1^2 - x_2^2}{x_1^2 - x_2^2}$, a bien un numérateur et un dénominateur symétriques.

Dans tout ce qui précède, les n symboles $x_1, x_2, \dots, x_n$ ont été regardés comme des indéterminées. Mais les résultats obtenus subsistent si l'on *spécialise* ces indéterminées dans un anneau $\mathbf{A}'$, extension de $\mathbf{A}$. On pourra, en particulier, remplacer les indéterminées x_i par les racines ξ_i d'une équation de la forme

$$F(u) = u^n - p_1 u^{n-1} + \dots + (-1)^n p_n = 0 \quad (p_i \in \mathbf{A})$$

ou plus généralement

$$(3) \quad F(u) = a_0 u^n + a_1 u^{n-1} + \dots + a_n = 0 \quad (a_i \in \mathbf{A}).$$

Toute expression rationnelle, entière et symétrique par rapport aux ξ_i est alors égale à une expression rationnelle entière des p_i ; toute expression rationnelle et symétrique par rapport aux ξ_i est égale à une expression rationnelle des a_i .

On peut, en outre, remplacer la symétrie formelle, considérée jusqu'à maintenant, par la simple *invariance numérique*; une expression rationnelle (entière ou non) $f(\xi_1, \dots, \xi_n)$, où les ξ_i sont les racines de l'équation (3) dans une extension de $\mathbf{A}$ où $F(u)$ se décompose en facteurs linéaires, est dite *numériquement invariante* si elle conserve la même valeur lorsqu'on effectue sur les ξ_i une substitution quelconque. Si la fonction rationnelle $f(x_1, \dots, x_n)$ est symétrique, l'expression rationnelle $f(\xi_1, \dots, \xi_n)$ qui s'en déduit par spécialisation, est numériquement invariante. Inversement, une expression rationnelle $f(\xi_1, \dots, \xi_n)$ peut être numériquement invariante sans que le polynôme $f(x_1, \dots, x_n)$ soit symétrique. Mais on peut trouver un polynome symétrique f^* , dont l'expression considérée est aussi la valeur pour la spécialisation $x_i = \xi_i$: il suffit de prendre

$$f^*(x_1, \dots, x_n) = \frac{1}{n!} \sum f(x_{i_1}, \dots, x_{i_n}),$$

où la somme Σ est étendue à toutes les permutations des indices. Nous voyons donc qu'une *expression rationnelle des racines* $\xi_1, \dots, \xi_n$ de l'équation (3), *numériquement invariante par toute substitution opérée sur les ξ_i , s'exprime rationnellement au moyen des coefficients a_k de cette équation.*

Exemple. — Les calculs faits à propos de la méthode de Cauchy permettent d'écrire immédiatement des expressions numériquement invariantes $f(\xi_1, \dots, \xi_n)$ telles que le polynôme $f(x_1, \dots, x_n)$ ne soit pas symétrique. Soit, par exemple, l'équation

$$x^3 + px + q = 0.$$

Dans le calcul fait plus haut, la spécialisation $\sigma_1 = 0$, $x_i = \xi_i$ donne

$$\Sigma \xi_i^2 = 2(\xi_1^2 + \xi_1 \xi_2 + \xi_2^2) = 2[(\xi_1 + \xi_2)^2 - \xi_1 \xi_2] = 2(\xi_3^2 - \xi_1 \xi_2).$$

Les expressions $\xi_1^2 + \xi_1 \xi_2 + \xi_2^2$ et $\xi_3^2 - \xi_1 \xi_2$ sont numériquement invariantes, bien que les polynômes $x_1^2 + x_1 x_2 + x_2^2$, $x_3^2 - x_1 x_2$ ne soient pas symétriques par rapport à x_1, x_2, x_3 .

Comme application de la théorie des fonctions symétriques, nous donnerons quelques propriétés fondamentales des *nombre algébriques*. Soit Γ le corps des nombres rationnels ; à tout nombre algébrique α , zéro d'un polynôme $f(x) \in \Gamma[x]$, irréductible sur Γ , associons ses conjugués $\alpha_1 = \alpha, \alpha_2, \dots, \alpha_m$ qui sont les différents zéros de $f(x)$ dans le corps Ω des nombres complexes ⁽¹⁾ : les fonctions symétriques élémentaires des α_i sont des nombres rationnels.

La somme $\alpha + \beta$, la différence $\alpha - \beta$, le produit $\alpha\beta$ de deux nombres algébriques sont des nombres algébriques. En effet, les polynômes $\Pi(x - \alpha_i - \beta_j)$, $\Pi(x - \alpha_i + \beta_j)$, $\Pi(x - \alpha_i \beta_j)$ dans lesquels α_i, β_j désignent respectivement tous les conjugués de α et de β , sont symétriques à la fois par rapport aux α_i et par rapport aux β_j , donc ont leurs coefficients rationnels : comme ils admettent respectivement les nombres $\alpha_1 + \beta_1 = \alpha + \beta$, $\alpha_1 - \beta_1 = \alpha - \beta$ et $\alpha_1 \beta_1 = \alpha\beta$ comme zéros, ces nombres sont bien algébriques. Comme, d'autre part, si β est différent de zéro, $\frac{1}{\beta}$ est évidemment algébrique en même que β , nous voyons que *l'ensemble des nombres algébriques est un corps $\mathfrak{A}$.*

⁽¹⁾ Nous utilisons dans ce qui suit, avec la théorie des fonctions symétriques, les propriétés du corps des nombres complexes, en particulier le théorème fondamental de l'Algèbre. Nous reviendrons ultérieurement (t. 2) sur les propriétés des nombres algébriques (par rapport à un corps quelconque), et nous les établirons alors à partir de résultats purement algébriques.

Une propriété importante de ce corps est la suivante : *tout zéro d'un polynome*

$$f(x) = x^m + \alpha x^{m-1} + \dots + \theta$$

dont les coefficients sont algébriques, est lui-même algébrique : par conséquent, le corps $\mathfrak{A}$ des nombres algébriques est algébriquement fermé.

En effet, le polynome

$$\varphi(x) = \Pi(x^m + \alpha_i x^{m-1} + \dots + \theta_i),$$

où $\alpha_i, \dots, \theta_i$ sont respectivement tous les conjugués de $\alpha, \dots, \theta$, est symétrique à la fois par rapport aux $\alpha_i, \dots$, et par rapport aux θ_i . Ses coefficients sont donc rationnels. Un zéro ω de $f(x)$ étant aussi zéro de $\varphi(x)$ est, par conséquent, un nombre algébrique.

Les propriétés arithmétiques des corps algébriques, c'est-à-dire des sous-corps de $\mathfrak{A}$, reposent sur une notion fondamentale, celle d'*entiers algébriques*. Ces éléments jouant un rôle analogue à celui des nombres entiers en arithmétique élémentaire, il y a lieu de les définir de manière à satisfaire aux conditions suivantes ⁽¹⁾.

1° Les entiers algébriques forment un anneau.

2° Un nombre ω qui est à la fois entier algébrique et nombre rationnel est un entier rationnel : $\omega \in \mathbb{C}$.

3° Si α est un entier algébrique, ses conjugués le sont également.

Ces conditions entraînent, si $f(x)$ désigne le polynome irréductible sur Γ ayant un entier algébrique α comme zéro et dans lequel le coefficient de la plus haute puissance de x a été ramené à l'unité, que les coefficients de f , polynomes symétriques en α et ses conjugués, sont d'une part des nombres rationnels, d'autre part des entiers algébriques, donc des entiers rationnels. Nous sommes ainsi conduits à la *définition* suivante.

Un nombre algébrique α , zéro du polynome

$$f(x) = x^n + a_1 x^{n-1} + \dots + a_n \quad (a_i \in \Gamma)$$

irréductible sur Γ , est un entier algébrique si tous les coefficients a_i du polynome f sont des entiers rationnels

$$a_i \in \mathbb{C}.$$

(1) Les remarques qui suivent sur la définition des entiers algébriques ont été formulées par E. HECKE (*Theorie der algebraischen Zahlen*, p. 76, Leipzig, 1923).

LEMME. — *Pour qu'un nombre algébrique α soit un entier algébrique, il suffit qu'il vérifie une équation de la forme*

$$F(x) = x^N + c_1 x^{N-1} + \dots + c_N = 0,$$

dont les coefficients c_i sont des entiers rationnels : $c_i \in \mathbb{C}$. [L'intérêt de ce lemme est que le polynôme $F(x)$ n'est pas nécessairement irréductible sur Γ .]

Soit, en effet,

$$f(x) = a_0 x^n + a_1 x^{n-1} + \dots + a_n, \quad a_i \in \mathbb{C} \quad (a_0 > 0)$$

le polynôme irréductible sur Γ et primitif par rapport à l'anneau $\mathbb{C}$ des entiers rationnels, dont le nombre algébrique α est un zéro. $F(x)$ ayant dans Ω un zéro commun, α , avec $f(x)$, est multiple de ce polynôme dans $\Gamma[x]$ (p. 360). Nous pouvons écrire le quotient sous la forme $\frac{r g(x)}{s}$, où r et s sont deux entiers rationnels et $g(x)$ un polynôme primitif de $\mathbb{C}[x]$. Dans l'égalité

$$sF(x) = rf(x)g(x)$$

le produit $f(x)g(x)$ des deux polynômes primitifs f et g est lui-même primitif (chap. VI, § 5, p. 344). Comme F l'est également, nous avons ⁽¹⁾ $r = s$ et

$$F(x) = f(x)g(x).$$

Le premier coefficient a_0 de $f(x)$ divise donc le premier coefficient de $F(x)$, qui est 1 : nous avons, par suite, $a_0 = 1$ et α est bien un entier algébrique.

THÉOREME. — *Les entiers algébriques forment un anneau* ⁽²⁾.

Soient α, β deux entiers algébriques et $\alpha_1 = \alpha, \alpha_2, \dots, \alpha_m; \beta_1 = \beta, \beta_2, \dots, \beta_n$ leurs conjugués (dans Ω , par rapport à Γ). Les polynômes $g_1(x) = \Pi(x - \alpha_i - \beta_j), \quad g_2(x) = \Pi(x - \alpha_i + \beta_j), \quad g_3(x) = \Pi(x - \alpha_i \beta_j),$ symétriques par rapport aux α_i et aux β_j , ont comme coefficients des expressions rationnelles entières par rapport aux fonctions symétriques élémentaires des α_i et à celles des β_j : ces coefficients sont donc entiers, et comme le premier coefficient de chacun des polynômes g_1, g_2, g_3 est égal à l'unité, $\alpha + \beta, \alpha - \beta$ et $\alpha\beta$ sont des entiers algébriques.

⁽¹⁾ En changeant au besoin le signe de g .

⁽²⁾ La première condition de la page 397 est donc bien vérifiée ; la deuxième aussi, puisqu'un nombre rationnel vérifie une équation du premier degré sur Γ . La troisième résulte immédiatement de la définition d'un entier algébrique.

Remarquons encore qu'un zéro ω d'un polynome de la forme

$$h(x) = x^m + \alpha x^{m-1} + \dots + \theta;$$

où $\alpha, \dots, \theta$ sont des entiers algébriques, est lui-même un entier algébrique. Le polynome

$$H(x) = \Pi(x^m + \alpha_l x^{m-1} + \dots + \theta_l),$$

où les $\alpha_i, \dots, \theta_i$ sont les différents conjugués de $\alpha, \dots, \theta$, admet en effet ω comme zéro; or il a pour coefficients des entiers rationnels, et son premier coefficient est égal à l'unité.

Exercices. — 1. Montrer au moyen des formules de Newton que

$$s_h = \sum_i x_i^h \quad (h > 0)$$

est un polynome isobare et de poids h en $\sigma_1, \sigma_2, \dots, \sigma_n$.

2. Soit h un entier négatif. Calculer, par la méthode de Newton, la fonction symétrique $s_h = \sum_i x_i^h$.

3. En prenant $n = 3$, puis $n = 4$, former, pour les différentes valeurs de k , le polynome $F_k(u)$ sur l'anneau $\mathbf{A}[\sigma_1, \dots, \sigma_{n-k}, x_1, \dots, x_k]$ qui admet pour zéros $x_{k+1}, \dots, x_n$.

1° Utiliser la méthode des divisions successives indiquée dans le texte;

2° Utiliser la méthode suivante : On désigne par $\sigma'_1, \sigma'_2, \dots$ les fonctions symétriques élémentaires de $x_1, \dots, x_k$, par $\sigma''_1, \sigma''_2, \dots$ les fonctions symétriques élémentaires de $x_{k+1}, \dots, x_n$, en convenant de poser $\sigma'_i = 0$ pour $i > k$, $\sigma''_i = 0$ pour $i > n - k$. Établir la relation

$$\sigma_h = \sigma'_h + \sigma'_{h-1} \sigma''_1 + \dots + \sigma'_{h-l} \sigma''_l + \dots + \sigma''_h \quad (h = 1, \dots, n).$$

En déduire les expressions de $\sigma''_1, \dots, \sigma''_{n-k}$ et le polynome $F_k(u)$.

4. Calculer par la méthode de Cauchy les fonctions symétriques Σx_i^3 et $\Sigma x_i^2 x_j$ des trois variables x_1, x_2, x_3 .

5. Calculer le discriminant de chacune des équations

$$a_0 x^2 + a_1 x + a_2 = 0, \quad a_0 x^3 + a_1 x^2 + a_2 x + a_3 = 0,$$

c'est-à-dire la fonction symétrique

$$D = a_0^{2n-2} \prod_{i < j} (\xi_i - \xi_j)^2,$$

où l'on désigne par n le degré de l'équation et par $\xi_1, \xi_2, \dots$ ses racines.



NOTE I.

ENSEMBLES FINIS.

1. Introduction. — Comme on l'a indiqué au chapitre I, la théorie des ensembles finis, qui va être développée ici, est la théorie *directe*, c'est-à-dire celle qui ne repose pas sur la notion de nombre naturel : c'est au contraire celle-ci qui, dans une certaine mesure, en dérivera (note II).

Nous nous proposons essentiellement, dans cet exposé, d'établir l'équivalence des trois définitions mentionnées au chapitre I.

1° *Définition ordinale* (A. Denjoy) : *Un ensemble est fini s'il peut être ordonné (totalement), et s'il est semblable à lui-même dans tous les ordres possibles.*

2° (Stäckel, Enriques) : *Un ensemble est fini s'il peut être doublement bien ordonné.*

3° *Définition cardinale* (Tarski) : *Un ensemble est fini s'il vérifie la condition minimale, à savoir si tout ensemble $\mathfrak{M}$ non vide de parties de E contient une partie A minimale (ou irréductible), c'est-à-dire ne contenant aucun autre sous-ensemble appartenant à $\mathfrak{M}$.*

Nous supposerons connues les notions fondamentales sur les ensembles ordonnés, exposées au chapitre I (§ 9 et 10). Nous devons d'abord les compléter par quelques indications sur les *procédés d'ordination*.

2. Procédés d'ordination. — 1° Il est souvent commode de désigner par la notation O_E un ordre [total, strict ⁽¹⁾] défini dans un ensemble E et d'écrire

$$x < y \quad (O_E)$$

(¹) Nous ne répéterons pas constamment ces adjectifs : dans tout ce qui suit, il s'agira d'ordre total strict, sauf avis contraire.

quand deux éléments x, y de E vérifient cette relation d'ordre. Toute partie A de E est elle-même ordonnée dans l'ordre envisagé, mais celui-ci, *lorsqu'on le considère seulement pour les éléments de A* , sera avantageusement désigné par la notation O_A : on dira que O_A est l'ordre O_E *restreint* à A , ou défini *par restriction* et, inversement, que O_E *prolonge* dans E l'ordre O_A .

2° Supposons E ordonné par un ordre O_E . La relation inverse, O_E^{-1} :

$$x < y \quad (O_E^{-1}) \quad \text{si et seulement si} \quad y < x \quad (O_E)$$

est encore, visiblement, un ordre total strict, appelé *ordre inverse* de O_E .

3° Supposons qu'un ensemble E soit la *somme* d'une famille $\mathcal{F}$ de *classes* $A, B, \dots, X, \dots$. Si chaque classe $X \in \mathcal{F}$ est ordonnée par un ordre O_X et si $\mathcal{F}$ est ordonné par un ordre Ω , on définit dans E un ordre O en posant :

$$x < y \quad (O) \quad \text{si} \quad \begin{cases} x < y \quad (O_X) & \text{quand } x \text{ et } y \text{ appartiennent à une même} \\ & \text{classe } X; \\ x \in X, y \in Y, X < Y \quad (\Omega) & \text{quand } x \text{ et } y \text{ appartiennent} \\ & \text{à deux classes distinctes } X, Y. \end{cases}$$

On vérifie immédiatement (en faisant les distinctions de cas nécessaires) que la relation ainsi définie est *transitive* et que l'une des relations $x < y, x = y, y < x$ a toujours lieu, à l'exclusion des deux autres : O est bien un ordre total strict.

Dans le cas où l'on a $E = A + B, A < B(\Omega)$, on dit qu'on ordonne E « en plaçant A avant B ».

THÉORÈME 1. — *Si E est ordonné par un ordre O et si a est un élément de E , il y a un ordre O_a de E dans lequel a est premier élément.*

Désignons par X l'ensemble des éléments x de E vérifiant $x < a(O)$, par Y l'ensemble des éléments y de E vérifiant $a \leq y(O)$, par O_X, O_Y l'ordre O restreint respectivement à X, Y . Puisque O est un ordre total, nous avons $E = X + Y$. En plaçant Y , ordonné par O_Y , avant X , ordonné par O_X , nous définissons un ordre O' de E , dans lequel a est bien premier élément de E .

4° Soit f une *application biunivoque* d'un ensemble E sur un ensemble E' . A partir d'un ordre O défini dans E , on peut introduire un ordre O' dans E' en posant

$$x' < y' \quad (O') \quad \text{si et seulement si} \quad x < y \quad (O),$$

x et y désignant les images inverses respectives de x' , y' dans O :

$$x = f^{-1}(x'), \quad y = f^{-1}(y').$$

On dit que O' est l'ordre déduit de O par *transfert* au moyen de l'application f . L'ensemble E ordonné par O et l'ensemble E' ordonné par O' sont semblables.

5° Une ensemble $\mathcal{C}$ de parties d'un ensemble E totalement ordonné par rapport à la relation d'inclusion, est appelé *chaîne de parties*. L'utilisation de ces chaînes conduit à un procédé d'ordination, le procédé d'Hessenberg-Kuratowski ⁽¹⁾, ramenant les relations d'ordre, portant sur les éléments, à des relations d'inclusion, portant sur les parties ⁽²⁾.

Une chaîne $\mathcal{C}$ de parties est *stricte* si elle ne contient pas deux fois la même partie :

$$\mathcal{C} \dots \subset \dots \subset A \subset B \subset \dots$$

Elle est *maximale* si elle est stricte et n'est partie propre d'aucune autre chaîne stricte. Cela signifie donc qu'il est impossible d'y faire figurer de nouvelles parties : elle contient nécessairement la partie vide $\emptyset$ et l'ensemble E lui-même, qui en sont respectivement premier et dernier élément.

THÉORÈME 2. — *Pour qu'un ensemble E puisse être totalement ordonné, il faut et il suffit qu'il existe dans $\mathfrak{X}(E)$ une chaîne maximale $\mathfrak{M}$.*

1° *La condition est nécessaire.* — Supposons E ordonné par une relation d'ordre stricte $x < y$. Considérons, par rapport à cet ordre, l'ensemble $\mathfrak{M} = \{F\}$ des *sections commençantes* F ($\emptyset$ compris). $\mathfrak{M}$ est une *chaîne*. Supposons, en effet,

$$F \& F' \in \mathfrak{M} \quad \text{et, par exemple,} \quad F \not\subseteq F'.$$

Il existe $a \in F$ tel que $a \notin F'$. Soit $b \in F'$. On ne peut pas avoir $a \leq b$, car il en résulterait $a \in F'$. Donc $b < a$, d'où $b \in F$ et $F' \subset F$.

⁽¹⁾ HESSENBERG, *Grundbegriffe der Mengenlehre* (Abh. Tries'schen Schule, I, t. 1, Göttingen, p. 674-685).

KURATOWSKI, *Sur la notion de l'ordre dans la Théorie des Ensembles* (Fundamenta Math., t. 2, 1921, p. 161-174).

⁽²⁾ Ce procédé sera utilisé seulement pour établir l'équivalence de la définition cardinale avec les deux autres (§ 6, th. 22) : son étude peut être différée jusque-là; elle n'est pas nécessaire pour le lecteur désirant seulement connaître la théorie ordinale des ensembles finis.

La chaîne $\mathcal{M}$ est *maximale*. Soit, en effet, K une partie de E qui n'est pas section commençante : il existe donc $r, s \in E$ tels que

$$r \in K, \quad s < r, \quad s \notin K.$$

Soit X la section commençante ensemble des x vérifiant $x < r$; on a $X \in \mathcal{M}$ et

$$\begin{array}{lll} r \in K, & r \notin X, & \text{donc } K \not\subseteq X; \\ s \in X, & s \notin K, & \text{donc } X \not\subseteq K. \end{array}$$

$\mathcal{M} + \{K\}$ n'est donc plus une chaîne, $\mathcal{M}$ est bien *maximale*.

2° La condition est suffisante. — Soit $\mathcal{M}$ une chaîne *maximale* de parties de E .

Posons

$$x < y \quad \text{s'il existe } X \in \mathcal{M} \quad \text{tel que } \begin{cases} x \in X, \\ y \notin X. \end{cases}$$

Cette relation est *transitive*. Soit, en effet,

$$y < z, \quad \text{c'est-à-dire il existe } Y \in \mathcal{M} \quad \text{tel que } \begin{cases} y \in Y, \\ z \notin Y. \end{cases}$$

Puisque $\mathcal{M}$ est une chaîne, l'une des parties X, Y est sous-ensemble de l'autre : or $Y \subseteq X$ est impossible. On a donc $X \subset Y$, d'où $x \in Y$ et, par conséquent,

$$x < z.$$

D'après la définition, $x < y$ est incompatible avec $x = y$; $x < y$ est aussi incompatible avec $y < x$, qui signifierait : il existe $Y \in \mathcal{M}$, avec $y \in Y$, $x \notin Y$, d'où $X \not\subseteq Y$, $Y \not\subseteq X$, ce qui est absurde puisque X et Y sont éléments de la chaîne $\mathcal{M}$.

