

ACTUALITÉS SCIENTIFIQUES ET INDUSTRIELLES

934-1144

ÉLÉMENTS DE MATHÉMATIQUE

PAR

N. BOURBAKI

IV

PREMIÈRE PARTIE

LES STRUCTURES FONDAMENTALES DE L'ANALYSE

LIVRE II

ALGÈBRE

CHAPITRE I

STRUCTURES ALGÉBRIQUES

DEUXIÈME ÉDITION



PARIS

HERMANN & C^e, ÉDITEURS

6, Rue de la Sorbonne, 6

1951

INTRODUCTION

Faire de l'Algèbre, c'est essentiellement *calculer*, c'est-à-dire effectuer, sur des éléments d'un ensemble, des « opérations algébriques », dont l'exemple le plus connu est fourni par les « quatre règles » de l'arithmétique élémentaire.

Ce n'est pas ici le lieu de retracer le lent processus d'abstraction progressive par lequel la notion d'opération algébrique, d'abord restreinte aux entiers naturels et aux grandeurs mesurables, a peu à peu élargi son domaine, à mesure que se généralisait parallèlement la notion de « nombre », jusqu'à ce que, dépassant cette dernière, elle en vint à s'appliquer à des éléments qui n'avaient plus aucun caractère « numérique », par exemple aux permutations d'un ensemble (voir Note historique du chap. I). C'est sans doute la possibilité de ces extensions successives, dans lesquelles la *forme* des calculs restait la même, alors que la *nature* des êtres mathématiques soumis à ces calculs variait considérablement, qui a permis de dégager peu à peu le principe directeur des mathématiques modernes, à savoir que les êtres mathématiques, en eux-mêmes, importent peu : ce qui compte, ce sont leurs *relations* (voir Livre I). Il est certain, en tout cas, que l'Algèbre a atteint ce niveau d'abstraction bien avant les autres parties de la Mathématique, et il y a longtemps déjà qu'on s'est accoutumé à la considérer comme l'étude des opérations algébriques, indépendamment des êtres mathématiques auxquels elles sont susceptibles de s'appliquer.

Dépouillée de tout caractère spécifique, la notion commune sous-jacente aux opérations algébriques usuelles est fort simple : effectuer une opération algébrique sur deux éléments a, b d'un même ensemble E , c'est faire correspondre au couple (a, b) un troisième élément bien déterminé c de l'ensemble E . Autrement dit, il n'y a rien de plus dans cette notion que celle de *fonction* : se donner une opération algébrique, c'est se donner une fonction, définie dans $E \times E$, et prenant ses valeurs dans E ; la seule parti-

Printed in France

Tous droits de traduction, de reproduction et d'adaptation réservés pour tous pays.

COPYRIGHT 1951 BY LIBRAIRIE SCIENTIFIQUE HERMANN ET C^{ie}
PARIS.

cularité réside dans le fait que l'ensemble de définition de la fonction est le produit de deux ensembles identiques à l'ensemble où la fonction prend ses valeurs ; c'est à une telle fonction que nous donnons le nom de *loi de composition interne*.

A côté de ces lois « internes », on a été conduit (principalement sous l'influence de la Géométrie) à considérer un autre type de « loi de composition » ; ce sont les lois « externes », où, en dehors de l'ensemble E (qui reste pour ainsi dire au premier plan) intervient un ensemble auxiliaire Ω , dont les éléments sont qualifiés d'*opérateurs* : la loi faisant cette fois correspondre à un couple (α, a) formé d'un opérateur $\alpha \in \Omega$ et d'un élément $a \in E$, un second élément b de E . Par exemple, une homothétie de centre donné, dans l'espace euclidien E , fait correspondre, à un nombre réel k (le « rapport d'homothétie », qui est ici l'opérateur) et à un point A de E , un autre point A' de E : c'est une loi de composition externe dans E .