Si x et y ne vérifient ni $x = y$, ni $y < x$, on a $x < y$. Tout $Y \in \mathcal{M}$ contenant y comme élément, contient aussi x , sans quoi nous aurions $y < x$. Considérons les parties $P \in \mathcal{M}$ contenant y (donc x) : E , par exemple, a cette propriété ($E \in \mathcal{M}$, puisque $\mathcal{M}$ est maximale). Soit $I = \bigcap P$ et $X = I - \{y\}$: $x \in I$, donc $x \in X$, alors que $y \notin X$; il suffit donc de montrer que $X \in \mathcal{M}$.

Utilisons le fait que la chaîne $\mathcal{M}$ est *maximale* : nous avons seulement à établir que, si $H \in \mathcal{M}$, on a $X \subseteq H$ ou $H \subseteq X$. Distinguons deux cas.

1^{er} cas. — $y \in H$, alors H est une partie P , donc

$$I \subseteq H, \quad \text{d'où} \quad X \subseteq H.$$

2° cas. — $y \notin H$, alors, aucune partie P n'est contenue dans H , donc $H \subset P$ pour tout P et, par suite,

$$H \subseteq I, \quad \text{puis } H \subseteq I - \{y\} = X.$$

C. Q. F. D.

Remarque. — Dans l'ordre construit ci-dessus (2° partie), tout $X \in \mathcal{M}$ est section commençante. Soit, en effet, $x' < x \in X$: il existe

$$X' \in \mathcal{M} \quad \text{tel que } \begin{cases} x' \in X', \\ x \notin X'. \end{cases}$$

On ne peut avoir $X \subseteq X'$, donc on a $X' \subset X$ et $x' \in X$.

Inversement, toute section commençante S appartient à $\mathcal{M}$. En effet, si une partie $H \in \mathcal{M}$ ne contient pas S , $S \not\subseteq H$, il existe au moins un élément s vérifiant $s \in S$, $s \notin H$ et, puisque H est une section commençante, on a, pour tout $h \in H$, $h < s$, donc $h \in S$, c'est-à-dire $H \subset S$.

On voit finalement qu'il y a une correspondance biunivoque entre les ordres et les chaînes maximales de parties; les parties constituant une telle chaîne sont les sections commençantes dans l'ordre correspondant.

THÉORÈME 3. — Si E est bien ordonné, la chaîne maximale $\mathcal{M}$ l'est aussi.

Soit $\mathcal{F}$ une partie non vide de $\mathcal{M}$. Si $\mathcal{F} = \{E\}$, E est élément minimum de $\mathcal{F}$.

Soit donc $\mathcal{F} \neq \{E\}$; posons $R = \bigcup_{X \in \mathcal{F}} (E - X)$. Nous avons $R \neq \emptyset$;

E étant bien ordonné, R a un élément minimum r , et il existe au moins une partie

$$A \in \mathcal{F} \quad \text{telle que } r \in E - A.$$

Soit maintenant X une partie quelconque élément de $\mathcal{F}$; si l'on avait $E - X \supset E - A$, il existerait $y \in E - X \subseteq R$ pour lequel $y \notin E - A$, c'est-à-dire $y \in A$. Mais, puisque $r \notin A$, cela entraînerait $y < r$, ce qui est absurde puisque $y \in R$. Nous avons donc $E - X \subseteq E - A$ c'est-à-dire $A \subseteq X$ pour tout $X \in \mathcal{F}$: A est élément minimum de $\mathcal{F}$.

Désignons par E^{-1} , $\mathcal{M}^{-1}$ les ensembles E , $\mathcal{M}$ dans lesquels on a remplacé respectivement les ordres $<$, $\subset$ par les ordres inverses.

THÉORÈME 3'. — Si E^{-1} est bien ordonné, $\mathcal{M}^{-1}$ l'est aussi; en d'autres termes, si toute partie non vide de E a un élément maximum, $\mathcal{M}$ possède la même propriété.

THÉOREME 4 (réciproque de 3). — Si la chaîne maximale $\mathfrak{M}$ est bien ordonnée, E l'est aussi.

Soit A une partie non vide de E .

Désignons par $\mathfrak{F}$ la famille des sections commençantes $S (\in \mathfrak{M})$ telles que $S \cap A \neq \emptyset$: $\mathfrak{F}$, qui n'est pas vide puisque $E \in \mathfrak{F}$, a une partie minimum C ; montrons que $C \cap A (\neq \emptyset)$ se compose d'un seul élément. Supposons, en effet, que nous ayons : $a \in C \cap A$, $a' \in C \cap A$, $a \neq a'$ et soit, par exemple, $a' < a$: alors il existerait $C' \in \mathfrak{M}$ tel que $a' \in C'$, $a \notin C'$; nous aurions $C' \cap A \neq \emptyset$, donc $C' \in \mathfrak{F}$ et $C \not\subseteq C'$, d'où $C' \subset C$, ce qui est absurde puisque C est élément minimum de $\mathfrak{F}$.

L'élément unique a de $C \cap A$ est minimum dans A , car, si $m \in A$ et $m \neq a$, on a $m \notin C$, donc $a < m$.

On a le théorème analogue suivant :

THÉOREME 4' (réciproque de 3'). — Si $\mathfrak{M}^{-1}$ est bien ordonné, E^{-1} l'est aussi (en d'autres termes, si toute partie non vide de $\mathfrak{M}$ a un élément maximum, E possède la même propriété).

3. **Théorie ordinale** ⁽¹⁾. — Nous dirons qu'un ensemble F est *ordinalement fini* s'il peut être ordonné (totalement) et s'il est semblable à lui-même dans tous les ordres possibles. L'ensemble vide $\emptyset$, des ensembles de la forme $\{a\}$ ou $\{a, b\}$ sont ordinalement finis.

Nous désignerons par F_0 l'ensemble F ordonné par un certain ordre O .

THÉOREME 5. — Un ensemble F' ayant même puissance qu'un ensemble fini F , est lui-même fini.

Soit φ une application biunivoque de F sur F' . F' peut être ordonné totalement, par exemple par l'ordre O' déduit d'un ordre O de F par transfert au moyen de φ . A deux ordres O'_1 , O'_2 quelconques de F' , φ^{-1} fait correspondre de même deux ordres O_1 , O_2 de F , et les ensembles F_{0i} , F'_{0i} sont semblables ($i = 1, 2$). Comme F_{01} et F_{02} sont semblables, F'_{01} et F'_{02} le sont aussi, et F' est bien un ensemble fini.

THÉOREME 6. — Dans tout ordre O , un ensemble ordinalement fini F a un premier et un dernier élément.

⁽¹⁾ Cf. A. DENJOY, *Les ensembles finis* (C. R. Acad. Sc., t. 224, 1947, p. 612); *L'énumération transfinie*, t. III, *Études complémentaires sur l'ordination*, chap. I (Gauthier-Villars, Paris, 1954).

D'après le théorème 1, il existe un ordre total dans lequel un élément donné, a , de F est premier élément. Puisque F est semblable à lui-même dans tous les ordres possibles, F possède dans chaque ordre un *premier élément*.

En passant d'un ordre à l'ordre inverse, on voit qu'il existe aussi, dans chaque ordre, un *dernier élément*.

Toute partie A (non vide) d'un ensemble ordinalement fini E peut être ordonnée par restriction. Inversement, tout ordre Ω de A s'obtient de cette façon. Ordonnons, en effet, d'une façon quelconque (par exemple par restriction) le complément $B = F - A$ de A dans F . Soit B_Ω l'ensemble ordonné ainsi obtenu. Plaçons A_Ω avant B_Ω : nous faisons de $F = A + B$ un ensemble ordonné F_Ω , et l'ordre O restreint à A est précisément Ω . D'après le théorème 6, F possède, dans l'ordre O , un premier élément a , qui appartient nécessairement à A , et en est le premier élément dans l'ordre Ω . Ainsi, A possède, dans tout ordre Ω , un premier élément, donc :

THÉORÈME 7. — Une partie A non vide d'un ensemble ordinalement fini F possède, dans tout ordre Ω , un premier élément.

THÉORÈME 7'. — Une partie A non vide d'un ensemble ordinalement fini F possède, dans tout ordre Ω , un dernier élément.

COROLLAIRE. — Tout ordre O de F est un double bon ordre, tout ensemble ordinalement fini est doublement bien ordonné.

Il en résulte que, dans tout ordre O de F , tout élément x de F autre que le premier, a un *précédent* x^- (dernier élément de la partie formée par les éléments qui sont avant x); tout élément x autre que le dernier a un *suivant* x^+ . F est donc un ensemble *discret* (admettant un *dernier élément*); chaque partie A non vide de P est aussi un ensemble *discret* (chap. I, § 10, p. 42) et l'on peut raisonner par induction complète dans F ou dans A .

THÉORÈME 8. — Soient F_1, F_2 deux ensembles ordinalement finis, semblables dans une application biunivoque

$$(\alpha) \quad F_1 \approx F_2$$

et ayant en commun une section commençante A . Tout élément x

de A est sa propre image dans l'application $\alpha : \alpha x = x$; α applique semblablement $F_1 - A$ sur $F_2 - A$ ⁽¹⁾.

Le théorème est évident si A est vide.

S'il n'est pas vide, A possède un premier élément a , qui est aussi premier élément de F_1 et de F_2 , ce qui, puisque α applique semblablement F_1 sur F_2 , entraîne

$$\alpha a = a.$$

Soient m un élément de A , M l'ensemble des $x \in A$ tels que $x \leq m$. La propriété (de l'élément m)

$$(\mathcal{X}) \quad \alpha x = x \quad \text{pour tout } x \in M$$

est vraie pour $m = a$; si elle est vraie pour un élément m distinct du dernier élément de A , α applique semblablement $F_1 - M$ sur $F_2 - M$; par suite, l'élément m^+ suivant m dans A , donc premier élément de $F_1 - M$ et premier élément de $F_2 - M$, est appliqué sur lui-même : m^+ a donc aussi la propriété $(\mathcal{X})$, et finalement tous les éléments de A ont cette propriété :

$$\alpha x = x \quad \text{pour tout } x \in A.$$

Il est clair que, dans ces conditions, α applique semblablement $F_1 - A$ sur $F_2 - A$.

COROLLAIRE 1. — Soient O_1, O_2 deux ordres d'un ensemble ordinalement fini F , tels que F_{O_1}, F_{O_2} aient en commun une section commençante A : il existe une application biunivoque α de F sur lui-même conservant chaque élément de A et appliquant semblablement $F - A$ (avec l'ordre induit par O_1) sur $F - A$ (avec l'ordre induit par O_2).

COROLLAIRE 2. — Un ensemble ordinalement fini F pourvu d'un ordre O , n'a pas d'autre application biunivoque semblable sur lui-même que l'application identique.

Il suffit d'appliquer le théorème 8 en prenant

$$F_1 = F_2 = F, \quad A = F.$$

COROLLAIRE 3. — Toute partie X d'un ensemble ordinalement fini F est ordinalement finie.

⁽¹⁾ Ce théorème généralise le théorème 1 de la Note de M. Denjoy (qui n'est autre que notre corollaire 2); il a l'avantage d'entraîner immédiatement que toute partie d'un ensemble fini est finie (cor. 3).

X est ordonnable, par exemple à partir d'un ordre de F , par restriction. Soient Ω_1, Ω_2 deux ordres de X , faisant de X respectivement des ensembles ordonnés X_1, X_2 . Ordonnons le complément $Y = F - X$ d'une façon quelconque (par exemple par restriction à partir de n'importe quel ordre de F) : en plaçant Y avant X_i , nous obtenons un ordre O_i de F ; soit $F_i = Y + X_i$ ($i = 1, 2$) l'ensemble F ainsi ordonné.

F étant ordinalement fini, F_1 et F_2 sont semblables dans une application biunivoque α : d'après le théorème 8, la section commençante commune Y est appliquée identiquement sur elle-même, et $X_1 = F_1 - Y$, $X_2 = F_2 - Y$ sont semblables.

LEMME. — Soit A une partie véritable, ordinalement finie, pourvue d'un certain ordre O , d'un ensemble M quelconque; si $m \in M - A$, les deux ensembles ordonnés

$$B = \{m\} + A, \quad C = A \cup \{m\}$$

obtenus en plaçant m avant A et après A , sont semblables.

Soient a le premier élément de A , d le dernier. L'application φ de B sur C définie par

$$\begin{aligned} \varphi m &= a \\ \varphi x &= x^+ \quad \text{pour tout } x \neq d \quad (x \in A) \\ \varphi d &= m \end{aligned}$$

est une application de B sur C , biunivoque [puisque $x < y$ ($< d$) entraîne $x^+ < y^+$]. Soient b_1, b_2 deux éléments de B vérifiant $b_1 < b_2$; posons

$$\varphi b_1 = c_1, \quad \varphi b_2 = c_2.$$

Si $b_1 = m$, nous avons $c_1 = a$, premier élément de C , donc $c_1 < c_2$.

Si $b_2 = d$, nous avons $c_2 = m$, dernier élément de C , donc $c_1 < c_2$.

Si b_1 est différent de m et b_2 différent de d , b_1 et b_2 ($\in A$) ont dans A des suivants

$$b_1^+ = \varphi b_1 = c_1, \quad b_2^+ = \varphi b_2 = c_2,$$

et nous avons encore $c_1 < c_2$.

B et C sont donc semblables.

THÉORÈME 9. — Si F est une partie véritable, ordinalement finie, d'un ensemble M , et si $m \in M - F$, l'ensemble $G = F \cup \{m\}$ est ordinalement fini.

On peut ordonner G (en plaçant, par exemple, $\{m\}$ avant F).

Soient G_1, G_2 les ensembles ordonnés obtenus en munissant G de deux ordres quelconques O_1, O_2 ; O_1, O_2 restreints à $F (\subset G)$, font de F des ensembles ordonnés que nous désignons respectivement par F_1, F_2 .

Par hypothèse, F_1 et F_2 sont semblables. Les ensembles $F_1 + \{m\}$, $F_2 + \{m\}$ qui s'en déduisent en plaçant $\{m\}$ après F_1 et après F_2 , sont semblables également.

Il suffit donc de montrer que G_i et $F_i + \{m\}$ sont semblables ($i = 1, 2$). Pour $i = 1$, par exemple, désignons par Z_1 l'ensemble des éléments de G_1 inférieurs à m dans l'ordre O_1 , par A_1 l'ensemble des éléments de G_1 supérieurs à m dans l'ordre O_1 : l'ensemble $G_1 = Z_1 + \{m\} + A_1$ est, d'après le lemme, semblable à

$$Z_1 + A_1 + \{m\} = F_1 + \{m\}.$$

C. Q. F. D.

4. Comparaison de deux ensembles ordinalement finis. — Soient d'abord F un ensemble ordinalement fini, ordonné par un ordre O , A une partie de F ordonnée par un ordre Ω .

THÉOREME 10. — *Si A est semblable à F , on a*

$$A = F.$$

Ordonnons, en effet, le complément $B = F - A$ d'une façon quelconque, par exemple par l'ordre O restreint à B . En plaçant A ordonné par Ω avant B ainsi ordonné, nous faisons de F un nouvel ensemble ordonné $F' = A + B$. F' , semblable à F , qui est lui-même semblable à A , est semblable à A : soit α l'application biunivoque de F' sur A qui réalise cette similitude. Puisque F' et A ont en commun la section commençante A , α , d'après le théorème 8, applique identiquement A sur lui-même, et semblablement $F' - A = B$ sur $A - A = \emptyset$: B est donc vide, et $A = F$.

COROLLAIRE (propriété de Dedekind). — *Un ensemble ordinalement fini F et une partie véritable A de F , n'ont jamais la même puissance.*

Si A était l'image de F par une application biunivoque φ , un ordre O de F transféré sur A au moyen de φ , ferait de A un ensemble ordonné semblable à F . On aurait alors, d'après le théorème 10, $A = F$, contrairement à l'hypothèse ($A \subset F$).

THÉOREME 11. — *Soient F et F' deux ensembles ordinalement finis : l'un de ces deux ensembles est semblable à une partie de l'autre.*

Ce théorème est évident si l'un des ensembles F, F' est vide. Supposons donc $F, F' \neq \emptyset$. Désignons par X l'ensemble des éléments x de F tels qu'on puisse associer à x un élément x' de F' de façon que les sections commençantes $C(x, F)$ et $C(x', F')$ soient semblables ⁽¹⁾. Le premier élément a de F appartient à X (on prendra $x' = a'$, premier élément de F'), donc X n'est pas vide et possède un dernier élément d . Si d coïncide avec le dernier élément z de F, le théorème est établi : $F = C(d, F)$ est semblable à la partie $C(d', F')$ de F', d' étant l'élément associé à d . Si d est différent de z , il faut que d' coïncide avec le dernier élément z' de F' [et alors F' est semblable à $C(d, F)$, partie de F] : dans le cas contraire, en effet, d et d' auraient respectivement des suivants, d^+ et d'^+ dans F et F', et en associant d'^+ à d^+ ($d'^+ = d'^+$), on ferait de

$$C(d^+, F) = C(d, F) + \{d^+\}$$

un ensemble semblable à

$$C(d'^+, F) = C(d', F) + \{d'^+\},$$

ce qui entraînerait $d^+ \in X$, contrairement à la définition de d .

COROLLAIRE. — *Deux ensembles finis F, F' ont toujours des puissances comparables.*

§. Ensembles doublement bien ordonnés. — **THÉOREME 12.** — *Tout ensemble E doublement bien ordonné est ordinalement fini.*

A chaque élément x de E, associons la section commençante $C(x, E)$. Considérons la propriété (concernant l'élément x)

($\mathcal{P}$) $C(x, E)$ est un ensemble ordinalement fini.

Le premier élément a de E a la propriété $\mathcal{P}$, puisque $C(a, E) = \{a\}$ est fini. Soit $x \neq a$; si le précédent x^- de x a la propriété $\mathcal{P}$, x l'a aussi, d'après le théorème 9, puisque

$$C(x, E) = C(x^-, E) + \{x\}.$$

Il en résulte, par induction complète, que tout élément de E a la propriété $\mathcal{P}$. Donc, si nous désignons par z le dernier élément de E, $C(z, E) = E$ est fini.

C. Q. F. D.

⁽¹⁾ Rappelons que $C(x, F)$ est, par définition, l'ensemble des éléments de F inférieurs ou égaux à x .

Le théorème 12 et le corollaire des théorèmes 7 et 7' entraînent que *chacune des deux propriétés* :

E est doublement bien ordonné,

E est ordinalement fini,

implique l'autre ⁽¹⁾.

Indiquons encore quelques propriétés simples équivalentes à celles d'être doublement bien ordonné, ou ordinalement fini.

THÉOREME 13. — *Pour qu'un ensemble E totalement ordonné (par O) soit doublement bien ordonné (par O), il faut et il suffit que toute section finissante non vide ait un premier élément et que toute section commençante non vide ait un dernier élément.*

La condition est évidemment nécessaire. Montrons qu'elle est suffisante. X étant une partie non vide de E, désignons par C l'ensemble des éléments *c* de E vérifiant

$$c \leq x \quad \text{pour au moins un } x \in X,$$

C est une section commençante, contenant X, donc non vide. Le dernier élément *z* de C ne peut pas vérifier une inégalité stricte $z < x$, où $x \in X \subseteq C$; *z* appartient donc à X, et en est dernier élément. On montre, par un raisonnement analogue, que X a un premier élément.

COROLLAIRE. — *Un ensemble bien ordonné dans lequel toute section commençante non vide a un dernier élément, est doublement bien ordonné.*

THÉOREME 14. — *Pour qu'un ensemble E bien ordonné (par O) soit doublement bien ordonné, il faut et il suffit que tout élément de E, sauf le premier *a*, admette un précédent et que E possède un dernier élément : les ensembles doublement bien ordonnés sont donc les ensembles discrets (chap. I, § 10, p. 42) possédant un dernier élément.*

La condition est évidemment nécessaire. Elle est suffisante, car si une section commençante C non vide coïncide avec E, elle a par hypo-

⁽¹⁾ La propriété d'être doublement bien ordonné a été utilisée par quelques auteurs pour la définition des ensembles finis : cf. STÄCKEL, *Zu H. Webers elementarer Mengenlehre* (Jahr. d. M. V., t. 16, 1907, p. 425); ENRIQUES (Sui fondamenti dell' Aritmetica e sul principio dell' invarianza del numero (Rend. R. Accad. Lincei, II, t. 32, 1923, p. 113-117). Le théorème 12 est le théorème III de la Note d'Enriques.

thèse un dernier élément; si $C \neq E$, $E - C$, non vide, a un premier élément $p (\neq a$, puisque $C \neq \emptyset$) dont le précédent p^- est *dernier élément* de C . Ainsi, toute section commençante non vide C a un dernier élément, et il suffit d'appliquer le corollaire précédent.

Remarque (Stäckel). — Un ensemble E peut être ordonné, avoir un premier élément a , un dernier élément z , être tel que tout élément $x \neq a$ ait un précédent x^- et que tout élément $y \neq z$ ait un suivant y^+ , sans pour cela être doublement bien ordonné. (C'est ce qui a lieu, par exemple, pour l'ensemble des nombres naturels ordonné de la façon suivante

$$1, 3, 5, \dots, 2n+1, \dots, \dots, 2n, \dots, 6, 4, 2.$$

L'ensemble des nombres impairs n'a pas de dernier élément, l'ensemble des nombres pairs n'a pas de premier élément.)

THÉORÈME 15. — *La somme $S = A + B + \dots + M$ d'une famille doublement bien ordonnée $\mathcal{F}$ d'ensembles $A, B, \dots, M$ doublement bien ordonnés deux à deux disjoints, est doublement bien ordonnée.*

Posons $x < y$ ($x, y \in S$) dans chacun des deux cas suivants :

1° x et y appartiennent à un même ensemble $C \in \mathcal{F}$ et x précède y dans l'ordre de C ;

2° x et y appartiennent à deux ensembles différents $C, C' \in \mathcal{F}$ et C précède C' dans l'ordre de $\mathcal{F}$ ($x \in C, y \in C'$).

La relation $<$ ainsi définie dans S est visiblement un ordre total. S_1 étant une partie non vide de S , soit $\mathcal{F}_1 (\subseteq \mathcal{F})$, la famille des $C \in \mathcal{F}$ tels que $C \cap S_1 \neq \emptyset$, $\mathcal{F}_1$ n'est pas vide, donc possède dans l'ordre de $\mathcal{F}$ un premier élément C_1 ; $C_1 \cap S_1$ n'est pas vide, donc possède, dans l'ordre de C_1 , un premier élément p_1 , qui est aussi premier élément de S_1 dans l'ordre de S . On montre, par un raisonnement tout à fait analogue, que S_1 a de même un dernier élément.

Remarque. — La démonstration s'applique sans changement à la réunion générale d'une famille doublement bien ordonnée d'ensembles doublement bien ordonnés.

COROLLAIRES. — 1. *La réunion d'une famille doublement bien ordonnée, $\mathcal{F}$, de parties doublement bien ordonnées d'un ensemble E , est un ensemble doublement bien ordonné.*

On se ramène immédiatement au théorème précédent en remplaçant chaque partie X de $\mathcal{F}$ par $X' = X - (X \cap R_X)$, où R_X désigne la réunion des éléments de $\mathcal{F}$ antérieurs à X .

2. Le produit $P = F \times F'$ de deux ensembles doublement bien ordonnés est doublement bien ordonné.

P est la somme de ses parties $X' = \bigcup_{x \in X} (x, x')$, ensembles des couples (x, x') dans lesquels le second élément x' est un élément fixe de F' . Chaque ensemble X' , étant semblable à F , est doublement bien ordonné; la famille $\mathcal{F}$ des X' , étant semblable à F' , est doublement bien ordonnée. P est donc doublement bien ordonné, d'après le théorème 15.

6. **Théorie cardinale.** — *Définition* ⁽¹⁾. — Un ensemble F est dit *cardinalement fini* s'il vérifie la *condition minimale* (pour ses sous-ensembles) : toute famille $\mathcal{M}$ non vide de parties de F contient au moins une partie minimale A, c'est-à-dire ne comprenant comme sous-ensemble aucune autre partie X qui soit élément de $\mathcal{M}$ ($X \in \mathcal{M}$ et $X \subseteq A$ entraînent $X = A$).

L'ensemble vide $\emptyset$ est cardinalement fini : nous n'avons ici qu'une famille non vide de parties, $\mathcal{M} = \{\emptyset\}$, dont l'unique élément, $\emptyset$, est minimal.

L'ensemble $\{a\}$ est cardinalement fini; ses parties sont, en effet, $\emptyset$ et $\{a\}$, donc les différentes familles $\mathcal{M}$ sont $\{\emptyset\}$, $\{\{a\}\}$, $\{\emptyset, \{a\}\}$: chacune d'elles contient une partie minimale.

THÉORÈME 16. — Si un ensemble F' a même puissance qu'un ensemble cardinalement fini F, F' est cardinalement fini.

Une application biunivoque de F sur F' établit une correspondance biunivoque entre les parties de ces ensembles, respectant les propriétés d'inclusion. A une famille $\mathcal{M}'$ non vide de parties de F' correspond une famille $\mathcal{M}$ non vide de parties de F; $\mathcal{M}$ contient au moins une partie minimale A, à laquelle correspond dans $\mathcal{M}'$ une partie minimale A' .

THÉORÈME 17. — Toute partie G d'un ensemble cardinalement fini F est un ensemble cardinalement fini.

Toute famille $\mathcal{M}$ non vide de parties de G est, en effet, une famille de parties de F, donc contient au moins une partie minimale A.

THÉORÈME 18. — Pour qu'un ensemble F soit cardinalement fini, il

⁽¹⁾ TARSKI, *Sur les ensembles finis* (*Fundamenta Math.*, t. 6, 1925, p. 45).

faut et il suffit qu'il vérifie la condition maximale (pour ses sous-ensembles) : toute famille $\mathcal{M}$ non vide de parties de F contient au moins une partie maximale Z ($X \in \mathcal{M}$ et $X \supseteq Z$ entraînent $X = Z$); en d'autres termes, la condition maximale et la condition minimale pour les parties d'un ensemble sont deux propriétés équivalentes.

A toute famille $\mathcal{M}$ de parties X de F , associons la famille $\mathcal{N}$ des compléments $Y = F - X$: $\mathcal{M}$ et $\mathcal{N}$ sont en même temps non vides; si $\mathcal{M}$ contient une partie maximale A , $\mathcal{N}$ contient la partie minimale $Z = F - A$, et inversement; le théorème en résulte.

THÉOREME 19. — *Si F, G , parties disjointes d'un ensemble E , sont cardinalement finies, leur somme $S = F + G$ est cardinalement finie.*

Soit X une partie de S ; posons $Y = X \cap F$, $Z = X \cap G$: nous avons

$$Y \cap Z = \emptyset, \quad X = Y + Z.$$

$\mathcal{M}$ étant une famille non vide de parties X de S , désignons par $\mathcal{N}$ la famille des Y correspondants. Puisqu'on a $Y \subseteq F$, $\mathcal{N}$ est une famille non vide de parties de F , donc contient un ensemble minimal A . Soit $\mathcal{X}$ la famille des parties P de G telles que $A + P \in \mathcal{M}$. Puisque $A \in \mathcal{N}$, $\mathcal{X}$ n'est pas vide, donc contient un ensemble minimal B . L'ensemble $A + B$, qui appartient à la famille $\mathcal{M}$, en est élément minimal, car les relations $X \in \mathcal{M}$, $X \subseteq A + B$ entraînent $X \cap F = Y \in \mathcal{N}$ et $Y \subseteq A$, donc $Y = A$, $X \cap G = Z \in \mathcal{X}$. Comme on a, en outre, $Z \subseteq B$, il vient finalement $Z = B$, donc $X = A + B$.

COROLLAIRES. — 1. *Si F et G , parties quelconques d'un ensemble E , sont cardinalement finies, leur réunion $R = F \cup G$ est cardinalement finie.*

L'ensemble $G' = G - (F \cap G) \subseteq G$ est cardinalement fini, et disjoint de F : $R = F \cup G = F + G'$ est donc cardinalement fini.

2. *Si A est une partie véritable, cardinalement finie, d'un ensemble E et si $x \in E - A$, $A + \{x\}$ est cardinalement fini.*

3. *Si chaque partie véritable d'un ensemble H non vide est cardinalement finie, H est cardinalement fini.*

Soit, en effet, $h \in H$; $H - \{h\}$ est cardinalement fini, donc

$$H = (H - \{h\}) + \{h\}$$

l'est aussi.

THÉOREME 20 (Équivalence avec la définition de Russell et Whitehead). — *Pour qu'une partie A d'un ensemble E soit cardinalement finie, il faut et il suffit que A appartienne à toute famille Φ de parties de E qui possède les deux propriétés suivantes :*

$$1^{\circ} \emptyset \in \Phi;$$

$$2^{\circ} X \in \Phi \text{ et } a \in A \text{ entraînent } X \cup \{a\} \in \Phi.$$

La condition est *suffisante*. En effet, la famille $\mathcal{F}$ des parties cardinalement finies de E possède les propriétés 1° et 2° , donc, si A appartient à toute famille Φ , A appartient à $\mathcal{F}$, c'est-à-dire est cardinalement fini.

Inversement, supposons A cardinalement fini; Φ étant une famille de parties de E possédant les propriétés 1° et 2° , considérons la famille $\mathcal{N} = \Phi \cap \mathcal{P}(A)$ des parties de A qui appartiennent à Φ . Comme la partie vide de A est un élément de $\mathcal{N}$, $\mathcal{N}$ n'est pas vide, donc possède un ensemble maximal $M (\subseteq A)$. Si nous avons $M \subset A$, l'ensemble $M + \{a\}$, où $a \in A - M$, appartiendrait à Φ et à $\mathcal{P}(A)$, donc à $\mathcal{N}$, ce qui est impossible d'après la maximalité de M. Nous avons donc $A = M \in \Phi$.

C. Q. F. D.

Remarques. — 1. Si A est cardinalement fini, l'intersection $\mathcal{N} = \Phi \cap \mathcal{P}(A)$ coïncide, pour toute famille Φ , avec l'ensemble $\mathcal{P}(A)$ de toutes les parties de A : dans le cas contraire, en effet, $\mathcal{P}(A) - \mathcal{N}$, non vide, aurait un élément *minimal* $H \neq \emptyset$; mais alors h désignant un élément de H, $H - \{h\}$ appartiendrait à $\mathcal{N}$ et $H = (H - \{h\}) + \{h\}$ appartiendrait à Φ , donc à $\mathcal{N}$, ce qui est contradictoire.

2. On notera que l'ensemble $\mathcal{P}(E)$ de toutes les parties de E est une famille Φ possédant les propriétés 1° et 2° .

3. On établit, tout à fait de la même façon, l'équivalence avec la définition, assez voisine de celle de Russel, donnée par Bourbaki [*Foundations of Mathematics for the working Mathematician* (*J. Symb. Logic.*, t. 14, 1949, p. 1-8).

THÉOREME 20'. — *Pour qu'une partie A non vide d'un ensemble E soit cardinalement finie, il faut et il suffit que A appartienne à toute famille ψ de parties de E qui possède les des deux propriétés suivantes :*

$$1^{\circ} \text{ Si } a \in E, \{a\} \in \psi;$$

$$2^{\circ} \psi \text{ est fermée pour la réunion des parties}$$

$$X \in \psi \text{ et } Y \in \psi \text{ entraînent } X \cup Y \in \psi.$$

THÉOREME 21. — *Si E est un ensemble cardinalement fini, l'ensemble de ses parties, $\mathcal{P}(E)$, est cardinalement fini.*

Soit $\mathcal{L}$ la famille des parties M de E ayant la propriété : l'ensemble $\mathfrak{T}(M)$ des parties de M est cardinalement fini. Nous avons : $\emptyset \in \mathcal{L}$, puisque $\mathfrak{T}(\emptyset) = \{\emptyset\}$ est cardinalement fini. Si nous montrons que :

2° $X \in \mathcal{L}$ et $a \in E$ entraînent $X \cup \{a\} \in \mathcal{L}$.

la famille $\mathcal{L}$, vérifiant les conditions 1° et 2° du théorème 20, où A est remplacé par l'ensemble E , cardinalement fini, contiendra comme élément l'ensemble E ; l'ensemble $\mathfrak{T}(E)$ des parties de E sera, par conséquent, fini.

La propriété 2° est évidente si nous avons $a \in X$. Supposons donc $a \notin X$, et montrons que $\mathfrak{T}(X + \{a\})$ est un ensemble cardinalement fini. Si Y est une partie de X , $Y + \{a\}$, qui n'appartient pas à $\mathfrak{T}(X)$, est une partie de $\mathfrak{T}(X + \{a\})$: nous avons donc

$$Y + \{a\} \in \mathfrak{T}(X + \{a\}) - \mathfrak{T}(X).$$

Inversement, si $Z \in \mathfrak{T}(X + \{a\}) - \mathfrak{T}(X)$, nous avons nécessairement $a \in Z$, donc $Z = Y + \{a\}$, où $Y \in \mathfrak{T}(X)$. Ainsi, l'application

$$Y \rightarrow Y + \{a\}, \quad \text{où } Y \in \mathfrak{T}(X)$$

est une application *biunivoque* de $\mathfrak{T}(X)$ sur $\mathfrak{T}(X + \{a\}) - \mathfrak{T}(X)$. Puisque $\mathfrak{T}(X)$ est cardinalement fini, il en est de même de

$$Q = \mathfrak{T}(X + \{a\}) - \mathfrak{T}(X),$$

donc aussi de $\mathfrak{T}(X + \{a\}) = \mathfrak{T}(X) + Q$.

Remarque. — Il est clair inversement qu'un ensemble E tel que $\mathfrak{T}(E)$ soit cardinalement fini, est lui-même cardinalement fini : E correspond, en effet, biunivoquement à l'ensemble $\mathcal{S}$ des parties $\{x\}$ formées d'un élément x appartenant à E ; et cet ensemble $\mathcal{S}$ est cardinalement fini, comme partie de $\mathfrak{T}(E)$.

THÉORÈME 22. — *Pour qu'un ensemble E soit cardinalement fini, il faut et il suffit qu'il soit doublement bien ordonné.*

1° *La condition est nécessaire.* — Soit E un ensemble cardinalement fini. L'ensemble Γ des chaînes de parties de E n'est pas vide car $\{\emptyset\}$, $\{E\}$, $\{\emptyset, E\}$ (si E n'est pas vide) sont de telles chaînes. Γ , contenu dans l'ensemble cardinalement fini $\mathfrak{T}(E)$, possède donc au moins un élément maximal $\mathcal{M}$. L'existence de cette chaîne maximale $\mathcal{M}$ permet d'ordonner totalement l'ensemble E .

Toute partie non vide $\mathcal{F}$ de $\mathcal{M}$ possède, puisque E est cardinalement fini, un élément minimal, qui est élément *minimum* de $\mathcal{F}$, puisque $\mathcal{F}$,

partie d'une chaîne, est elle-même une chaîne. De même, $\mathcal{T}$ a un élément *maximum* et, par conséquent, la chaîne maximale $\mathcal{M}$ est doublement bien ordonnée. Il en est de même de E .

2° *La condition est suffisante.* — Soient E un ensemble doublement bien ordonné, $\mathcal{M}$ une chaîne maximale de parties de E , construite à partir de l'ordre de E , et elle-même doublement bien ordonnée. $\mathcal{M}$ étant maximale, nous avons $\emptyset \in \mathcal{M}$, $E \in \mathcal{M}$.

Soit $\mathcal{L}$ la famille des parties de E qui figurent dans $\mathcal{M}$ et sont cardinalement finies : puisque $\emptyset \in \mathcal{L}$, $\mathcal{L}$ n'est pas vide ; par conséquent, $\mathcal{L}$ possède un élément *maximum* C ($C \subseteq E$). Si $C = E$, E est cardinalement fini et le théorème est démontré.

Supposons donc C partie véritable de E : $C \subset E$. Alors, E n'appartient pas à $\mathcal{L}$, donc $\mathcal{M} - \mathcal{L} = \mathcal{L}'$ n'est pas vide et a, par suite, un élément *minimum* D qui, n'appartenant pas à $\mathcal{L}$, ne peut pas être cardinalement fini.

C et D appartenant à la chaîne $\mathcal{M}$, et $D \subseteq C$ étant impossible puisque $C (\in \mathcal{L})$ est cardinalement fini, nous avons $C \subset D$. Si une partie X de E , figurant dans la chaîne $\mathcal{M}$, est cardinalement finie, X appartient à $\mathcal{L}$ et l'on a $X \subseteq C$; si X n'est pas cardinalement finie, X appartient à $\mathcal{L}'$ et l'on a $D \subseteq X$. Aucun élément X de $\mathcal{M}$ n'est donc strictement compris entre C et D .

Soit a un élément de $D - C$. On a

$$(1) \quad C \subset C + \{a\} \subset D,$$

la deuxième inclusion étant stricte parce que $C + \{a\}$ est, comme C , cardinalement fini. D'après (1), $C + \{a\}$ n'appartient pas à la chaîne $\mathcal{M}$, en l'intercalant entre C et D , nous obtiendrions une chaîne $\mathcal{M}'$ contenant strictement $\mathcal{M}$, ce qui est absurde puisque $\mathcal{M}$ a été supposée maximale. Il est donc impossible que C soit partie véritable de E , ce qui établit la proposition.

Nous avons ainsi démontré l'équivalence logique des diverses propriétés fondamentales d'un ensemble E considérées au chapitre I (§ 10, p. 46) :

1° E est ordinalement fini, c'est-à-dire totalement ordonné et semblable à lui-même dans toutes les ordinations possibles ;

2° E est doublement bien ordonné ;

3° E est bien ordonné ; tout élément de E , sauf le premier, a un pré-

cèdent; E possède un dernier élément (en d'autres termes, E est un ensemble discret avec dernier élément);

4° E est cardinalement fini, c'est-à-dire vérifie la condition minimale (ou maximale) pour ses sous-ensembles;

5° E appartient à toute famille Φ de parties de E telle que :
 a. $\emptyset \in \Phi$,
 b. $X \in \Phi$ et $a \in E$ entraînent $X \cup \{a\} \in \Phi$.

Tout ensemble ayant l'une de ces propriétés et, par conséquent, toutes les autres, est, par définition, *un ensemble fini*. Toute partie d'un ensemble fini est finie; la réunion, la somme, le produit d'une famille finie d'ensembles finis sont finis; l'ensemble des parties d'un ensemble fini est fini.

NOTE II.

NOMBRES NATURELS.

1. **Ensembles naturels.** — Nous avons appelé *ensemble discret* tout ensemble E bien ordonné dans lequel chaque élément, sauf le premier a , possède un précédent (chap. I, § 10, p. 42). Un tel ensemble se prête au *raisonnement par induction complète*. C'est un *ensemble fini* s'il possède un dernier élément, et seulement dans ce cas (Note I, p. 412).

Nous appellerons *ensemble naturel* ⁽¹⁾ tout ensemble discret non vide sans dernier élément ou, ce qui revient au même, tout ensemble discret infini. Il est normal d'étudier les propriétés de ces ensembles infinis qui paraissent *a priori*, et qui sont en fait, les plus proches des ensembles finis. De plus, comme nous allons le voir, ils jouent un rôle fondamental dans la comparaison des ensembles finis ⁽²⁾.

⁽¹⁾ Cette terminologie diffère de celle de la première édition : nous appelions *ensemble naturel* ce qui sera nommé ici *ensemble péanien* (ensemble vérifiant les axiomes de Peano, § 2, p. 425). A vrai dire, ces deux propriétés sont équivalentes (§ 2, p. 430) et ce changement de vocabulaire est destiné seulement à permettre un exposé plus complet et plus précis.

Signalons, d'autre part, que dans cette Note II, nous supposons connus certains résultats de la Note I.

⁽²⁾ Nous étudierons les ensembles naturels, catégorie particulière d'ensembles *infinis*, sans nous préoccuper de leur « existence » : les problèmes d'existence risquent d'être fort confus, en raison des sens très divers qui peuvent être attribués au mot « exister ». Il ne paraît pas déraisonnable, à vrai dire, de considérer qu'un ensemble naturel existe en tant que création de l'esprit humain, en tant qu'être défini par une combinaison précise de notions dont chacune a déjà été jugée admissible.

Il est indispensable de noter, d'autre part, qu'une foule d'êtres mathématiques se construisent facilement à partir de celui-là. En rejetant la notion d'ensemble naturel (ce qu'assurément on est libre de faire !), on se condamnera à refuser la presque totalité des acquisitions mathématiques.

Au surplus, c'est plutôt la non-existence qui a un sens précis pour le mathématicien : ce qui, à ses yeux, n'existe pas, c'est ce qui est contradictoire. Or « la non contradiction de l'Arithmétique » est maintenant un fait établi.

Soient D un ensemble discret, a son premier élément. Le *segment initial* $S = [a, n]$, ensemble des éléments x de D qui vérifient $(a \leq) x \leq n$, est une section commençante de D .

THÉOREME 1. — *Tout segment initial $S = [a, n]$ d'un ensemble discret D , est un ensemble fini.*

La proposition est évidente si D est fini, ou si $n = a$.

S est lui-même un ensemble discret (chap. I, § 10, th. 3); ayant d'autre part un dernier élément, n , S est bien un ensemble fini.

COROLLAIRE. — *Tout ensemble F ayant même puissance qu'un segment initial $[a, n]$ d'un ensemble naturel N , est fini.*

THÉOREME 2. — *Si une section commençante C d'un ensemble discret D est une partie véritable de D ($\emptyset \subset C \subset D$), C est un segment initial $[a, n]$ de D , donc un ensemble fini.*

Puisque C n'est pas vide, le premier élément a de D appartient à C . Le complément $T = D - C$ ($\neq \emptyset$) a un premier élément $t > a$. Le précédent $t - n$ de t appartient à C et en est dernier élément. La section commençante C coïncide donc avec le segment $[a, n]$, qui est fini d'après le théorème 1.

COROLLAIRE. — *Toute partie infinie P d'un ensemble naturel N est un ensemble naturel (avec l'ordre de N restreint à P).*

En tant que partie de l'ensemble discret N , P est un ensemble discret (chap. I, § 10, p. 42), et si P avait un dernier élément, il serait fini, contrairement à l'hypothèse.

THÉOREME 3. — *Soient Δ , un ensemble discret, fini ou infini, de premier élément α , E un ensemble bien ordonné infini, de premier élément a . On peut construire une application semblable f de Δ sur une section commençante S de E ; $S = f\Delta$ est un ensemble discret.*

Considérons la propriété $(\mathfrak{X})$ suivante, concernant un élément v de Δ : $(\mathfrak{X})$ le segment $[\alpha, v]$ de Δ est semblable à un segment initial $[a, n]$ de E .

Le premier élément α de Δ a la propriété $(\mathfrak{X})$, puisque $\{\alpha\}$ est semblable à $\{a\}$. De plus, un élément $v \neq \alpha$, tel que son précédent $v-$ dans l'ensemble discret Δ ait la propriété $(\mathfrak{X})$, a lui-même cette

propriété : en effet, le segment $[\alpha, \nu^-]$ étant semblable au segment $[a, m]$ de E, $[\alpha, \nu] = [\alpha, \nu^-] + \{\nu\}$ est semblable à $[a, m^+] = [a, m] + \{m^+\}$, m^+ désignant l'élément qui suit m dans l'ensemble bien ordonné E. Par conséquent, tout élément ν de Δ a la propriété ($\mathfrak{E}$).

Si ν est fixé, il existe dans E un seul élément n vérifiant la condition ($\mathfrak{E}$). En effet, d'après le théorème 1, le segment $[\alpha, \nu]$ est fini; tout segment semblable $[a, n]$ l'est aussi. Or, si n, n' sont deux éléments distincts de E, l'un des segments $[a, n], [a, n']$ est partie véritable de l'autre, donc ne peut pas lui être semblable puisqu'il s'agit d'ensembles finis (Note I, th. 10, p. 410).