Conformément aux définitions générales (*Ens. R*, § 8), la donnée, dans un ensemble E , d'une ou plusieurs lois de composition (internes ou externes) définit une *structure* sur E ; c'est aux structures définies de cette manière que nous réservons, de façon précise, le nom de *structures algébriques*, et c'est l'étude de ces structures qui constitue l'Algèbre.

Il y a de nombreuses *espèces* (*Ens. R*, § 8) de structures algébriques, caractérisées, d'une part par les lois de composition qui les définissent, de l'autre par les *axiomes* auxquels sont assujetties ces lois. Bien entendu, ces axiomes n'ont pas été choisis arbitrairement, mais ne sont autres que les propriétés appartenant à la plupart des lois de composition qui interviennent dans les applications, telles que l'associativité, la commutativité, etc. Le chapitre I est essentiellement consacré à l'exposé de ces axiomes et des conséquences générales qui en découlent ; on y fait aussi une étude plus détaillée des deux espèces de structures algébriques les plus importantes, celle de *groupe* (où n'intervient qu'une loi de composition interne) et celle d'*anneau* (à deux lois de composition internes), dont la structure de *corps* est un cas particulier.

Au chapitre I sont aussi définis les *groupes à opérateurs* et *anneaux à opérateurs*, où, en plus des lois de composition internes, interviennent une ou plusieurs lois *externes*. Les plus importants

des groupes à opérateurs sont les *modules*, dans lesquels rentrent en particulier les *espaces vectoriels*, qui jouent un rôle prépondérant aussi bien dans la Géométrie classique que dans l'Analyse moderne. L'étude des structures de module tire son origine de celle des *équations linéaires*, d'où son nom d'*Algèbre linéaire* ; on en trouvera les résultats généraux au chapitre II.

De même, les anneaux à opérateurs qui interviennent le plus souvent sont ceux qu'on désigne sous le nom d'*algèbres* (ou *systèmes hypercomplexes*). Aux chapitres III et IV, on fait une étude détaillée de deux algèbres particulières : l'*algèbre extérieure*, qui, avec la théorie des déterminants qui en découle, est un auxiliaire précieux de l'Algèbre linéaire ; et l'*anneau des polynomes*, qui est à la base de la théorie des équations algébriques.

Au chapitre V est exposée la théorie générale des *corps commutatifs*, et de leur classification. L'origine de cette théorie est l'étude des équations algébriques à une inconnue ; les questions qui lui ont donné naissance n'ont plus guère aujourd'hui qu'un intérêt historique, mais la théorie des corps commutatifs reste fondamentale en Algèbre, étant à la base de la théorie des nombres algébriques, d'une part, de la Géométrie algébrique, de l'autre.

Comme l'ensemble des entiers naturels est muni de deux lois de composition internes, l'addition et la multiplication, l'Arithmétique (ou Théorie des Nombres) classique, qui est l'étude des entiers naturels, est subordonnée à l'Algèbre. Toutefois, il intervient, en liaison avec la structure algébrique définie par ces deux lois, la structure définie par la *relation d'ordre* « a divise b » ; et le propre de l'Arithmétique classique est précisément d'étudier les relations entre ces deux structures associées. Ce n'est pas le seul exemple où une structure d'ordre soit ainsi associée à une structure algébrique par une relation de « divisibilité » : cette relation joue un rôle tout aussi important dans les anneaux de polynomes. Aussi en fera-t-on une étude générale au chapitre VI ; cette étude sera appliquée au chapitre VII à la détermination de la structure des modules sur certains anneaux particulièrement simples, et en particulier à la théorie des « diviseurs élémentaires ».