Nous avons, par suite, une application univoque

$$(f) \quad \nu \rightarrow n = f\nu$$

de Δ dans E. Soit $S = f\Delta \subseteq E$ l'image de Δ dans E; ordonnons S par restriction de l'ordre de E, et montrons que l'application f de Δ sur S est biunivoque et respecte les ordres, S est donc semblable à E. Il suffit d'établir que l'inégalité $\nu_1 < \nu$ dans Δ entraîne $n_1 < n$ ($n_1 = f\nu_1, n = f\nu$) dans E ou S. Or, l'application φ_ν qui, d'après la propriété ($\mathfrak{E}$), applique semblablement $[\alpha, \nu]$ sur $[a, n]$, applique le sous-segment $[\alpha, \nu_1]$ sur un segment $[a, m_1]$ de $[a, n]$, qui en est une partie véritable, de sorte qu'on a : $m_1 = \varphi_\nu \nu_1 < n$. Mais $[a, m_1]$ est aussi un segment de E, ce qui entraîne $m_1 = n_1$ d'après l'unicité de l'élément n_1 associé à ν_1 par la propriété ($\mathfrak{E}$). Nous avons donc bien $n_1 < n$ et, en outre,

$$f\nu_1 = \varphi_\nu \nu_1,$$

ce qui montre que l'application φ_ν est la restriction de f au segment $[\alpha, \nu]$.

Tout élément n' de E inférieur à un élément $n = f\nu$ de S appartient au segment $[a, n]$, donc admet dans $[\alpha, \nu]$ une image inverse $\nu' = f^{-1}n'$: S est une section commençante de E. Puisqu'il est semblable à l'ensemble discret Δ , S est lui-même un ensemble discret.

Le théorème 3 admet plusieurs conséquences importantes :

1^o Supposons Δ infini : Δ est alors un ensemble naturel. L'ensemble discret S, semblable à Δ , est nécessairement infini; c'est un ensemble naturel. On voit (à partir du moment où l'on admet l'existence d'un ensemble naturel Δ) que tout ensemble bien ordonné infini E contient un ensemble naturel, qui est une section commençante S de E.

2^o Prenons encore pour Δ un ensemble naturel, et supposons que E

soit lui-même un *ensemble naturel*, donc *discret* : alors S , section commençante de E et ensemble infini, ne peut pas, d'après le théorème 2, être une partie véritable de E : nous avons

$$S = E$$

et, par conséquent, deux ensembles naturels quelconques Δ , E sont semblables.

Il suffira donc de choisir, une fois pour toutes, un ensemble naturel N dont les éléments seront nommés, pour la commodité du langage, *nombres naturels*; le premier sera appelé *un* et désigné par 1, le suivant de un sera appelé *deux* et désigné par 2, etc. :

$$N = \{1, 2, \dots, n, \dots\}.$$

3° $N - \{1\}$, $N - [1, n]$ ou une *partie infinie quelconque* P de N , sont, d'après le corollaire du théorème 2, des ensembles naturels, c'est-à-dire des ensembles semblables à N : un ensemble naturel est donc semblable à certaines de ses parties véritables. Il en est de même pour tout ensemble infini bien ordonné E . Soit, en effet,

$$E = N + E',$$

où N est un ensemble naturel, section commençante de E . Soit M une partie véritable de N , semblable à N : $M + E'$, partie véritable de E , est semblable à E . (On rapprochera cette propriété du théorème 10 sur les ensembles finis, et de son corollaire, Note I, p. 410.)

4° Dans le théorème 3, prenons comme ensemble Δ un ensemble fini F et, comme ensemble E , l'ensemble N des nombres naturels. F , ordonné totalement, est semblable à une section commençante finie S de N : on a donc $S \subset N$ et, par suite, S est un segment initial $[1, n]$. A tout ensemble fini F est ainsi associé un nombre naturel n , parfaitement déterminé, tel que F et le segment $[1, n]$ de N soient semblables. On dit que n est le nombre d'éléments de F , ou que l'ensemble F a n éléments.

Compter les éléments de F , c'est déterminer leur nombre n . A cet effet, on ordonne F en associant successivement à chacun de ses éléments les nombres naturels pris dans l'ordre de N .

Exemple :

$$F = \{a, e, i, o, u, y\}, \\ [1, n] = \{1, 2, 3, 4, 5, 6\};$$

F a six éléments.

Il est clair que : *pour que deux ensembles finis soient semblables, il faut et il suffit qu'ils aient le même nombre d'éléments.*

THÉOREME 4. — *Soient F et F' deux ensembles finis ayant respectivement n et n' éléments. Pour que F soit semblable à une partie véritable A' de F', il faut et il suffit que l'on ait $n < n'$.*

1° Supposons F semblable à une partie véritable A' de F' : ordonnons A' et $F' - A' = B'$ en restreignant à ces parties l'ordre donné O' de F', puis plaçons A' avant B', nous obtenons ainsi un certain ordre Ω' de $F' = A' + B'$. Pourvu de cet ordre, F' est encore semblable au segment $[1, n']$ de N, d'après la définition ordinaire des ensembles finis. Puisque B' n'est pas vide, le dernier élément d' de A' a pour image dans N un élément $m' < n'$. Mais les deux ensembles semblables F et A' ont le même nombre d'éléments

$$n = m', \quad \text{d'où} \quad n < n'.$$

2° Supposons $n < n'$. Alors F est semblable au segment $[1, n]$, partie véritable du segment $[1, n']$ auquel F' est semblable. Soit A' l'image dans F' du segment $[1, n]$: A' est bien une partie véritable de F', à laquelle A est semblable.

Des propositions que nous avons établies, et qui expriment que deux ensembles sont semblables, ou que l'un d'eux est semblable à une partie de l'autre, nous pouvons déduire des propositions exprimant que deux ensembles ont même puissance, ou que l'un d'eux a même puissance qu'une partie de l'autre.

Il est clair que deux ensembles semblables ont même puissance. Inversement, soient E, E' deux ensembles ayant même puissance : si E est ordonné et si l'on ordonne E' par *transfert* de l'ordre de E (cf. Note I, p. 403), on fait de E' un ensemble semblable à E.

En tenant compte de la définition ordinaire des ensembles finis, on voit que *si l'on ordonne de façon quelconque deux ensembles finis ayant même puissance, on en fait deux ensembles semblables. On en déduit :*

THÉOREME 4'. — *Soient F et F' deux ensembles finis ayant respectivement n et n' éléments. Pour que F et F' aient même puissance, il faut et il suffit que $n = n'$. Pour que F ait même puissance qu'une partie véritable A' de F', il faut et il suffit que l'on ait $n < n'$.*

Appelons *ensemble dénombrable* tout ensemble ayant même puissance que l'ensemble N des nombres naturels (ou qu'un ensemble naturel quelconque). D'après le corollaire du théorème 2, *toute partie infinie d'un ensemble dénombrable est dénombrable*. D'après les conséquences du théorème 3, *tout ensemble bien ordonné infini E contient d'une part un ensemble dénombrable, d'autre part des parties véritables qui ont même puissance que lui*.

2. Ensembles péaniens. — Appelons *ensemble péanien* tout ensemble P vérifiant les axiomes suivants ⁽¹⁾ :

1° P n'est pas vide;

2° A tout élément x de P est associé un élément bien déterminé de P , que nous désignons par x' ;

3° P contient un élément u tel que l'on ait $x' \neq u$ quel que soit $x \in P$;

4° Pour tout élément $p \neq u$ de P , il existe $x \in P$ tel que $x' = p$. Cet élément x est unique : $x' = y'$ entraîne $x = y$;

5° (Principe de récurrence) Si A est un sous-ensemble de P ayant les deux propriétés suivantes :

$$u \in A,$$

$$a \in A \quad \text{entraîne} \quad a' \in A,$$

on a

$$A = P.$$

Les axiomes précédents entraînent

$$a' \neq a \quad \text{pour tout} \quad a \in P.$$

Soit, en effet, A l'ensemble des éléments a de P tels que $a' \neq a$. Nous avons $u \in A$ (axiome 3°); soit, d'autre part, $a \in A$: l'égalité $(a')' = a'$ entraînerait (axiome 4°) $a' = a$, qui est absurde : nous avons donc $a' \in A$. Il en résulte (axiome 5°) $A = P$.

Tout ensemble naturel N est péanien. — Prenons, en effet, comme élément x' associé à x son suivant x^+ dans l'ordre de N , et comme élément u le premier élément de N : les cinq axiomes définissant les ensembles péaniens sont vérifiés.

(1) Ces axiomes ne diffèrent pas essentiellement de ceux de Peano (*Arithm. principia*, Turin, 1889; *Rivista Math.*, t. 1, 1891, p. 19). Voir aussi *Encyclopédie des Sciences Mathématiques*, I, t. 1, p. 1-9). Voir également E. LANDAU, *Grundlagen der Analysis* (Leipzig, 1930, p. 2); C. CHEVALLEY, *Encyclopédie Française*, t. I, p. 60-62; R. POIRIER, *Le nombre* (Paris, Alcan, 1938, p. 91 et 92).

Proposons-nous inversement d'établir que *tout ensemble p'eanien, P, convenablement ordonné, est un ensemble naturel*, ce qui établira l'équivalence des deux notions. Cette démonstration va d'ailleurs coïncider avec le début de la théorie des nombres entiers, faite à partir des axiomes de Peano.

Définissons d'abord, dans P, l'addition en introduisant la somme $x + y$ comme une fonction, définie et prenant ses valeurs dans P, et vérifiant les deux relations fonctionnelles :

$$\begin{aligned} (1) \quad & x + u = x', \\ (2) \quad & x + y' = (x + y)'. \end{aligned}$$

Il existe au plus une telle fonction $x + y$ vérifiant (1) et (2). Soient, en effet, $f(x, y)$, $g(x, y)$ deux fonctions vérifiant (1) et (2). Fixons x et considérons l'ensemble A des éléments y de P pour lesquels on a

$$(3) \quad f(x, y) = g(x, y).$$

D'après (1), u appartient à A; et si $y \in A$, il en est de même de y' d'après (2): donc $A = P$, les fonctions $f(x, y)$, $g(x, y)$ coïncident pour tout y , quel que soit x .

Montrons maintenant qu'il y a bien une fonction $x + y$ vérifiant (1) et (2), en la construisant par récurrence.

Posons

$$(3) \quad u + y = y'.$$

Nous avons bien :

$$\begin{aligned} (1') \quad & u + u = u', \\ (2') \quad & u + y' = (y')' = (u + y)'. \end{aligned}$$

Supposons que, pour x fixé dans P, $x + y$ existe quel que soit y , avec les propriétés (1) et (2). Considérons l'élément x' associé à x et posons

$$(4) \quad x' + y = (x + y)'.$$

Nous avons

$$\begin{aligned} (1'') \quad & x' + u = (x + u)' = (x')', \\ (2'') \quad & x' + y' = (x + y')' = [(x + y)']' = (x' + y)'. \end{aligned}$$

Les conditions (1) et (2) sont encore vérifiées : l'ensemble des éléments x pour lesquels on peut trouver une fonction de y vérifiant (1) et (2),

coïncide avec P. La fonction $x + y$, ainsi construite par récurrence, vérifie en outre les relations (3) et (4), et nous pouvons énoncer :

THÉORÈME 5. — *Il existe une seule fonction $x + y$, définie dans l'ensemble péanien P, prenant ses valeurs dans P, vérifiant les relations (1), (2), (3), (4).*

Cette fonction définit dans P une opération

$$(x, y) \rightarrow x + y$$

appelée *addition*, dont le résultat $x + y$ est la *somme* de x et y .

THÉORÈME 6. — *L'addition est : 1° associative; 2° commutative.*

1° Fixons x et y dans P et soit B l'ensemble des éléments z de P vérifiant l'égalité

$$(5) \quad (x + y) + z = x + (y + z).$$

Nous avons $u \in B$, car

$$(x + y) + u = (x + y)' = x + y' = x + (y + u).$$

Si $z \in B$, il en résulte, d'après (2) et (5) :

$$(x + y) + z' = [(x + y) + z]' = [x + (y + z)]' = x + (y + z)' = x + (y + z'),$$

c'est-à-dire $z' \in B$. Nous avons donc $B = P$, quels que soient x et y .

2° Fixons x dans P, et soit C l'ensemble des y vérifiant

$$(6) \quad x + y = y + x.$$

Nous avons $u \in C$ car, d'après (1), $x + u = x'$ et, d'après (3), $u + x = x'$. Si maintenant $y \in C$, il en résulte, d'après (2), (6) et (4) :

$$x + y' = (x + y)' = (y + x)' = y' + x,$$

c'est-à-dire $y' \in C$. Nous avons donc $C = P$ quel que soit x .

LEMME 1. — *On a $x + y \neq y$ quels que soient $x, y \in P$.*

Fixons x dans P, et soit D l'ensemble des y pour lesquels la propriété est vraie. Nous avons $u \in D$, puisque $x + u = x'$ est différent de u (axiome 3). D'autre part, $y \in D$ entraîne

$$x + y' = (x + y)' \neq y'$$

(axiome 4), donc $y' \in D$. Nous avons donc $D = P$, quel que soit x .

Remarque. — En prenant $x = u$, nous retrouvons la propriété établie plus haut

$$y' = u + y \neq y.$$

LEMME 2 (règle de simplification). — *L'égalité*

$$a + x = b + x \quad \text{entraîne} \quad a = b.$$

En supposant a et b fixés, considérons l'ensemble E des éléments x de P pour lesquels l'énoncé est vrai. Nous avons $u \in E$ (axiome 4); si $x \in E$, l'égalité $a + x' = b + x'$, équivalente à $(a + x)' = (b + x)'$, entraîne, d'après l'axiome 4, $a + x = b + x$, donc $a = b$: nous avons donc $x' \in E$, d'où $E = P$, quels que soient a et b .

On voit que P est un semi-groupe par rapport à l'addition.

THÉORÈME 7. — *Soient x et y deux éléments de P . On a toujours une et une seule des trois égalités*

$$\begin{aligned} (7) \quad & y = x, \\ (7') \quad & y = x + a \quad (a \in P), \\ (7'') \quad & y + b = x \quad (b \in P). \end{aligned}$$

Les égalités (7) et $(7')$ s'excluent l'une l'autre d'après le lemme 1; de même, (7) et $(7'')$; $(7')$ et $(7'')$, vérifiées simultanément, entraîneraient

$$x = y + b = (x + a) + b = x + (a + b)$$

également impossible. Nous avons donc *au plus* une des relations (7) , $(7')$ et $(7'')$.

Fixons x et désignons par F l'ensemble des éléments y de P pour lesquels on a effectivement *une* de ces relations. Nous avons $u \in F$, car si $x \neq u$, il existe, d'après l'axiome 4, un élément b tel que

$$x = b' = u + b.$$

Soit maintenant $y \in F$. Si $y = x$, on a

$$y' = x' = x + u, \quad \text{donc} \quad y' \in F;$$

si $y = x + a$, on a

$$y' = (x + a)' = x + a', \quad \text{donc} \quad y' \in F;$$

si enfin $x = y + b$, on a

$$x' = y' + b,$$

c'est-à-dire : 1° si $b = u$,

$$x' = (y')', \quad \text{donc} \quad x = y', \quad y' \in F;$$

2° si $b \neq u$, d'où $b = c'$,

$$x' = y' + c' = (y' + c)', \quad \text{donc } x = y' + c, \quad y' \in F.$$

La relation $y \in F$ entraîne donc dans tous les cas $y' \in F$, d'où $F = P$, quel que soit x .

Lorsque x est différent de y , posons $x < y$ (ou $y > x$) si et seulement si l'on a la relation (γ'); écrivons également, dans ce cas, $a = y - x$: a s'appelle *différence* de y et de x , et l'opération ainsi définie, non toujours possible, mais soumise au contraire à la condition $x < y$, est la *soustraction*. Nous laisserons de côté les propriétés de la soustraction, telles que

$$a - (b + c) = (a - b) - c,$$

pour insister sur la relation $x < y$ qui vient d'être définie.

Remarque. — On voit immédiatement, d'après la définition (γ'), et en tenant compte de l'associativité et de la commutativité de l'addition, que $x < y$ entraîne $p + x < p + y$ pour tout $p \in P$. La réciproque s'obtient en utilisant, en outre, la règle de simplification (lemme 2).

THÉOREME 8. — 1° La relation $x < y$ est une relation d'ordre total strict dans P ; 2° u est le premier élément de P , $x' = x + u$ est le suivant de x , $x' = x^+$; 3° P est bien ordonné.

1° Le théorème 7 impliquant déjà le second axiome des relations d'ordre total strict, il suffit d'établir la transitivité (¹). Or, $x < y$ et $y < z$, c'est-à-dire $y = x + a$ et $z = y + b$ entraînent

$$z = (x + a) + b = x + (a + b), \quad \text{donc } x < z.$$

2° Si s est différent de u , nous avons

$$s = r' = r + u > u.$$

On a $x < x + u = x'$. Soit, d'autre part, $x < y$, c'est-à-dire $y = x + a$. Nous avons $u \leq a$, donc

$$x' = x + u \leq x + a = y,$$

x' est donc bien le suivant de x dans l'ensemble P ordonné par $<$.

3° Soit A une partie non vide de P . Désignons par X l'ensemble des éléments x de P vérifiant la relation

$$x \leq a \quad \text{pour tout } a \in A.$$

(¹) Cf. chap. I, § 4, p. 18.

A n'étant pas vide, contient au moins un élément a , et a n'appartient pas à X , donc $X \neq P$. Cela posé, comme $u \in X$, il existe au moins un élément p de P tel que $p \in X$, $p' \notin X$ (puisque, dans le cas contraire, nous aurions $X = P$ d'après l'axiome 5). L'inégalité $p < a$ pour tout $a \in A$ entraînerait $p' \leq a$ pour tout $a \in A$, c'est-à-dire $p' \in X$, contrairement à la définition de p : l'élément p appartient donc à A et en est premier élément.

En résumé, on peut, dans tout ensemble péanien P , introduire une relation d'ordre total strict. Par rapport à cet ordre, qui sera appelé *ordre naturel*, P a les trois propriétés suivantes :

- I. P est bien ordonné (th. 8);
- II. Chaque élément, sauf le premier u , admet un précédent (axiome 4 et th. 8, 2°);
- III. P n'a pas de dernier élément (axiome 2 et th. 8).

L'ensemble P ainsi ordonné est donc un *ensemble naturel* : nous avons établi l'équivalence entre les deux notions d'ensemble naturel et d'ensemble péanien.

En particulier, la définition de l'addition dans les ensembles péaniens s'applique aux nombres naturels, pour lesquels les relations fondamentales (1) et (2) s'écrivent

$$\begin{aligned}x + 1 &= x^+, \\x + y^+ &= (x + y)^+.\end{aligned}$$

3. Compléments. — *a.* THÉORÈME 9. — Si deux parties disjointes P et Q d'un ensemble E sont finies non vides et ont respectivement p et q éléments, leur somme $P + Q$ a $p + q$ éléments.

Par hypothèse, P et Q (ordonnées de façons quelconques) sont semblables respectivement aux segments $[1, p]$ et $[1, q]$ de l'ensemble N des nombres naturels. Mais, d'après la remarque précédant le théorème 8, la loi

$$x \rightarrow p + x$$

applique biunivoquement et semblablement le segment $[1, q]$ sur le segment $[p + 1, p + q]$, donc Q est semblable à ce segment, qui est disjoint de $[1, p]$. En plaçant P avant Q , nous voyons que $P + Q$ est semblable à $[1, p] + [p + 1, p + q]$, c'est-à-dire au segment $[1, p + q]$ de N : nous retrouvons le fait que $P + Q$ est fini (cf. Note I, th. 15, p. 413) et nous voyons que le nombre de ses éléments est égal à $p + q$.

b. Il est souvent commode d'adjoindre formellement au semi-groupe additif N des nombres naturels un *élément neutre* ⁽¹⁾ appelé *zéro* et désigné par 0 , c'est-à-dire un élément vérifiant

$$x + 0 = 0 + x = 0 \quad \text{pour tout } x \in N, \quad \text{et pour } x = 0.$$

Cette convention n'altère ni l'associativité, ni la commutativité de l'addition, ni la règle de simplification. Désignons par N_0 le semi-groupe additif ainsi obtenu :

$$N_0 = N + \{0\}.$$

Nous avons

$$0 = x - x \quad \text{pour tout } x \in N_0$$

et, conformément à la définition de l'ordre naturel dans N , nous devons poser, dans N_0 ,

$$0 < x \quad \text{pour tout } x \in N,$$

ce qui fait de N_0 un ensemble ordonné, discret, sans dernier élément, donc un ensemble naturel dont 0 est le premier élément (l'application $x \rightarrow x + 1$ est d'ailleurs une application biunivoque semblable de N_0 sur N).

On peut considérer 0 comme le nombre d'éléments d'un ensemble vide, ce qui permet de ne pas exclure le cas des parties vides dans différents énoncés, tels que celui du théorème 9.

c. Le produit xy de deux nombres x, y peut se définir par un procédé analogue à celui qui a servi pour la somme : *x étant donné, il existe une seule fonction xy de y vérifiant les relations récurrentes* ⁽²⁾ :

$$(8) \quad x \cdot 1 = x,$$

$$(9) \quad x \cdot y^+ = xy + x \quad \text{ou} \quad x(y + 1) = xy + x.$$

On voit sans peine que la multiplication ainsi définie est commutative, distributive par rapport à l'addition et associative. Elle vérifie, dans N , la règle de simplification.

⁽¹⁾ Cf. chap. II, p. 77. B. Russel signale que le symbole 0 « est d'addition toute récente; les Grecs et les Romains n'avaient point ce chiffre » (*Introduction à la Philosophie Mathématique*, Paris, 1928, p. 13).

⁽²⁾ Démonstration analogue à celle du théorème 5 (cf. E. LANDAU, *Grundlagen der Analysis*, p. 14).

Pour définir le produit de zéro par un élément quelconque $x \in N_0$, on tient compte, *a priori*, de la distributivité :

$$ax = (a + 0)x = ax + 0x, \quad \text{d'où} \quad 0x = 0.$$

Zéro est, par conséquent, *élément permis* par rapport à la multiplication, et celle-ci ne vérifie plus, dans N_0 , la règle de simplification.

Mais on peut aussi rattacher la multiplication des nombres naturels à la notion d'*ensemble-produit* : si A et B sont deux ensembles finis, ayant respectivement a et b éléments, le produit $P = A \times B$ est fini (Note I, corollaire du théorème 15); le nombre p des éléments de P est, par définition, le produit ab de a par b . Si B est la somme de deux parties disjointes B_1, B_2 , on a

$$(10) \quad P = A \times (B_1 + B_2) = A \times B_1 + A \times B_2,$$

car chaque couple (α, β) , où $\alpha \in A, \beta \in B$ est de la forme (α, β_1) avec $\beta_1 \in B_1$ ou de la forme (α, β_2) , avec $\beta_2 \in B_2$, l'un de ces cas excluant l'autre; inversement, chaque couple ayant l'une de ces deux formes appartient à $A \times B$. La distributivité de la multiplication par rapport à l'addition résulte de (10) :

$$(10') \quad a(b_1 + b_2) = ab_1 + ab_2,$$

$A \times B$ et $B \times A$ ayant évidemment même puissance, on a $ab = ba$. De même, $(A \times B) \times C$ et $A \times (B \times C)$ ayant tous deux même puissance que l'ensemble des systèmes (α, β, γ) , où $\alpha \in A, \beta \in B, \gamma \in C$, on a $a(bc) = (ab)c$. On obtient ainsi les règles de calcul fondamentales.

Cette deuxième définition est équivalente à la première.

Si, en effet, $B = \{b\}$, $A \times B$ a même puissance que A : la condition (8) est vérifiée et (9) n'est qu'un cas particulier de (10').

Nous laisserons de côté la théorie de la *numération* qui permet de *nommer* (numération parlée) et d'*écrire* (numération écrite) les nombres naturels, et d'effectuer commodément les opérations fondamentales sur ces nombres (¹).

(¹) Voir, par exemple, J. TANNERY, *Leçons d'Arithmétique*, p. 18 à 32; *Encyclopédie des Sciences Mathématiques*, I, t. 1, p. 9 à 21; O. ORE, *Number Theory and its history* (Mc Graw-Hill Book Co, New-York, 1948).

NOTE III.

AXIOME DU CHOIX. THÉORÈME DE ZERMELO. THÉORÈME DE ZORN.

1. Nous démontrerons en premier lieu le

THÉORÈME DE ZERMELO. — *Moyennant l'axiome du choix, tout ensemble E peut être bien ordonné.*

Conformément à l'axiome du choix, nous pouvons distinguer dans chaque partie non vide A de E un élément $a \in A$. Nous dirons qu'un ensemble $\mathbf{k}$ de parties de E est une Θ -chaîne si $\mathbf{k}$ possède les propriétés suivantes :

1. $\mathbf{k}$ comprend l'ensemble E;
2. Si $\mathbf{k}$ comprend A, il comprend aussi l'ensemble $A' = A - \{a\}$ obtenu en retranchant de A l'élément a distingué dans A;
3. Étant donné un ensemble quelconque $\mathfrak{M}$ de parties A, B, ... appartenant à $\mathbf{k}$, $\mathbf{k}$ comprend l'intersection $\bigcap_{A \in \mathfrak{M}} A$.

Il existe bien de telles chaînes, puisque l'ensemble de toutes les parties de E en est une. D'autre part, l'intersection d'un ensemble quelconque de Θ -chaînes est encore une Θ -chaîne : en particulier, l'intersection de toutes les Θ -chaînes est une Θ -chaîne que nous désignerons par Δ . Tout véritable sous-ensemble de Δ n'est plus une Θ -chaîne : Δ est minimale.

Il existe dans Δ des parties A de E telles que toutes les autres parties appartenant à Δ contiennent A ou en sont sous-ensembles : l'ensemble $E (\in \Delta)$ possède en effet lui-même cette propriété P. A étant une telle partie, désignons par O_A les véritables sur-ensembles de A appartenant à Δ , par U_A les véritables sous-ensembles de A appartenant également

à Δ . Désignons enfin par V_A tout U_A qui est sous-ensemble (véritable ou non) de $A' = A - \{a\}$.

A étant fixé (avec la propriété précédente P), les parties O_A et V_A correspondantes forment, avec A lui-même, un ensemble de parties, $\mathfrak{h}$, qui est une Θ -chaîne. En effet :

1° E est un O_A ou coïncide avec A , donc $E \in \mathfrak{h}$.

2° Considérons $(O_A)' = O_A - \{\alpha\}$ α étant l'élément distingué dans O_A . Si α n'appartient pas à A , $(O_A)'$ est encore sur-ensemble de A . Et comme $(O_A)'$ appartient à Δ , c'est soit un O_A , soit A lui-même. Si, au contraire, α appartenait à A , $(O_A)'$ serait, non plus sur-ensemble, mais véritable sous-ensemble de A , puisqu'il appartient à Δ , et que toute partie appartenant à Δ est sur-ensemble ou sous-ensemble de A . Mais O_A , véritable sur-ensemble de A , contient au moins un élément α_1 non contenu dans A (et, par suite, différent de α), donc *a fortiori* non contenu dans $(O_A)'$: il y aurait donc deux éléments distincts, α et α_1 , de O_A n'appartenant pas à $(O_A)'$, ce qui est contraire à la définition de $(O_A)'$: le dernier cas ne peut donc pas se présenter et nous avons $(O_A)' \in \mathfrak{h}$.

D'autre part, A' et les $(V_A)'$ appartiennent à Δ et sont sous-ensembles de A' , donc sont des V_A et appartiennent à $\mathfrak{h}$.

3° Enfin l'intersection I de plusieurs parties appartenant à $\mathfrak{h}$ est encore un ensemble de $\mathfrak{h}$. Si, en effet, aucun V_A ne figure parmi ces parties, l'intersection en question, qui appartient à Δ , est sur-ensemble de A , donc est un O_A ou A lui-même. Si parmi ces ensembles figure au moins un V_A , l'intersection I , qui appartient à Δ , est sous-ensemble de A' , donc est un V_A : dans tous les cas $I \in \mathfrak{h}$.

$\mathfrak{h}$ étant une Θ -chaîne contenue dans Δ , qui est minimale, coïncide nécessairement avec Δ : celle-ci se compose donc uniquement des O_A , de A et des V_A , et tout U_A est nécessairement un V_A : *A' possède donc, en même temps que A , la propriété P : tout ensemble de Δ est sur-ensemble ou sous-ensemble de A' .*

Si plusieurs ensembles $A, B, \dots$ possèdent la propriété P , il en est de même de leur intersection I . Si, en effet, X est un ensemble quelconque de Δ , ou bien il contient un des ensembles $A, B, \dots$ et, par suite, aussi leur intersection I , ou bien il est contenu dans tous les ensembles $A, B, \dots$, donc aussi dans leur intersection I .

Nous voyons donc que les ensembles de Δ qui possèdent la propriété P forment une Θ -chaîne ; celle-ci coïncidant nécessairement avec Δ , tous les ensembles de Δ possèdent la propriété P : *A et B étant deux parties*

de E appartenant à Δ , l'une est nécessairement contenue dans l'autre, $A \subseteq B$ ou $B \subseteq A$.

Soit alors M un sous-ensemble non vide quelconque de E , et M_0 l'intersection des parties de E appartenant à Δ , qui contiennent M comme sous-ensemble (E est une telle partie) : $M_0 \in \Delta$ et $M_0 \supseteq M$. L'élément m_0 distingué dans M_0 est contenu dans M , car autrement $(M_0)'$ contiendrait encore M comme sous-ensemble. Or, $(M_0)'$ appartient à Δ et est véritable sous-ensemble de M_0 .

Si M_1 est une autre partie appartenant à Δ et contenant M , M_0 est véritable sous-ensemble de M_1 , donc, d'après ce qui a été démontré plus haut (tout U_λ est un V_λ), sous-ensemble de $(M_1)'$. Par suite, l'élément m_1 distingué dans M_1 n'appartient pas à M_0 ni à plus forte raison à M . Il n'y a donc dans Δ qu'un ensemble M_0 qui contienne M et dont l'élément distingué m_0 appartienne à M .

En particulier, supposons que M se compose d'un seul élément x : il existe un seul ensemble de Δ contenant x et dont x soit l'élément distingué, désignons-le par $R(x)$. Si $x \neq y$, $R(x)$ et $R(y)$ sont eux-mêmes différents et l'on a, soit $R(x) \subset R(y)$, soit $R(y) \subset R(x)$. Nous poserons dans le premier cas $y < x$, dans le second $x < y$. La relation ainsi définie par le signe $<$ est visiblement une relation d'ordre et E est un ensemble ordonné.

Si enfin M est une partie non vide de E , un élément quelconque m de M est contenu dans l'ensemble $M_0 = R(m_0)$. L'ensemble $R(m) \in \Delta$, qui est par définition l'intersection des ensembles de Δ qui contiennent m , est contenu dans $R(m_0)$: on a par conséquent

$$m_0 \leq m.$$

C'est dire que M admet le premier élément m_0 et que, par suite, E est bien ordonné.

C. Q. F. D.

2. Comme nous l'avons vu (chap. I, § 10, p. 44), tout ensemble bien ordonné E vérifie l'axiome du choix, puisqu'on peut associer à chaque partie non vide X de E son premier élément : vérifier l'axiome du choix et être (ou pouvoir être) bien ordonné, sont donc, pour un ensemble, des propriétés équivalentes, que nous noterons respectivement (C) et (B. O.) :

$$(C) \Leftrightarrow (B. O.).$$

Nous allons voir que ces propriétés sont liées encore à d'autres condi-

tions remarquables; la première, considérée par Hausdorff⁽¹⁾, s'énonce : dans l'ensemble E (non vide), pourvu d'un ordre partiel O , toute chaîne C est contenue dans une chaîne maximale. Cette propriété (H) entraîne l'existence d'au moins une chaîne maximale (H'), puisque l'ensemble $\{x\}$ formé par un élément x de E est une chaîne C .

L'équivalence de l'énoncé (H) avec (C) et (B. O.) résultera des deux théorèmes suivants :

THEOREME 1. — Soit C une chaîne dans un ensemble E partiellement ordonné par O . S'il existe dans E un bon ordre Ω , C est contenue dans une chaîne maximale M (par rapport à l'ordre O) :

$$(B. O.) \Rightarrow (H).$$

Dans l'ensemble $\Delta = E - C$, bien ordonné par la trace Ω_Δ du bon ordre Ω , définissons par induction transfinie une fonction (uniforme) f prenant ses valeurs dans $\{0, 1\}$. Nous poserons $f(x) = 0$ si l'élément x de Δ est comparable, dans l'ordre O , à chaque élément de C et à chacun des éléments m de Δ qui précèdent x dans l'ordre Ω et vérifient $f(m) = 0$. Dans le cas contraire, nous poserons $f(x) = 1$.

Soit C' l'ensemble des éléments x de Δ pour lesquels $f(x) = 0$. L'ensemble $M = C + C'$ est, par construction, une chaîne (dans l'ordre O); M contient C ; montrons que M est maximale. Supposons qu'il existe une chaîne M' contenant strictement M : si $r \in M' - M$, nous avons $r \in \Delta$ et $f(r) = 1$; d'autre part, r est comparable, dans l'ordre O à tous les éléments de C , et à tous ceux de C' donc en particulier aux éléments de Δ qui précèdent r dans l'ordre Ω et pour lesquels f est nulle; cela entraîne $f(r) = 0$, et il y a contradiction : M est bien maximale.

E étant un ensemble quelconque, considérons les fonctions g suivantes : $g(P)$ est défini pour certaines parties P , non vides, de E , et est un élément de P :

$$g(P) \in P.$$

Par exemple, la loi qui associe à toute partie $\{x\}$ comprenant un seul élément, cet élément x , est une fonction g . Dans l'ensemble Γ de ces fonctions g , posons $g_1 \leq g_2$ si $g_2(P)$ existe et est égal à $g_1(P)$ pour toute partie P telle que $g_1(P)$ existe : nous définissons ainsi dans Γ une relation d'ordre partiel $\leq$.

(1) *Grundzüge der Mengenlehre*, 1^{re} éd., p. 140.

THÉORÈME 2. — Si l'ensemble partiellement ordonné Γ ainsi défini contient une chaîne maximale $\mathcal{M}$, E vérifie l'axiome du choix :

$$(H')_{\text{dans } \Gamma} \Rightarrow (G)_{\text{dans } E}.$$

Soit $\mathcal{X}$ l'ensemble des parties X , non vides, de E ayant la propriété suivante : il existe au moins une fonction g appartenant à la chaîne maximale $\mathcal{M}$ telle que $g(X)$ soit défini ⁽¹⁾. Si une partie non vide Y n'appartenait pas à $\mathcal{X}$, en posant

$$\gamma(X) = g(X)$$

pour $X \in \mathcal{X}$ et $g \in \mathcal{M}$ telle que $g(X)$ existe,

$$\gamma(Y) = y,$$

où y désigne un élément quelconque de Y , nous définirions une fonction γ supérieure strictement à toute fonction g de $\mathcal{M}$, ce qui est impossible puisque $\mathcal{M}$ est maximale.

$\mathcal{X}$ est donc l'ensemble de toutes les parties non vides de E . La fonction $\varphi(X)$ définie par

$$\varphi(X) = g(X) \in X$$

pour $X \in \mathcal{X}$ et g telle que $g(X)$ existe, associe à toute partie non vide de E un élément de cette partie, ce qui démontre le théorème.

3. Rappelons qu'un ensemble inductif est un ensemble partiellement ordonné E tel que toute chaîne C extraite de E possède une borne supérieure s ($s \in E$); rappelons aussi que le principe de l'élément maximal ou théorème de Zorn (Z) s'énonce : dans un ensemble inductif, il existe un élément maximal.

THÉORÈME 3. — Si un ensemble inductif E contient une chaîne maximale M , il existe dans E un élément maximal :

$$(H) \Rightarrow (Z), \quad \text{donc} \quad (C) \Rightarrow (Z).$$

M a, en effet, une borne supérieure s ; puisque M est maximale, $s \in M$ et il ne peut y avoir dans E aucun élément $x > s$: s est bien, dans E , élément maximal.

Remarque. — Si E est un ensemble inductif, l'ensemble E_0 des éléments de E qui sont supérieurs ou égaux à un élément fixe x_0 , est visiblement aussi un ensemble inductif; le théorème de Zorn peut donc encore s'énoncer :

⁽¹⁾ $g(X)$ est alors le même pour toutes les fonctions g de la chaîne $\mathcal{M}$ qui répondent à la question, d'après la définition de la relation d'ordre partiel $\leq$ dans Γ .

(Z'). Dans un ensemble inductif E , il existe un élément maximal contenant un élément donné x_0 .

Une propriété $\mathcal{P}$, portant sur des ensembles, est appelé *propriété de caractère fini* si, pour que $\mathcal{P}$ soit vraie pour un ensemble X , il faut et il suffit qu'elle le soit pour toute partie finie de X . Par exemple, pour les parties x d'un ensemble partiellement ordonné E , être une chaîne est une propriété de caractère fini : X est, en effet, une chaîne si et seulement si toute partie de X formée de deux éléments $\{x_1, x_2\}$ en est une, et cela entraîne que toute partie (finie ou non) de X est une chaîne.

Nous dirons qu'un ensemble E vérifie la *condition de Tukey* (T) si, Π étant une propriété de caractère fini concernant les parties de E , il existe une partie maximale M possédant la propriété Π (c'est-à-dire une partie M ayant cette propriété et qui n'est contenue strictement dans aucune partie l'ayant aussi).

THÉOREME 4. — L'ensemble $\mathcal{A}$ des parties de E qui possèdent une propriété Π de caractère fini, est inductif (on prend comme relation d'ordre partiel dans l'ensemble $\mathcal{P}(E)$ des parties de E la relation d'inclusion $\subseteq$).

Soit $\mathcal{C}$ une chaîne de parties, extraite de $\mathcal{A}$. Dans $\mathcal{P}(E)$, $\mathcal{C}$ admet la borne supérieure $R = \bigcup_{x \in \mathcal{C}} x$: montrons que $R \in \mathcal{A}$, et pour cela,

puisque Π est de caractère fini, que toute partie finie $R_0 = \{x_1, \dots, x_n\}$ de R a la propriété Π . Chaque élément x_i appartient à une partie $X_i \in \mathcal{C}$; or, l'un des X_i , X_α , contient tous les autres puisque $\mathcal{C}$ est une chaîne. Mais alors, R_0 , partie finie de $X_\alpha \in \mathcal{A}$, possède aussi la propriété Π , ce qu'il fallait démontrer.

Cela posé, il est clair que, si l'ensemble inductif $\mathcal{A}$ des parties de E qui ont la propriété Π contient un élément maximal M (en d'autres termes, si l'on admet le principe de Zorn pour $\mathcal{A}$), l'ensemble E vérifie la condition de Tukey :

$$(Z)_{\text{dans } \mathcal{A}} \Rightarrow (T)_{\text{dans } E}.$$

Il est clair enfin, puisque être une chaîne est une propriété de caractère fini, que la condition de Tukey entraîne celle de Hausdorff

$$(T) \Rightarrow (H).$$

En résumé, nous avons établi, entre les propriétés ou axiomes (C),

(BO), (H), (Z), (T) les implications représentées par le tableau suivant : deux symboles sont reliés par une *flèche en trait plein* si la propriété P_2 représentée par le second et relative à un certain ensemble E , résulte de la propriété P_1 représentée par le premier, relative au *même* ensemble ; par une *flèche en trait interrompu* si P_2 , pour E , résulte de P_1 supposée vraie pour un ensemble E' dépendant d'une façon simple de E , mais *distinct* de E [par exemple, $E' = \mathfrak{X}(E)$].

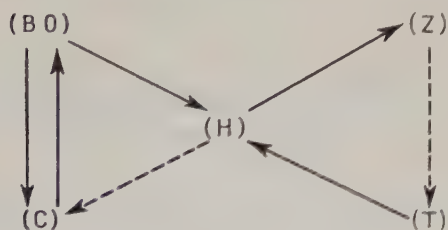


Fig. 9.

L'existence de flèches en traits interrompus dans ce tableau, exprime la nécessité de passer dans certains cas d'un ensemble à un autre ; cela explique pourquoi on préfère souvent adopter une fois pour toutes, par raison de simplicité, le postulat de Zermelo (« *Tout ensemble vérifie l'axiome du choix* ») ou le théorème de Zorn, considéré lui aussi comme postulat *général* de la Théorie des Ensembles.

Remarque. — Comme le propose N. Bourbaki ⁽¹⁾, on peut aussi établir le théorème de Zorn pour un ensemble inductif E , au moyen du lemme suivant :

LEMME. — Soient E un ensemble inductif et f une application de E dans E telle que l'on ait

$$x \subseteq f(x) \quad \text{pour tout } x \in E.$$

1° Il existe des parties X de E telles que : a. $x \in X$ entraîne $f(x) \in X$; b. Si Y est une chaîne contenue dans X , sa borne supérieure (dans E) appartient à X . Parmi ces parties X , il y en a une, Λ , qui est contenue dans toutes les autres.

⁽¹⁾ *Théorie des Ensembles* (Fascicule de résultats, *Act. scient. et ind.*, n° 846, Hermann, Paris, 1939). Dans le texte, l'énoncé du lemme ne comporte pas la première partie ; celle-ci, qui facilite la démonstration de la deuxième, m'a été aimablement communiquée par N. Bourbaki.

2° Dans cette partie Λ , il existe un élément a vérifiant l'égalité

$$a = f(a).$$

La démonstration de ce lemme ne repose pas sur l'axiome du choix, qui intervient seulement dans le passage du lemme au théorème de Zorn.



NOTE IV.

ESPACES.

1. Nous rappellerons brièvement, dans cette Note, les définitions des principaux types d'espaces que nous avons eu ou aurons l'occasion d'utiliser.

L'espace le plus simple est la *droite*, telle qu'on la considère en géométrie élémentaire, d'une façon plus précise la *droite euclidienne*. La définition la plus simple qu'on puisse en donner consiste à l'identifier avec l'ensemble **P** des nombres réels. La distance de deux points a , b de la droite est le nombre positif ou nul $|a - b|$.

On donne le nom de *plan euclidien* à l'ensemble des couples (x_1, x_2) de deux nombres réels, ces couples étant par définition les *points* du plan euclidien. De même, l'espace euclidien E_r de dimension r (ou à r dimensions) est, par définition, l'ensemble des systèmes

$$x = (x_1, x_2, \dots, x_r)$$

de r nombres réels; chacun de ces systèmes est un *point* de E_r dont les nombres x_i sont les coordonnées. Deux points de E_r coïncident si et seulement si leurs coordonnées de même indice sont égales.

Dans un espace euclidien E_r , les différents êtres géométriques sont définis à partir des points, par leurs équations ou par leur expression analytique. Par exemple, la droite joignant deux points distincts x , y de E_r est l'ensemble des points m dont les coordonnées sont de la forme

$$m_i = \frac{\lambda x_i + \mu y_i}{\lambda + \mu} \quad (i = 1, 2, \dots, r),$$

où λ et μ décrivent l'ensemble des nombres réels ($\lambda + \mu \neq 0$).

La *distance* d_{xy} de deux points x , y de E est, par définition, le nombre réel positif ou nul

$$d_{xy} = \sqrt{(x_1 - y_1)^2 + (x_2 - y_2)^2 + \dots + (x_r - y_r)^2}.$$

La définition précédente fait de tout espace euclidien un *espace métrique* ⁽¹⁾, c'est-à-dire un ensemble d'éléments, appelés points, tel qu'à tout couple de points x, y corresponde un nombre réel positif ou nul d_{xy} , appelé distance de ces points et possédant les propriétés suivantes, connues sous le nom d'*axiomes de la distance* :

1° *Axiome de coïncidence.* — On a

$$d_{xy} = 0$$

si et seulement si les points x et y coïncident.

2° *Axiome de symétrie.* — On a

$$d_{xy} = d_{yx}$$

quels que soient x et y .

3° *Axiome du triangle.* — Quels que soient les trois points x, y, z , on a

$$d_{xz} \leq d_{xy} + d_{yz}.$$

Les deux premiers axiomes sont évidemment satisfaits par la distance telle qu'elle a été définie dans l'espace euclidien E_r . Si nous posons

$$x_i - y_i = \xi_i, \quad y_i - z_i = \eta_i,$$

la vérification du troisième axiome revient à établir l'inégalité

$$\sqrt{\sum_{i=1}^r (\xi_i + \eta_i)^2} \leq \sqrt{\sum_{i=1}^r \xi_i^2} + \sqrt{\sum_{i=1}^r \eta_i^2},$$

équivalente elle-même à l'*inégalité de Schwarz*

$$\sum_{i=1}^r \xi_i \eta_i \leq \sqrt{\sum_{i=1}^r \xi_i^2} \sqrt{\sum_{i=1}^r \eta_i^2}.$$

Celle-ci est évidente si le premier membre est négatif ou nul. S'il est au contraire positif, on obtient une inégalité équivalente en élevant au carré. Or, la forme quadratique en u et v

$$\sum_{i=1}^r (u\xi_i + v\eta_i)^2 = u^2 \sum_{i=1}^r \xi_i^2 + 2uv \sum_{i=1}^r \xi_i \eta_i + v^2 \sum_{i=1}^r \eta_i^2$$

(1) Cette notion a été introduite par M. FRÉCHET, *Sur quelques points du Calcul fonctionnel* (Rend. Cir. mat. Palermo, t. 22, 1906, p. 17). Voir aussi le livre du même Auteur, *Les Espaces abstraits* (Paris, Gauthier-Villars, 1928, p. 61-62).

étant définie positive, c'est-à-dire positive ou nulle quelles que soient les valeurs réelles attribuées à u et v , on a

$$\left(\sum_{i=1}^r \xi_i^2 \right) \cdot \left(\sum_{i=1}^r \eta_i^2 \right) - \left(\sum_{i=1}^r \xi_i \eta_i \right)^2 \geq 0,$$

et, par conséquent, l'inégalité de Schwarz est établie ⁽¹⁾.

2. Une suite de points $\{x^{(n)}\}$ dans un espace euclidien ou dans un espace métrique est convergente et admet pour limite le point x si la suite des nombres $d_{x, x^{(n)}}$ tend vers zéro dans le corps $\mathbf{P}$ des nombres réels. De même, une suite de points $x^{(n)}$ est fondamentale s'il existe, pour tout nombre réel positif ε un entier naturel N tel que l'on ait.

$$(1) \quad d_{x^{(p)}, x^{(q)}} < \varepsilon \quad \text{dès que } p > N, \quad q > N.$$

Un espace métrique dans lequel toute suite fondamentale est convergente est dit *complet*. *Tout espace euclidien est complet*. Pour $r = 1$, cette proposition constitue le théorème de Cauchy (chap. V, § 9, p. 300). Pour r quelconque, soit $x^{(n)}$ une suite de points fondamentale, avec

$$x^{(n)} = (x_1^{(n)}, x_2^{(n)}, \dots, x_r^{(n)}).$$

L'inégalité (1) entraîne

$$|x_i^{(p)} - x_i^{(q)}| < \varepsilon \quad \text{dès que } p > N, \quad q > N.$$

Les coordonnées x_i forment donc, pour chaque valeur de l'indice i , une suite fondamentale, qui converge dans $\mathbf{P}$ vers une certaine limite ξ_i , et la suite $x^{(n)}$ tend vers le point

$$\xi = (\xi_1, \xi_2, \dots, \xi_r).$$

Si un espace métrique $\mathcal{E}$ n'est pas complet, on peut le compléter, c'est-à-dire définir un espace métrique complet $\mathcal{E}'$ contenant $\mathcal{E}$, par un

⁽¹⁾ Il existe bien d'autres espaces métriques que les espaces euclidiens, notamment l'espace de Hilbert (voir, par exemple, HAUSDORFF, *Grundzüge der Mengenlehre*, chap. VIII, § 5). Deux autres exemples simples sont fournis par l'ensemble E des fonctions continues $x(t)$ d'une variable réelle t dans l'intervalle fermé $(0, 1)$: la distance dans E peut être définie, soit par

$$d_{xy} = \text{Max } |x(t) - y(t)|,$$

soit par

$$\delta_{xy} = \sqrt{\int_0^1 [x(t) - y(t)]^2 dt}.$$

procédé tout à fait analogue à celui que nous avons utilisé pour définir le corps des nombres réels à partir du corps des nombres rationnels (qui est un exemple très simple d'espace métrique incomplet).

Il importe de remarquer que la convergence et les notions qui s'y rattachent peuvent être définies dans des espaces plus généraux que les espaces métriques. Dans les espaces métriques eux-mêmes, il est commode d'introduire un langage géométrique en appelant, par exemple, *voisinages sphériques* d'un point a , les ensembles de points x de l'espace vérifiant une inégalité de la forme

$$d_{xa} < \varepsilon,$$

où ε est un nombre réel positif donné. En axiomatisant la notion de voisinage, Hausdorff a défini une catégorie d'espaces, qui porte son nom, comprend comme cas particulier celle des espaces métriques, et se prête particulièrement bien à l'étude de la convergence. Un tel *espace de Hausdorff* est un ensemble $E = \{a, b, \dots\}$ d'éléments ou *points* vérifiant les conditions suivantes (axiomes des voisinages) :

1° A chaque point a de E sont associés des sous-ensembles V_a de E appelés *voisinages* de a et tels que a appartienne à chacun de ses voisinages : $a \in V_a$;

2° Si V'_a, V''_a sont deux voisinages de a , il existe un voisinage V_a du même point contenu dans l'intersection $V'_a \cap V''_a$;

3° Si un point b appartient à V_a , il existe un voisinage V_b de b contenu dans V_a ;

4° Si a et b sont deux points distincts, il existe un voisinage V_a du premier et un voisinage V_b du second qui n'ont aucun point commun.

On constate sans peine que ces axiomes sont vérifiés par les voisinages sphériques d'un espace métrique : tout espace métrique, en particulier tout espace euclidien, est donc un espace de Hausdorff.

A leur tour, les espaces de Hausdorff rentrent dans une catégorie plus générale, celle des *espaces topologiques*. Un tel espace E peut être défini par les trois premiers axiomes de Hausdorff. Deux familles de voisinages V_a, W_a définissent la même *topologie*, ou sont *équivalentes*, si chaque V_a contient un W_a et inversement.

Soit A une partie de E . Un point x de E est dit *point intérieur* de A s'il possède un voisinage V_x contenu dans A (cette propriété et celles que nous considérons ensuite subsistent si l'on remplace les voisinages V par une famille équivalente de voisinages W). Un point intérieur x

de A appartient à A . Un ensemble C ($\subseteq E$) dont tout point est intérieur est dit *ouvert*. On vérifie aisément les propriétés suivantes :

- I. L'espace E est ouvert; l'ensemble vide $\varnothing$ est ouvert;
- II. Toute réunion d'ensembles ouverts est un ensemble ouvert;
- III. L'intersection d'un nombre fini d'ensembles ouverts est un ensemble ouvert.

Ces trois propriétés remarquablement simples des ensembles ouverts fournissent une deuxième définition des espaces topologiques : un espace topologique E est un ensemble dans lequel on a distingué une famille Ω de parties $G, \dots$ appelées *ensembles ouverts* et vérifiant les axiomes I, II, III ci-dessus. La considération d'une *base* $\mathcal{B}$, c'est-à-dire d'une sous-famille de Ω telle que tout ensemble $G \in \Omega$ soit une réunion d'ensembles $B \in \mathcal{B}$ permet de constater que tout espace topologique au sens de la deuxième définition est un espace topologique au sens de la première ⁽¹⁾.

Appelons *ensemble fermé* F dans un espace topologique E tout complément d'ensemble ouvert : $F = E - G$. Les ensembles fermés ont les propriétés suivantes :

- I. E et $\varnothing$ sont fermés;
- II. Toute intersection d'ensembles fermés est fermée;
- III. La réunion d'un nombre fini d'ensembles fermés est un ensemble fermé.

Il est clair que ces trois propriétés fournissent aussi une définition des espaces topologiques, duale de la définition par les ensembles ouverts.

A toute partie A d'un espace topologique E , associons l'intersection $\bar{A}$ de tous les ensembles fermés contenant A ; $\bar{A}$ est le plus petit ensemble fermé contenant A (*fermeture* ou *adhérence* de A). L'application

$$(\gamma) \quad A \rightarrow \bar{A}$$

(1) Pour qu'une famille $\mathcal{B}$ de parties de E , considérée *a priori*, puisse être la base d'une topologie, c'est-à-dire pour que les réunions G d'ensembles $B \in \mathcal{B}$ vérifient les axiomes I, II, III des ensembles ouverts, il faut et il suffit que :

α . E soit une réunion d'ensembles B ;

β . l'intersection de deux ensembles B soit une réunion d'ensembles B .

$\mathcal{B}$ vérifiant les conditions α et β , si l'on appelle voisinages V_α de α ($\alpha \in E$) les ensembles $B \in \mathcal{B}$ auxquels α appartient, on obtient un système de voisinages pour lequel les ouverts sont précisément les ensembles G réunions de B .

possède les propriétés suivantes : on a $A \subseteq \bar{A}$, avec l'égalité si A est fermé, et seulement dans ce cas; $\bar{A}$ étant fermé, on a $\bar{\bar{A}} = \bar{A}$; $\bar{\emptyset} = \emptyset$; $X \subseteq Y$ entraîne $\bar{X} \subseteq \bar{Y}$ (isotonie); on a même $\overline{A \cup B} = \bar{A} \cup \bar{B}$, car, en raison de l'isotonie, on a $A \cup B \subseteq \bar{A} \cup \bar{B}$, d'où, puisque le second membre est fermé, $\overline{A \cup B} \subseteq \bar{A} \cup \bar{B}$; mais l'isotonie entraîne aussi $\bar{A} \subseteq \overline{A \cup B}$, $\bar{B} \subseteq \overline{A \cup B}$ donc $\bar{A} \cup \bar{B} \subseteq \overline{A \cup B}$, d'où l'égalité.

L'application (φ) , appelée fermeture topologique, est en particulier, d'après ce qui précède, une fermeture de Moore (chap. I, § 11), mais elle représente une notion plus forte.

Si l'on considère inversement dans un ensemble E une application

$$(\varphi) \quad A \rightarrow \bar{A}$$

telle que

$$\begin{aligned} A &\subseteq \bar{A}, \\ \bar{\bar{A}} &= \bar{A}, \\ \bar{\emptyset} &= \emptyset, \\ \overline{A \cup B} &= \bar{A} \cup \bar{B}, \end{aligned}$$

la famille Φ des parties F de E telles que $\bar{\bar{F}} = F$ possède les propriétés I, II, III : E est un espace topologique.

3. En remplaçant dans la définition d'un espace euclidien E_r les nombres réels par les nombres complexes, on obtient l'espace cartésien C_r , ensemble des systèmes de r nombres complexes ⁽¹⁾

$$x = (x_1, x_2, \dots, x_r).$$

Le passage aux coordonnées homogènes conduit à l'espace projectif P_r , dans lequel un point est l'ensemble de tous les systèmes de $r+1$ nombres complexes de la forme

$$X = (\lambda x_0, \lambda x_1, \dots, \lambda x_r),$$

où les x_i sont donnés, non tous nuls, et où λ est un nombre complexe arbitraire non nul : les points de P_r et les rayons de C_{r+1} , c'est-à-dire les droites issues de l'origine, se correspondent biunivoquement.

(1) Plus généralement, on pourra supposer que les coordonnées x_i sont prises dans un corps ou un anneau quelconque A . On obtient ainsi des espaces dont la considération est souvent utile en Algèbre [voir plus haut, p. 340; on pourra consulter, à ce sujet, François CHÂTELET, *Essais de Géométrie Galoisienne (Travaux et Mémoires de l'Université de Lille, 1944-1945)*].

NOTE V.

CORRESPONDANCES BIUNIVOQUES.

1. Nous nous proposons de rappeler ici brièvement quelques résultats importants sur les correspondances biunivoques. Indiquons d'abord certains théorèmes concernant les ensembles les plus fondamentaux.

THÉORÈME 1. — *Le corps Γ des nombres rationnels est dénombrable.*

Ordonnons, en effet, l'ensemble des fractions irréductibles $\frac{p}{q}$ en posant $\frac{p}{q} < \frac{p'}{q'}$ si $|p| + q < |p'| + q'$ ou si $|p| + q = |p'| + q'$ et $p < p'$. Cet ensemble se met alors sous la forme d'une suite infinie

$$\begin{aligned} & -\frac{1}{1}, \frac{1}{1}; \quad -\frac{2}{1}, -\frac{1}{2}, \frac{1}{2}, \frac{2}{1}; \\ & -\frac{3}{1}, -\frac{1}{3}, \frac{1}{3}, \frac{3}{1}; \quad -\frac{4}{1}, -\frac{3}{2}, \dots, \end{aligned}$$

ce qui démontre la proposition.

THÉORÈME 2. — *Le corps Λ des nombres algébriques est dénombrable.*

Tout nombre algébrique est racine d'une équation irréductible

$$(E) \quad \alpha_0 x^n + \alpha_1 x^{n-1} + \dots + \alpha_n = 0,$$

où les α_i sont des entiers relatifs premiers entre eux dans leur ensemble, avec $\alpha_0 > 0$. On peut ordonner les n racines $\xi, \dots$ d'une même équation E en posant $\xi < \xi'$ si $|\xi| < |\xi'|$ ou si $|\xi| = |\xi'|$ avec $\arg \xi < \arg \xi'$ (chaque argument étant supérieur ou égal à zéro et inférieur à 2π).

Montrons que l'ensemble des équations E, ... peut être ordonné de façon à former une suite illimitée. Appelons *rang* de E l'entier

$$r = n + \alpha_0 + |\alpha_1| + \dots + |\alpha_n|.$$

Il n'y a qu'un nombre fini d'équations E d'un rang donné. Nous poserons $E < E'$ si $r < r'$ ou si $r = r'$, $n < n'$, ..., ou si $r = r'$, $n = n'$, ..., $a_{i-1} = a'_{i-1}$, $a_i < a'_i$, ..., ce qui établit la proposition.

Les démonstrations des deux théorèmes précédents peuvent être rattachées au *procédé diagonal* de Cantor, qui permet de ranger en une seule suite les éléments d'une infinité dénombrable de suites illimitées $A^1, \dots, A^k, \dots$. Ces suites étant écrites les unes sous les autres

$$\begin{array}{ccccccc} A^1 & a_1^1 & a_2^1 & a_3^1 & \dots & a_n^1 & \dots \\ & \nearrow & & \nearrow & & & \\ A^2 & a_1^2 & a_2^2 & a_3^2 & \dots & a_n^2 & \dots \\ & \nearrow & & \nearrow & & & \\ A^3 & a_1^3 & a_2^3 & a_3^3 & \dots & a_n^3 & \dots \\ & \dots\dots\dots & & & & & \end{array}$$

on lit les éléments du tableau ainsi constitué, parallèlement aux diagonales indiquées, en prenant les termes sur chaque diagonale de la gauche vers la droite; on obtient ainsi la suite

$$a_1^1; a_1^2, a_2^1; a_1^3, a_2^2, a_3^1; \dots,$$

De l'application de ce procédé résulte immédiatement la proposition suivante :

THÉOREME 3. — *La réunion d'une infinité dénombrable (ou d'un nombre fini) de parties dénombrables d'un même ensemble, est dénombrable.*

THÉOREME 4. — *L'ensemble X des nombres réels x vérifiant la double inégalité*

$$0 \leq x < 1$$

n'est pas dénombrable.

Définissons chaque nombre x par son développement décimal

$$x = 0, a_1 a_2 \dots a_n \dots$$

Afin d'éviter qu'un même nombre admette deux développements différents ($0,2999\dots = 0,30000\dots$), nous excluons les développements décimaux dont tous les chiffres à partir d'un certain rang sont des 9.

Supposons l'ensemble X dénombrable

$$X = \{x_1, \dots, x_n, \dots\}$$

et désignons par a_n^k le $k^{\text{ième}}$ chiffre dans le développement de x_n .

Posons

$$\alpha_n = \alpha_n^n + 1 \quad \text{si} \quad \alpha_n^n = 0, 1, 2, 3, 4;$$

$$\alpha_n = \alpha_n^n - 1 \quad \text{si} \quad \alpha_n^n = 5, 6, 7, 8, 9.$$

Nous avons dans tous les cas $\alpha_n \neq \alpha_n^n$ et, par suite, le nombre réel

$$\xi = 0, \alpha_1 \alpha_2 \dots \alpha_n \dots$$

diffère de x_n quel que soit n , ce qui est absurde ⁽¹⁾.

On dit que l'ensemble X a la *puissance du continu*. Les ensembles X' et X'' des nombres réels appartenant à l'*intervalle ouvert* $0 < x < 1$ ou au *segment* $0 \leq x \leq 1$, ont même puissance que X , car les ensembles des nombres rationnels de X , X' , X'' ayant même puissance, on peut, en faisant se correspondre à lui-même tout nombre irrationnel, définir une correspondance biunivoque entre X et X' , ou entre X et X'' . La fonction $y = (b - a)x + a$ établissant une correspondance biunivoque entre l'intervalle $(0, 1)$ et l'intervalle (a, b) , l'ensemble des nombres réels d'un intervalle (a, b) quelconque, a la puissance du continu. De même, le corps $\mathbf{P}$ des nombres réels a la puissance du continu, puisque la fonction $y = \frac{x}{x^2 - 1}$, par exemple, réalise une correspondance biunivoque entre $\mathbf{P}$ et l'intervalle $(-\infty, +\infty)$.

L'ensemble des nombres algébriques réels étant dénombrable (comme partie infinie de l'ensemble dénombrable de tous les nombres algébriques), *l'ensemble des nombres réels transcendants ne peut être ni vide, ni fini, ni dénombrable* ⁽²⁾.

THÉORÈME 5. — *L'ensemble T des nombres transcendants réels a la puissance du continu.*

En effet, soit τ un nombre transcendant fixe et Δ l'ensemble dénombrable des nombres $\frac{\tau}{n}$, où n décrit l'ensemble des nombres naturels : posons $T' = T - \Delta$. Nous avons, A désignant l'ensemble dénombrable des nombres algébriques,

$$\mathbf{P} = A + T = (A + \Delta) + T',$$

⁽¹⁾ On trouvera une autre démonstration, se rattachant au procédé des intervalles emboîtés, dans É. BOREL, *Leçons sur la Théorie des Fonctions* (Gauthier-Villars, Paris, 1914, p. 14-15). Le théorème 4 a été découvert en 1873, par G. CANTOR (cf. *Briefwechsel Cantor-Dedekind*, Paris, Hermann, 1937, p. 14).

⁽²⁾ Cela entraîne l'existence de nombres transcendants que Liouville avait d'ailleurs, avant Cantor, établie par une autre méthode (voir, par exemple, É. BOREL, *Leçons sur la Théorie des Fonctions*, Paris, 1914, p. 26; G. VALIRON, *Théorie des fonctions*, Paris, 1942, p. 15).

$A + \Delta$ étant dénombrable comme Δ , $T = \Delta + T'$ et P ont visiblement même puissance.

Associons à tout nombre réel x tel que $0 < x \leq 1$ son développement binaire ou dyadique, c'est-à-dire son développement

$$x = 0, c_1, c_2, \dots, c_n, \dots \quad (c_i = 0 \text{ ou } 1),$$

dans le système de numération de base 2. Excluons les développements qui ne comportent qu'un nombre fini de 1 (¹). En écrivant seulement les termes d'un tel développement qui correspondent à des 1, nous avons

$$x = \frac{1}{2^{\alpha_1}} + \frac{1}{2^{\alpha_2}} + \dots + \frac{1}{2^{\alpha_k}} + \dots,$$

où les α_i forment une suite croissante illimitée. Posons $\alpha_k = \alpha_k - \alpha_{k-1}$ ($\alpha_0 = 0$), nous réalisons ainsi une correspondance biunivoque entre l'ensemble X des nombres réels x et l'ensemble des suites $\{a_1, a_2, \dots, a_k, \dots\}$ d'entiers naturels, d'où le théorème suivant :

THÉORÈME 6. — *L'ensemble des suites de nombres naturels a la puissance du continu.*

COROLLAIRE. — *L'ensemble des suites de nombres réels, $\{x_i\}$ ($0 < x_i \leq 1$), a la puissance du continu.*

Si, en effet, nous considérons chacune des suites de nombres naturels $\{a_1^1, \dots, a_l^k, \dots\}$ associées aux x_i , le procédé diagonal permet d'associer biunivoquement à la suite $\{x_i\}$ la suite de nombres naturels $\{a_1^1, a_2^1, a_1^2, \dots\}$ et, par conséquent, le nombre réel correspondant.

A un couple (x, y) de nombres réels ($0 < x \leq 1$, $0 < y \leq 1$) associés aux suites $\{a_i\}$, $\{b_i\}$, nous pouvons de même associer biunivoquement le nombre réel t correspondant à la suite $\{a_1, b_1, a_2, b_2, \dots\}$. *L'ensemble des points du carré $0 < x \leq 1$, $0 < y \leq 1$ dans le plan euclidien a donc la puissance du continu.* Il suffit maintenant d'associer biunivoquement les carrés découpés dans le plan par les droites $x = n$, $y = n'$ (dont l'ensemble est dénombrable), aux intervalles $(m, m+1)$ de la droite pour obtenir le théorème suivant :

THÉORÈME 7. — *L'ensemble des points du plan euclidien a la puissance du continu.*

(¹) On a, par exemple, $0,0\dots0100\dots = 0,0\dots0011\dots$

Ce résultat s'étend immédiatement à un espace euclidien de dimension quelconque.

2. Donnons pour terminer un théorème fondamental, dû à F. Bernstein, sur la *comparaison des puissances*.

Soient A et B deux ensembles. Si nous comparons ces ensembles avec leurs parties (véritables ou non), quatre cas, dont chacun exclut les trois autres, sont *a priori* possibles :

1° Il existe une partie A' de A et une partie B' de B telles que l'on ait

$$A' \leftrightarrow B \quad \text{et} \quad B' \leftrightarrow A.$$

2° Aucune partie de A n'a même puissance que B, mais il existe une partie B' de B telle que

$$B' \leftrightarrow A.$$

3° Aucune partie de B n'a même puissance que A, mais il existe une partie A' de A telle que

$$A' \leftrightarrow B.$$

4° Aucune partie de A n'a même puissance que B; aucune partie de B n'a même puissance que A.

THÉORÈME 8 (THÉORÈME DE BERNSTEIN). — *Dans le premier cas, les relations*

$$A' \subseteq A, \quad A' \leftrightarrow B; \quad B' \subseteq B, \quad B' \leftrightarrow A$$

entraînent

$$A \leftrightarrow B.$$

La correspondance biunivoque $B \leftrightarrow A'$ associe à la partie B' de B une partie A'' de A'. Nous avons donc

$$A'' \leftrightarrow B' \leftrightarrow A, \quad \text{avec} \quad A'' \subseteq A' \subseteq A$$

et il suffit de montrer que ces relations entraînent

$$A' \leftrightarrow A.$$

Posons $A'' = P$, $A' - A'' = Q$, $A - A' = R$. Nous devons montrer que

$$(f) \quad P + Q + R \leftrightarrow P \quad \text{entraîne} \quad P \leftrightarrow P + Q.$$

Soient X une partie de $P + Q + R$, $f(X)$ son image dans P par l'application biunivoque f . X sera dite *normale* si l'on a

$$(r) \quad f(X) \subseteq X$$

et

$$(2) \quad Q \subseteq X.$$

Toute intersection d'ensembles normaux est normale. Il existe d'ailleurs des parties normales, car $P + Q + R$ en est une.

L'image $f(X)$, étant contenue dans P , n'a aucun élément commun avec Q et les relations (1) et (2) sont équivalentes à

$$(3) \quad f(X) + Q \subseteq X.$$

De plus, si X est normale, $X_1 = f(X) + Q$ l'est aussi, car on a $Q \subseteq X_1$ et la relation $X_1 \subseteq X$ entraîne $f(X_1) \subseteq f(X) \subseteq X_1$.

Si, par conséquent, X_0 désigne l'intersection de toutes les parties normales, c'est-à-dire la plus petite partie normale, on a nécessairement

$$X_0 = f(X_0) + Q.$$

L'image $f(X_0)$ étant contenue dans P , posons

$$P = f(X_0) + Y.$$

Nous avons

$$P + Q = f(X_0) + Q + Y = X_0 + Y \leftrightarrow f(X_0) + Y = P,$$

ce qu'il fallait démontrer.

Montrons enfin, en utilisant l'axiome du choix sous la forme (II) de Hausdorff (existence d'une chaîne maximale, cf. Note III, p. 436) que le quatrième des cas envisagés plus haut ne peut pas se présenter.

THÉORÈME 9. — *Il est impossible que, simultanément, aucune partie de A n'ait même puissance que B, aucune partie de B même puissance que A.*

Soit Φ l'ensemble des applications biunivoques d'une partie de A sur une partie de B; Φ n'est pas vide, puisqu'on a par exemple

$$\emptyset \leftrightarrow \emptyset, \quad \{a\} \leftrightarrow \{b\} \quad (a \in A, b \in B).$$

Considérons deux telles applications

$$(\varphi_1) \quad A_1 \leftrightarrow B_1 \quad (A_1 \subseteq A, B_1 \subseteq B);$$

$$(\varphi_2) \quad A_2 \leftrightarrow B_2 \quad (A_2 \subseteq A, B_2 \subseteq B)$$

et convenons de poser

$$\varphi_1 \prec \varphi_2$$

si l'on a : $A_1 \subset A_2$ et $\varphi_1(x) = \varphi_2(x)$ pour tout $x \in A_1$, ce qui entraîne

$$B_1 = \varphi_1(A_1) = \varphi_2(A_1) \subset B_2$$

puisque α_1 est biunivoque. La relation $\prec$ ainsi définie est une relation d'ordre partiel stricte.

L'ensemble partiellement ordonné Φ contient une chaîne maximale $\mathcal{M}$ (propriété H⁽¹⁾). Designons par A_μ la partie de A qu'une application $\mu \in \mathcal{M}$ applique biunivoquement sur une partie de B , et posons

$$\bar{A} = \bigcup_{\mu \in \mathcal{M}} A_\mu.$$

Si x appartient à $\bar{A}$, x appartient à A_μ pour au moins un $\mu \in \mathcal{M}$; si plusieurs applications $\mu, \mu', \dots$ de $\mathcal{M}$ ont cette propriété, on a, puisque $\mathcal{M}$ est une chaîne,

$$\mu(x) = \mu'(x) = \dots \quad (= y \in B).$$

Nous définissons alors une application uniforme z en posant

$$(z) \quad x \rightarrow y \quad (x \in \bar{A}).$$

Supposons $y = z x_1 = z x_2$, où $x_1 \in A_{\mu_1}$, $x_2 \in A_{\mu_2}$ et par exemple $\mu_1 \prec \mu_2$; il en résulte

$$\mu_2(x_1) = \mu_1(x_1) = y = \mu_2(x_2),$$

ce qui exige $x_1 = x_2$ puisque μ_2 est univalente; z est donc une application biunivoque de $\bar{A}$ sur une partie $\bar{B}$ de B .

Par définition, z contient (strictement ou non) toute application μ de $\mathcal{M}$. Puisque $\mathcal{M}$ est maximale, il faut que z appartienne à $\mathcal{M}$ et soit maximale dans Φ . Mais alors, si $\bar{A}$ et $\bar{B}$ étaient des parties véritables de A et B , l'application β définie par

$$\begin{aligned} \beta x &= z x && \text{pour } x \in \bar{A}, \\ \beta u &= v, \end{aligned}$$

où u est un élément de $A - \bar{A}$, v un élément de $B - \bar{B}$, contiendrait strictement z , ce qui est impossible. Nous avons donc au moins une des deux égalités $A = \bar{A}$, $B = \bar{B}$, ce qui démontre le théorème (1).

Ainsi, l'axiome du choix étant admis, il devient toujours possible de comparer les puissances de deux ensembles A et B :

(1) Il suffit de modifier légèrement la démonstration précédente pour appliquer le théorème de Zorn (Z) au lieu de la propriété de Hausdorff (H).

1° Si

$$A \leftrightarrow B' \subseteq B \quad \text{et} \quad B \leftrightarrow A' \subseteq A,$$

A et B ont même puissance, d'après le théorème de F. Bernstein;

2° Si

$$A \leftrightarrow B' \subseteq B$$

sans que B ait même puissance qu'une partie de A, on dira que A a une puissance moindre que B;

3° Dans le cas symétrique du précédent, on dit que B a une puissance moindre que A.

La relation ainsi introduite entre ensembles est transitive : c'est une relation d'ordre total.



INDEX ALPHABÉTIQUE.

	Pages.
Abélien (demi-groupe-, groupeïde-).	80
— (groupe -).....	104
Absolue (relation-).....	11
Absorbant (relation- une autre)....	16
Absorption (loi d ²).....	96
Adjonction.....	303
— symbolique.....	371
d'Alembert (théorème de-).....	375
Algèbre.....	67
Algébrique (-élément).....	305
Algébrique (extension-simple).....	305
Algébriques (nombres-).....	305, 396
Algébriquement fermé (corps-).....	374
Alterné (groupe-).....	163, 166, 169
Anneau.....	138, 179
— de classes résiduelles... 148,	187
— des entiers.....	138
— euclidien.....	318
— à factorisation unique.....	313
— à idéaux principaux.... 192,	316
— noëthérien.....	192, 331
— de polynômes.....	328, 329
— quotient.....	148
— de quotients total.....	283
— des quotients.....	280
— régulier.....	279
Antérieur (élément-).....	17
Antisymétrique (relation-).....	15
Appartenance.....	1
Application inverse.....	29
— multiforme.....	24
Application semi-uniforme..... 35,	235
— uniforme.....	23, 27
Archimédien (corps ordonné-).....	287
Associables (équivalences-).....	63
Associative (opération-).....	78
Associativité faible.....	80
Associés (éléments-).....	202

	Pages.
Automorphisme.....	28, 128
— extérieur.....	176
— intérieur.....	176, 266
Axiome de la base finie.....	192, 205
Axiome des chaînes de diviseurs...	206
Axiome du choix.....	44
Axiome des quotients ¹	90
Axiomes des groupes ²	100
Axiomes de Peano.....	47, 425

B

Base (d'un idéal).....	192
Base finie (axiome de la-)....	192, 205
— (théorème de la-).....	331
Bernstein (théorème de F-).....	451
Bezout (relation de-).....	307
Bien ordonné (ensemble-).....	41
Bilatère (idéale-).....	76, 186
Biunivoque (application-).....	27
Bon ordre.....	41
Boole (treillis de-).....	95
Borne (inférieure, supérieure)..	39, 40
Boucle.....	91
Brandt (groupeïde de-).....	70

C

Annulation (élément-)	85
Annulation (loi de-)	85
Caractéristique (d'un anneau, d'un corps)	182
Caractéristique (polynôme-)	367
Cartésien (espace-)	446
Cauchy (critère de-)	295
— (méthode de-)	392
Centre	83, 168
Chaîne	37
— maximale	37, 403
— stricte	403
Θ -chaîne	433

	Pages.		Pages.
Champs de Galois.....	140	Conoyau.....	175
Choix (axiome du-).....	44	Consécutifs (éléments-).....	37
Circulaires (permutations-).....	113	Convexe (partie-).....	37
— (systèmes-).....	159	Corps.....	140
Classes.....	8	— de décomposition.....	371
— résiduelles.....	20, 148	— gauche.....	140
— de transitivité.....	126	— imparfait.....	363
— (équation des-).....	178	— des nombres complexes.....	373
Classe-unité.....	150	— des nombres rationnels.....	230
Codivisibles (complexes-).....	242	— des nombres réels.....	298
Cohérent (semi-groupe-).....	308	— ordonné.....	284
Commutant.....	173	— ordonné complet.....	295
Commutateur.....	173	— parfait.....	363
Commutative (opération-).....	80	— premier.....	303
Comparables (éléments-).....	17	— des quotients.....	280
Comparaison des puissances.....	451	— de rupture.....	371
Complément.....	3	— complet d'ensembles.....	32
— (dans un treillis).....	94	Correspondance.....	23
— relatif.....	96	— biunivoque.....	4
Complémentaire (sous-ensemble-).....	3	— de Galois.....	119
— (de a par m).....	90	— de Galois inversée.....	121
Complémenté (treillis-).....	94	Coupe (d'une relation).....	13
Complet (corps ordonné-).....	295	Critère de Cauchy.....	295
— (semi-groupe-).....	309	Cycle.....	160
— (treillis-).....	50	Cyclique (sous-groupe-).....	75
Complexe.....	72, 113	— (demi-groupe-).....	113
— équirésiduel.....	234	— (groupe-).....	111, 155
— fort.....	235		
— parfait.....	242	D	
— symétrique.....	234	Décomposition en classes.....	8
— transformé.....	166	— en facteurs.....	210, 343
— trivial.....	233	— d'un groupe par rap- port à un sous- groupe.....	151
Complexes (nombres-).....	373	— noethérienne.....	212
Composants primaires.....	214	Degré d'un élément algébrique.....	367
Composé (groupe-).....	115	— d'un polynome.....	329
Composée (application ou fonction-).....	26	Demi-groupe.....	78
Composition des segments.....	70	Demi-treillis.....	49
Composition (loi de-).....	67	Dénombrable (ensemble-).....	47
Concordance (principe de-).....	132	Dérivation.....	366
Condition de chaîne ascendante.....	50, 206	Dérivé (d'un groupe).....	173
— de chaîne descendante.....	51	Dérivée.....	362, 366
— maximale.....	50, 205, 415	Dernier (élément).....	37
— minimale.....	51, 414	Diagonale.....	15
— de réduction.....	313	Différence symétrique.....	9
— $\mathcal{C}$ de Ore.....	269	Différences.....	358
— Z de Malcev.....	267	Directions.....	20
Conditions de Moore... 52, 74, 170,	188	Discret (ensemble-).....	42, 420
Congruences.....	12, 20	Discriminant.....	399
Conjugués (éléments-).....	177	Disjoints (sous-ensembles-).....	6
— (éléments-d'une extension).....	370	Distance.....	441
Conjugués (éléments-par rapport à un groupe de transfor- mations).....	159		

	Pages.
Distingué (sous-groupe-)	165
Distributif (treillis-)	88
Distributive (opération-)	88
Diviseur	214
Diviseur (idéal-d'un autre)	189
Diviseur de zéro	181, 231
Division	91
— avec reste	319
— des polynomes	338
Domaine	67
— à factorisation unique	313
— d'intégrité	139, 181
— — ordonné	284
— de rationalité	140
Doublement bien ordonné(ensemble-)	42, 411
Droite	441
E	
Égalité	15
— d'ensembles	1
— de relations	12
Eisenstein (théorème d'-)	351
Élément	1
Élément-limite	42
Élément-neutre	77
Élément-unité	77
Élément-zéro	77, 104
Endomorphisme	146
Engendré (sous-groupe-)	75
— (sous-groupe-)	110
— (idéal-)	190
Ensemble	1
— discret	42, 420
— fermé	445
— fini	46, 401, 419
— inductif	45
— naturel	47, 420
— ordonné	17, 36
— ouvert	445
— des parties	3
— péanien	425
— produit	4
— quotient	20
— représentatif (d'une relation)	11
— représentatif (d'une application)	25
Ensembles de même puissance	27
— équipotents	27
— semblables	27
Entiers algébriques	397
— de Gauss	377

	Pages.
— naturels	47, 423
— rationnels	134
— relatifs	134, 226
Équation algébrique	354
— binome	376
— des classes	178
— de Pell	323
Équirésiduel (complexe-)	234
Équivalence (relations d'-)	18
— absolue	18
— d'application	29
— c	33, 59
— d'homomorphisme	29
— principale	233
— régulière	141, 150, 164, 185, 222, 234
— réversible	259
— simplifiable	144
— de transitivité	126, 159, 162
— universelle	18
Équivalence associables	63
— permutables	63
Équivalentes (extensions-)	133
Espace	441
— cartésien	446
— euclidien	441
— de Hausdorff	444
— métrique	442
— métrique complet	443
— projectif	446
— topologique	444
Essentiel (idéal premier-)	214
Euclide (algorithme d'-)	321
Euclidien (anneau-)	318
— (espace-)	441
Euler (indicateur ou fonction d'-)	156
Exposant (d'un groupe)	197
— (d'un idéal primaire)	202
Expression rationnelle	304
— — entière	305
Extension	132
Extension (ou sur-corps)	302
Extension saturée	21
Extension simple	304
Extensions conjuguées	370
— équivalentes	133, 369
Extérieurs (automorphismes-)	176
F	
Facteur (groupe-)	148
Facteur constant	344
Facteurs premiers	311

	Pages.		Pages.
Factorisation unique.....	311, 348	Groupe simple.....	168
Factoroïde.....	142	— symétrique.....	104, 163
Faible (ordre partiel-).....	17	— de transformations.....	117
Famille (de parties).....	3	— transitif.....	126
Fermat (théorème de : $x^p \equiv x \pmod{p}$)... 158, 184,	366	Groupeïde.....	67
Fermé (élément-).....	53	— de Brandt.....	67, 70
— (ensemble-).....	445	— quotient.....	142
— (multiplicativement-).....	73		
Fermeture.....	52	H	
Ferméture (propriétés de-).....	73	Hausdorff (condition de-).....	436
— (topologique).....	445	— (espaces de-).....	444
— transitive.....	57	Hessenberg-Kuratowski (procédé de-).....	403
Fini (ensemble-)..... 46, 401,	419	Hilbert (théorème de-).....	331
— (groupe-).....	105, 155	Holoïde..... 81, 209,	216
Fonction multiforme.....	24	— linéaire.....	209
— symétrique.....	385	Homogène (idéal-).....	336
— uniforme.....	23	Homogène (polynome-).....	329
Fonctionnelle (relation-).....	25	Homologues (fractions-).....	276
Fondamentales (relations-).....	112	Homomorphe (ensemble-à un autre). — (groupeïde-à un autre).	24 145
— (suites-).....	293	Homomorphisme (théorème d'-) 29, 147, 175, 187,	257
Forme.....	329	Hypergroupe.....	167
Forme normale (d'une table).....	106		
Fort (complexe-).....	235	I	
Fractions..... 226,	269	Idéal (dans un groupeïde).....	76
— rationnelles.....	328	— (dans un anneau).....	186
— rationnelles symétriques... 394		— maximal.....	197
Frobenius (théorème de-).....	178	— premier.....	198
		Idéal premier associé (à un idéal primaire)..	201
G		— premier essentiel.....	214
Galois (champ de-).....	140	— primaire.....	200
— (correspondance de-)... 119,	121	— principal.....	190
Gauche (corps-).....	140	— produit.....	194
Gauss (théorème de-).....	346	— sans diviseurs.....	197
Gauss (entiers de-).....	377	Idempotent (élément-).....	74
Générateurs..... 112,	156	— (groupeïde-).....	74
Gibbs (formule de-).....	79	Image..... 23,	24
Globalement idempotent (groupeïde-). Groupe.....	76 98	— inverse.....	27
— abélien.....	104, 175	Immersion..... 132, 224, 228, 266,	279
— alterné..... 163, 166,	169	Impaire (substitution-).....	163
— composé.....	114, 115	Imparfait (corps-).....	363
— cyclique.....	111, 155	Inclusion (des ensembles).....	2
— des déplacements.....	123	— (des relations).....	12
— facteur.....	148, 165	Indécomposable.....	216
— fini.....	105, 155	Index.....	155
— hamiltonien.....	168	Indexée (famille-).....	4
— intransitif.....	126, 159	Indicateur d'Euler.....	156
— de Klein.....	107, 166	Indivisible (partie-).....	21
— libre.....	112	Inductif (ensemble-).....	45
— quotient.....	148, 165		
— des quotients.....	271		

	Pages.
Induction complète.....	45
— transfinie.....	43
Induite (application-).....	24
Inférieur (élément-).....	17
Infini (ensemble-).....	47
Infiniment grands, ou petits (dans un corps ordonné non archimédien).....	288
Inséparable (polynome-).....	363
Intégrité (domaine d').....	139
Intérieur (d'un semi-groupe).....	266
Intérieurs (automorphismes-).....	176, 266
Intersection (de parties).....	5, 7
— (de relations).....	12
— (dans un ensemble partiellement ordonné).....	39, 52
— de sous-groupes... ..	110, 170
— d'idéaux.....	189
Intervalle (d'un ensemble ordonné).....	37
Intransitif (groupe-).....	126
Invariance numérique (d'une fonction).....	395
Invariant (élément-, sous-ensemble-).....	117
Invariant (sous-groupe-).....	165
Inverse (application-).....	31
— (élément-).....	93
— (opération-).....	91
— (relation-).....	11
Inversible (élément-).....	93, 104, 215
Inversif (demi-groupe-).....	104
Inversion (propriétés d').....	89
Involutif (élément-).....	93
Irréductible (élément-).....	210
Isobare (polynome-).....	386
Isomorphes (ensembles-).....	27
— (groupoïdes-).....	128
Isomorphisme.....	27, 128
Isotone.....	27, 122
J	
Jacobi (identité de-).....	79
K	
Klein (groupe de-).....	107, 166
Kronecker (procédé de-).....	359
Krull (condition de-).....	313
L	
Lagrange (formule d'interpolation de-).....	355
Libre (groupe-).....	112
Limite (élément-).....	42

	Pages
Limite (d'une suite).....	289
Limitée (application-).....	24
Linéaire (holoïde-).....	209
Loi de cancellation.....	85
— composition.....	67
Lois d'associativité faibles.....	80
Loop.....	91
M	
Majorant (élément-).....	38
Majoré (sous-ensemble-).....	38
Malcev (condition de-).....	267, 273
Maximal (élément-).....	38
Maximum (élément-).....	37
Minimal (élément-).....	37
Minimum (élément-).....	37
Minorant (élément-).....	39
Minoré (sous-ensemble-).....	39
Modulaire (treillis-).....	171, 189
Module.....	104
Module (d'un nombre complexe)....	373
Monome.....	329
Moore (conditions de-, théorème de-).....	52, 53, 74, 170, 188
Multiforme (application-).....	24
Multiples (dans un demi-groupe additif).....	78
— dans un anneau.....	190
—.....	214
Multiplicateur commun.....	280
Multiplicativement fermé.....	73
N	
Naturel (ensemble-).....	47, 420
Naturels (nombres-).....	47, 423
Négatifs (entiers-).....	134
Négation.....	3, 11
Net (complexe-).....	92, 222, 256
Neutre (élément-).....	77
Newton (méthode de-).....	390
Nilpotent (élément-).....	181
Noëther (multiplicité de-, théorème de-).....	381
Noëthérien (anneau-).....	192, 331
Nombres algébriques....	305, 396, 447
— complexes.....	373
— naturels.....	47, 423
— rationnels.....	230, 447
— réels.....	298, 448
— relatifs.....	134
— transcendants.....	305, 449
Normal (sous-groupe-).....	165
— (sous demi-groupe-).....	256

	Pages.
Normalisateur.....	178
Normée (représentation).....	214
Notations : voir <i>signes</i> .	
Noyau.....	231, 250
— d'un homomorphisme.....	174
Nul (élément-).....	37
O	
Opération.....	67
Oposé (élément-).....	93, 104
Ordination (procédés d'-).....	401
Ordonné (ensemble-).....	17, 36
— (domaine d'intégrité ou	
— corps-).....	284
Ordre (relation d'-, -partiel, -total)	
.....	17, 18
— (d'un groupoïde).....	68
— (d'un élément dans un groupe)	111
— (en un point).....	381
— (d'un zéro).....	361
P	
Paire (substitution-).....	163
Parfait (complexe-).....	242
— (corps-).....	363
Partiel (ordre-).....	17
Parties (d'un ensemble).....	2
— (ensemble des-).....	3
Partition.....	8
Pell (équation de-).....	323
Permis (complexe-, élément-).....	75
Permutables (équivalences-).....	63
— (complexes-).....	82
— (sous-groupes-).....	117
Permutation.....	28
— circulaire.....	113
Plan.....	441
Plus grand commun diviseur	
— (p. g. c. d.).....	308
— d'idéaux.....	189
Plus petit commun multiple	
— (p. p. c. m.).....	323
— d'idéaux.....	189
Poids.....	386
Point.....	441
— intérieur.....	444
— simple.....	382
Polynome.....	326
— inséparable (ou de seconde	
— espèce).....	363
— primitif.....	344
— séparable (ou de première	
— espèce).....	363

	Pages.
Positifs (entiers-).....	134
Postulat de Zermelo.....	439
Précédent.....	38
Premier (élément-).....	37, 217
— (élément- à un autre).....	307
— au sens strict.....	217
— (idéal-).....	198
— (sous-corps-).....	303
Premiers (éléments- entre eux).....	307
Préordre.....	22
Primaire (composant-).....	214
— (idéal-).....	200
Primitif (polynome-).....	344
Primitives (racines-).....	377
Principal (anneau-).....	192, 316
— (idéal-).....	190
Principale (équivalence-).....	233
Principe de concordance.....	132
— de l'élément maximal	
— (Zorn).....	45
— de spécialisation.....	330
Produit (ensemble-).....	4
— (relation-).....	14
— d'applications.....	26
— de complexes.....	72
— d'équivalences.....	61
— de groupes permutables.....	117
— d'idéaux.....	194
— transitif.....	57, 61
Progressions arithmétiques (d'ordre	
quelconque).....	358
Projectif (espace-).....	446
Projections (d'une relation).....	13
Prolongement (d'un isomorphisme).	133
Propre (partie-).....	3
— (relation-).....	15
Propriété du rectangle.....	84, 106
Pseudo-groupe, Pseudo-semi-groupe.	232
Pseudo-normal (sous-demi-groupe-).	255
Puissance (ensembles de même-)...	27
— du continu.....	449
Puissances (d'un élément).....	75, 78
Q	
Quasi fonctionnelle (relation-).....	25
Quasi-groupe.....	91
Quasi-ordre.....	22
Quotient (anneau-).....	148
— (d'un complexe par un	
— élément).....	92, 233
— (d'un élément par un	
— autre).....	90

	Pages.
Quotient (ensemble-)	20
— (groupe-)	148, 165
Quotients (anneau des-)	280, 283
— (axiome des-)	90
— (corps des-)	280
— (groupes des-)	271

R

Racine	354
— multiple, simple	361
Racines de l'unité	377
— primitives	377
Radical (d'un idéal)	188, 201
Rationnelle (expression-)	304
— (fraction-)	328, 394
Rationnels (entiers-)	134
— (nombres-)	230, 447
Réalisation	130
Réciproque (relation-)	15
Rectangle (propriété du-)	84, 106
Récurrence (raisonnement par-)	45
Réels (nombres-)	298, 448
Réflexive (relation-)	15
Règle de simplification	85
Régulier (anneau —)	279
— (demi-groupe-)	86, 267
Régulière (application-)	128
— (décomposition-)	141
— (équivalence-)	141, 150, 164, 185, 222, 234
Relatifs (entiers-)	134
Relation binaire	10
— $\mathcal{C}$	33, 59
— d'équivalence	18
— d'inclusion	2
— d'ordre	17
— produit	14
— de réversibilité	258
— $\mathcal{E}$	31, 59
Relations fondamentales	112
Représentants	20
Représentation isomorphe	130
Résidu	92, 233
Respectant (relation-une autre-)	16
— (transformation-)	123
Restreint (ordre-)	402
Restriction (d'une relation)	15, 402
Réticulé (ensemble-)	49
Réunion (de parties)	5, 7
— (de relations)	12
— complète	116
— générale	5

	Pages.
Réversible (équivalence-)	259
— (groupoïde-)	84
Rupture (corps de-)	371

S

Sans diviseurs (idéal-)	197
— diviseurs communs (éléments-)	307
Saturée (extension-, partie-)	21
Seconde espèce (polynome de-)	363
Section	37
— commençante, finissante	37
Segment (dans un ensemble ordonné)	37
— initial	37
Segment (ou vecteur lié)	20
Semblables (ensembles-)	27
Semi-groupe, D-semi-groupe	86, 87
Séparable (polynome-)	363
Signes principaux :	
$\in, \ni, \notin$	1
$=$	1
$\neq$	1
$\subset, \subseteq$ ou $\subseteq$	2, 12, 17
$\supset, \supseteq$	3
$\emptyset$	3
$\mathcal{E}(E)$	3
$\sim$	4
$\cap, \cup$	5, 7
$+$	6
$\sum$	8, 20
$\mathcal{S}\mathcal{A}$	11
$\mathcal{A}', \mathcal{A}''$	11
$ $	11, 214
$+$	214
χ	12
0	14
$=, \neq$	15
$<, >, \leq, \geq$	17
$\prec, \succ, \preceq, \succeq$	17
$x \equiv y(\mathcal{A})$	19
$E/\mathcal{A}$	20, 148
$\sim, \approx$	24, 145
$\simeq, \cong, \approx$	27, 128
$\sim$	133
$[A]$	
$\sim$	28
f^{-1}	30
$[a, b]$	37
(a, b)	37
$G(m, E)$	2

	Pages.		Pages.
x^+, x^-	38	Suivant.....	38
$\cap, \wedge, \inf$	39	Supérieur.....	17
$\cup, \vee, \sup$	39	Sur-corps.....	302
$\times, \prod$	57, 61	Symétrique (complexe-).....	234
$\square$	63	(fonction-) (polynome-).....	385
$a \circ b$	67	(groupe-)....., 104, 163	
$+, -, \times, :$	67, 68	(relation-).....	15
$:$	92	Système de représentants.....	20
a', a'', a^{-}	93	Systèmes circulaires.....	159
x^{-1}, H^{-1}	138		
W_H, HW	92, 233, 234	T	
$\mathcal{R}S, \mathcal{S}\mathcal{R}$	151, 152	Table d'opération.....	68, 83
$\mathcal{R}H, H\mathcal{R}$	234	Tangente.....	382
G/S	165	Théorème de d'Alembert (-fonda-	
A/m	187	mental de l'Algèbre).....	375
$a + b, (a, b), \sum m$	188, 189	— de Bernstein (F.).....	451
$a \cap b, [a, b], \cap m$	188, 189	— de décomposition (d'un idéal	
$A[x], A(x)$	328	dans un anneau noëthérien)....	212
Simple (extension-).....	304	— d'Eisenstein.....	351
— (groupe-).....	168	— de Fermat [$x^p \equiv x \pmod{p}$]... 184,	366
— (racine-, zéro-).....	361	— de Frobenius.....	178
Simplifiable (élément-).....	85	— de Gauss.....	346
— (équivalence-)....	144, 237	— de Hilbert (-de la base finie)..	331
Simplification (règle de-).....	85	— d'homomorphisme.....	29
Somme (de parties).....	6	147, 175, 187, 257	
— (d'idéaux).....	189	— de Moore.....	53
Sous-anneau.....	139	— de Noëther.....	381
Sous-corps.....	302	— de Wilson.....	367
— premier.....	303	— de Zermelo.....	44, 433
Sous-ensemble.....	2	— de Zorn.....	45, 437
Sous-groupe.....	107	Théorèmes sur les limites.....	290
— invariant (distingué,		Total (ordre-).....	18
normal).....	165	Trace (d'une relation).....	15
— propre, véritable, vrai....	107	Transcendant (élément- extension-e	
Sous-groupeïde.....	74	simple)....	305
Sous-module.....	107	Transcendants (nombres-)....	305, 449
Sous-treillis.....	49	Transformation.....	28
Spécialisation (principe de-).....	330	Transformations (groupes de-).....	117
Stable (sous-ensemble-).....	31	Transformé (complexe-,	
Strict (ordre-).....	17	élément-)....	166, 177
Substitution.....	28, 159	Transitif (groupe-).....	126
— paire, impaire.....	163	Transitive (relation-).....	16
Substitutions (groupes de-).....	163	Transitivité (équivalence de-, classes	
Suites.....	48	de-).....	126, 159, 162
— bornées.....	289	Transposition.....	161
— convergentes.....	289	Treillis.....	48
— fondamentales.....	293	— complémenté.....	94
— monotones.....	289	— distributif.....	88
— nulles.....	290	— modulaire.....	171, 189
— nulles triviales.....	290	— multiplicatif.....	196
		Trivial (complexe-).....	233
		Tukey (condition de-).....	438

U

	Pages.
Uniforme (application-, fonction-)..	23
Unitaire (complexe-).....	91, 243
Unité (élément-).....	77
Unités.....	215
Univalente (application-, fonction-)..	27
Universel (élément-).....	37
Universelle (relation-).....	11

V

Valeur absolue.....	134
Vecteur (-glissant, -libre -lié).....	20
Véritable (sous-ensemble).....	3
Vide (ensemble-, partie-).....	3

Pages.

Voisinages.....	444
Vrai (sous-ensemble).....	3

W

Waring (méthode de-).....	389
Wilson (théorème de-).....	367

Z

Zermelo (théorème de-).....	44, 433
Zéro (élément-).....	77, 104
Zéro (d'un polynome).....	354, 361
Zéroïde (élément-).....	249
Zorn (théorème de-).....	45, 437



TABLE DES MATIÈRES.

PRÉFACE.....	Pages. v
INTRODUCTION.....	ix

CHAPITRE I.

ENSEMBLES, RELATIONS, CORRESPONDANCES.

A. — <i>Éléments, sous-ensembles.</i>	
1. Principes de la théorie des Ensembles.....	1
2. Intersection, réunion.....	5
B. — <i>Relations.</i>	
3. Relations binaires; calcul des relations.....	10
4. Relations d'ordre.....	17
5. Relations d'équivalence.....	18
C. — <i>Correspondances.</i>	
6. Notions générales.....	23
7. Applications uniformes; théorème d'homomorphisme.....	27
8. Cas général : application inverse, sous-ensembles stables.....	29
D. — <i>Ensembles ordonnés.</i>	
9. Notions générales.....	36
10. Ensembles bien ordonnés, discrets, finis, naturels.....	41
11. Treillis.....	48
E. — <i>Relations transitives; relations d'équivalence.</i>	
12. Produit transitif, fermeture transitive.....	56
13. Produits de relations d'équivalence.....	61

CHAPITRE II.

OPÉRATIONS.

A. — <i>Groupoïdes. Algèbres.</i>	
1. Loi de composition.....	67
2. Remarques sur la notion d'opération.....	68
3. Complexes.....	72
B. — <i>Propriétés remarquables.</i>	
4. Propriétés de fermeture.....	73
5. Règles de calcul.....	77
6. Propriétés d'inversion.....	89

CHAPITRE III.

GROUPES.

Pages.

A. — *Définition des groupes.*

- | | |
|--|-----|
| 1. Propriétés d'inversion dans un demi-groupe; notion de groupe..... | 98 |
| 2. Groupes finis..... | 105 |

B. — *Sous-groupes.*

- | | |
|---|-----|
| 3. Conditions nécessaires et suffisantes..... | 107 |
| 4. Groupes cycliques..... | 111 |
| 5. Complexes et sous-groupes d'un groupe..... | 113 |
| 6. Groupes de transformations; propriétés d'invariance..... | 117 |

C. — *Isomorphismes.*

- | | |
|---|-----|
| 7. Notion d'isomorphismes..... | 127 |
| 8. Application à la définition des groupes. Extensions..... | 131 |
| 9. Entiers relatifs..... | 133 |
| 10. Anneaux; corps..... | 138 |

CHAPITRE IV.

ÉQUIVALENCES RÉGULIÈRES.

A. — *Équivalences régulières dans un groupoïde.*

- | | |
|---|-----|
| 1. Équivalences régulières, équivalences simplifiables..... | 141 |
| 2. Homomorphismes..... | 145 |

B. — *Équivalences régulières à droite dans un groupe.*

- | | |
|--|-----|
| 3. Décomposition d'un groupe en classes à droite par rapport à un sous-groupe. | 150 |
| 4. Groupes finis; groupes cycliques..... | 155 |
| 5. Groupes intransitifs. Substitutions, cycles, transpositions..... | 159 |

C. — *Équivalences régulières dans un groupe.*

- | | |
|--|-----|
| 6. Sous-groupes invariants..... | 164 |
| 7. Théorème d'homomorphisme (cas des groupes)..... | 174 |
| 8. Automorphismes intérieurs..... | 176 |

D. — *Équivalences régulières dans un anneau.*

- | | |
|---|-----|
| 9. Classification des anneaux..... | 179 |
| 10. Notion d'idéal..... | 185 |
| 11. Idéaux d'un anneau..... | 188 |
| 12. Idéaux sans diviseurs, idéaux premiers, idéaux primaires..... | 197 |
| 13. Condition maximale. Base finie. Axiome des chaînes de diviseurs..... | 205 |
| 14. Décomposition en facteurs dans un demi-groupe abélien avec élément-unité. | 209 |

CHAPITRE V.

DEMI-GROUPES. CORPS.

A. — *Demi-groupes abéliens. Problèmes d'immersion commutatifs.*

- | | |
|---|-----|
| 1. Groupes homomorphes à un demi-groupe abélien..... | 220 |
| 2. Immersion d'un semi-groupe abélien dans un groupe..... | 224 |
| 3. Immersion d'un domaine d'intégrité dans un corps..... | 228 |

B. — *Demi-groupes. Problèmes d'immersion : cas non commutatif.*

	Pages.
4. Équivalences principales. Complexes forts.....	230
5. Complexes symétriques forts. Pseudo-groupes et groupes homomorphes. à un demi-groupe D donné.....	249
6. Immersion d'un demi-groupe régulier à droite dans un groupe.....	266
7. Immersion d'un anneau régulier dans un corps. Généralisation.....	279

C. — *Corps ordonnés.*

8. Domaines ordonnés. Convergence.....	284
9. Corps ordonnés complets. Nombres réels.....	292
10. Sous-corps et sur-corps.....	302

CHAPITRE VI.

ANNEAUX

A. — *Factorisation.*

1. Éléments premiers entre eux; semi-groupes cohérents; semi-groupes complets.....	307
2. Semi-groupes à factorisation unique; anneaux à factorisation unique.....	311
3. Anneaux à idéaux principaux; anneaux euclidiens.....	316

B. — *Anneaux et idéaux de polynomes.*

4. Polynomes. Opérations entières.....	326
5. Idéaux de polynomes.....	331
6. Décomposition des polynomes.....	343

CHAPITRE VII.

ÉQUATIONS ALGÈBRIQUES.

A. — *Racines.*

1. Propriétés générales.....	354
2. Extensions simples, adjonction symbolique.....	367
3. Applications géométriques; théorème de Noëther.....	378

B. — *Fonctions symétriques.*

4. Théorème fondamental; méthode de Waring.....	385
5. Méthodes de Newton et de Cauchy. Applications.....	390

NOTE I. — *Ensembles finis.*..... 401

1. Introduction.....	401
2. Procédés d'ordination.....	401
3. Théorie ordinale.....	406
4. Comparaison de deux ensembles ordinalement finis.....	410
5. Ensembles doublement bien ordonnés.....	411
6. Théorie cardinale.....	414

NOTE II. — *Nombres naturels.*..... 420

1. Ensembles naturels.....	420
2. Ensembles péaniens.....	425
3. Compléments.....	430

NOTE III. — *Axiome du choix. Théorème de Zermelo. Théorème de Zorn.*..... 433NOTE IV. — *Espaces.*..... 441NOTE V. — *Correspondances biunivoques.*..... 447

INDEX ALPHABÉTIQUE..... 455

OUVRAGES DE LA COLLECTION

FASCICULES IN-8 RAISIN (16-25), SE VENDANT SÉPARÉMENT

- I. **Leçons sur quelques types simples d'Équations aux dérivées partielles, avec des Applications à la Physique mathématique**, par Emile PICARD, Professeur à l'Université de Paris; de 214 pages, avec 73 figures. Nouveau tirage; 1950.
- II. **Leçons sur la Géométrie des Espaces de Riemann**, par E. CARTAN, Professeur à la Faculté des Sciences de Paris; de vii-378 pages. Nouveau tirage; 1963.
- III. **Leçons sur quelques Equations fonctionnelles, avec des Applications à divers problèmes d'Analyse et de Physique mathématique**, par Emile PICARD, Professeur à l'Université de Paris. Rédigées par Eugène BLANC, Agrégé de l'Université; de 184 pages, avec 61 figures; 1950.
- IV. **Leçons sur les Systèmes d'Equations aux dérivées partielles**, par Maurice JANET, Professeur à l'Université de Caen; de viii-124 pages, 1929.
- V. **Leçons sur quelques Problèmes aux limites de la Théorie des Equations différentielles**, par Emile PICARD, Professeur à l'Université de Paris. Rédigées par Marcel BRELOT, ancien Elève de l'Ecole Normale; de 271 pages, 1930.
- VI. **Principes géométriques d'Analyse. 1^{re} Partie. Leçons faites à la Sorbonne** par Gaston JULIA, Professeur à la Faculté des Sciences de Paris. Recueillies et rédigées par Marcel BRELOT et René DE POSSEL, Agrégés de l'Université, anciens Elèves de l'Ecole Normale supérieure; de 116 pages, nouveau tirage; 1956.
- VII. **Leçons sur la Théorie mathématique de la Lutte pour la vie**, par Vito VOLTERRA, Professeur à l'Université de Rome, rédigées par Marcel BRELOT, ancien Elève de l'Ecole Normale supérieure; de 210 pages, 1931. (épuisé)
- VIII. **Leçons sur la Représentation conforme des aires simplement connexes**, par Gaston JULIA, Professeur à la Faculté des Sciences de Paris, de viii-114 pages; 2^e Edition. Nouveau tirage; 1950.
- IX. **Quelques applications analytiques de la Théorie des courbes et des surfaces algébriques**, par Emile PICARD, Professeur à l'Université de Paris. Leçons rédigées par Jean DIEUDONNÉ, Agrégé de l'Université; de viii-224 pages, 1931.
- X. **Leçons sur la Géométrie projective complexe**, par E. CARTAN, Professeur à la Faculté des Sciences de Paris, d'après des Notes recueillies et rédigées par F. MARTY, Elève à l'Ecole Normale supérieure; de vii-326 pages, 1931.
- XI. **Principes géométriques d'Analyse, 2^e Partie. Leçons faites à la Sorbonne**, par Gaston JULIA, recueillies et rédigées par André MAGNIER, Elève de l'Ecole Normale supérieure; de vii-122 pages, avec figures; Nouveau tirage; 1952.
- XII. **Figures planétaires et Géodésie**, par R. WAVRE, Professeur à l'Université de Genève, Préface de J. HADAMARD, Membre de l'Institut, Professeur au Collège de France et à l'Ecole Polytechnique; de viii-194 pages, 1932.
- XIII. **Leçons sur les fonctions presque périodiques**, par J. FAVARD, Maître de Conférences à la Faculté des Sciences de Grenoble. Préface de M. Gaston JULIA, Professeur à la Faculté des Sciences de Paris; de viii-184 pages, 1933.
- XIV. **Leçons sur la Représentation conforme des aires multiplement connexes**, par Gaston JULIA, Professeur à la Faculté des Sciences de Paris, Leçons recueillies et rédigées par MM. Georges BOURION et Jean LERAY, Docteur ès Sciences; de vi-93 pages. Nouveau tirage; 1956.
- XV. **Potentiels et Prépotentiels**, par Pierre HUMBERT, Professeur à l'Université de Montpellier. Préface de M. Louis de BROGLIE, Membre de l'Institut; de vii-78 pages, 1936.
- XVI. **Introductions mathématiques aux théories quantiques. (Première partie)**, par Gaston JULIA, Professeur à la Faculté des Sciences de Paris. Leçons rédigées par J. DUFRESNOY, Elève de l'Ecole Normale supérieure; de vi-218 pages, 3^e édition, revue et augmentée, 1958.

- XVII. Leçons sur la théorie des espaces à connexion projective**, par E. CARTAN, Professeur à la Faculté des Sciences de Paris. Leçons rédigées par P. VINCENSINI Docteur ès Sciences, Chargé de recherches; de vi-308 pages, 1937.
- XVIII. La théorie des groupes finis et continus et la géométrie différentielle traitées par la méthode du repère mobile**. Leçons professées à la Sorbonne par E. CARTAN, Membre de l'Institut. Rédigées par Jean LERAY, Maître de Conférences à la Faculté des Sciences de Nancy; de vi-270 pages, 1937.
- XIX. Introduction mathématique aux Théories quantiques**. 2^e Partie, par G. JULIA, Membre de l'Institut. Leçons rédigées par R. MARROT; de vii-322 pages. 2^e Edition revue et augmentée; 1955.
- XX. ALGÈBRE. TOME I. Equivalence, Opérations, Groupes, Anneaux, Corps**, par Paul DUBREIL, Professeur à la Faculté des Sciences de Nancy. Maître de Conférences à l'Ecole Polytechnique. Préface de M. Gaston JULIA, Membre de l'Institut; de xii-468 pages. 3^e Ed. revue et augmentée, 1963.
- XXI. Leçons sur la théorie des treillis**, par M^{me} M.-L. DUBREIL-JACOTIN, R. CROISOT, Professeurs à la Faculté des Sciences de Poitiers, et R. LESIEUR, Maître de Conférences à la Faculté des Sciences de Besançon; de vii-383 pages, 88 figures; 1953.
- XXII. Représentation conforme et transformations à intégrale de Dirichlet bornés** par M^{me} J. LELONG-FERRAND, Professeur à la Faculté des Sciences de Lille; de 222 pages, 1955.
- XXIII. Produits d'inversions et métriques, conforme**, par R. LAGRANGE, Professeur à la Faculté des Sciences de Dijon; de x-332 pages; 1957.
- XXIV. Cours de géométrie différentielle locale**, par J. FAVARD, Professeur à la Faculté des Sciences de Paris; de x-553 pages; 1957.
- XXV. Les algèbres d'opérateurs dans l'espace Hilbertien (Algèbres de Von Neumann)**, par J. DIXMIER, Professeur à la Faculté des Sciences de Paris; de vi-367 pages, 1957.
- XXVI. Cours d'analyse de l'Ecole Polytechnique. TOME I. Introduction, Opérations**, par J. FAVARD, Professeur à l'Ecole Polytechnique et à la Faculté des Sciences de Paris; de viii-676 pages, 1960.
TOME II. Représentations. Fonctions analytiques, vi-578 pages; 1960.
TOME III. Théorie des Equations - Fasc. I. Equations différentielles. viii-194 pages, 1962; Fasc. II. Equations aux dérivées partielles. Equations intégrales. Calcul des variations. 542 pages, 24 figures. 1963.
- XXVII. Algèbre géométrique**, par ARTIN, Professeur à l'Université de Princeton. Traduit par M. LAZARD, Professeur à la Faculté des Sciences de Poitiers. Préface de M. Gaston JULIA, Membre de l'Institut; de x-212 pages, 1962.

Joseph FLOCH, Maître-Imprimeur à Mayenne 15 Juillet 1963 - N° 1993
Dépôt légal 1148 N° de Code 512,77

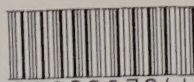
6337

IMPRIMÉ EN FRANCE

512.D819 1963 V01



a39001



006896784b

512
D819
1963
V.1