Les chapitres VIII et IX sont consacrés à des théories plus particulières, mais qui ont de multiples applications en Analyse : d'une part, celle des *formes quadratiques* et des *formes hermitiennes*, avec l'étude des groupes qui leur sont associés ; d'autre part, les

géométries élémentaires (affine, projective, euclidienne, etc.) dans ce qu'elles ont de purement algébrique : il n'y a guère là qu'un langage nouveau pour exprimer des résultats d'Algèbre déjà obtenus par ailleurs, mais c'est un langage particulièrement bien adapté aux développements ultérieurs de la Géométrie algébrique et de la Géométrie différentielle, auxquelles ce chapitre sert d'introduction.



ALGÈBRE

CHAPITRE I

STRUCTURES ALGÉBRIQUES

§ 1. — Lois de composition internes ; associativité ; commutativité.

1. Lois de composition internes.

DÉFINITION 1. — On appelle *loi de composition interne* entre éléments d'un ensemble E une application f d'une partie A de $E \times E$ dans E . La valeur $f(x, y)$ de f pour un $(x, y) \in A$ s'appelle le composé de x et de y pour cette loi.

Par abus de langage, on dit qu'une telle loi est donnée (ou définie) sur E . Les lois de composition internes les plus importantes sont celles qui sont définies pour tous les couples $(x, y) \in E \times E$: par abus de langage, on dit qu'une telle loi est *partout définie* sur E . Dans ce qui suit, il sera surtout question de lois partout définies.

Le composé de x et de y se note le plus souvent en écrivant x et y dans un ordre déterminé et en les séparant par un signe caractéristique de la loi envisagée (signe qu'on pourra convenir d'omettre éventuellement). Parmi les signes dont l'emploi est le plus fréquent, citons dès maintenant $+$ et \cdot , étant convenu en général que ce dernier peut s'ommettre à volonté ; avec ces signes, le composé de x et de y s'écrira respectivement $x + y$, et $x \cdot y$ ou xy . Une loi notée par le signe $+$ s'appelle le plus souvent *addition* (le composé $x + y$ s'appelant alors la *somme* de x et de y) et on

dit qu'elle est *notée additivement*; une loi notée par le signe \cdot s'appelle le plus souvent *multiplication* (le composé $x \cdot y = xy$ s'appelant alors *produit de x et de y*), et on dit qu'elle est *notée multiplicativement*. Dans les raisonnements généraux des paragraphes 1 à 5 du présent chapitre, on se servira ordinairement des signes τ et \perp pour noter des lois de composition quelconques.

Il est indispensable, en Algèbre, de savoir *traduire* immédiatement toute proposition, relative à une loi de composition, d'une notation dans une autre. Pour lui faciliter sa tâche à cet égard, le lecteur trouvera, à la fin de ce chapitre (Dépliant II), un *lexique* des termes et symboles relatifs aux principales notions concernant les lois de composition, exprimés dans les notations les plus usitées (notamment la notation additive et la notation multiplicative).

Exemples. — 1) Les applications $(X, Y) \rightarrow X \cup Y$ et $(X, Y) \rightarrow X \cap Y$ sont des lois de composition internes (partout définies) entre parties d'un ensemble E .

2) Dans l'ensemble N des entiers naturels, l'addition, la multiplication, l'exponentiation sont des lois de composition partout définies (les composés de $x \in N$ et de $y \in N$ par ces lois se notant respectivement $x + y$, xy ou $x \cdot y$, et x^y ; voir *Ens.*, chap. III).

3) Dans l'ensemble N des entiers naturels, la soustraction $x - y$ est une loi de composition interne qui n'est définie que pour les couples (x, y) tels que $x \geqslant y$; de même, la division $\frac{x}{y}$ n'est définie que pour les couples (x, y) tels que $y \neq 0$ et que x soit multiple de y .

4) Soit E un ensemble quelconque; l'application $(X, Y) \rightarrow X \circ Y$ est une loi de composition entre parties de $E \times E$ (*Ens.*, R, § 3, no 10); l'application $(f, g) \rightarrow f \circ g$ est une loi de composition entre applications de E dans E (*Ens.*, R, § 2, no 11).

5) Dans l'ensemble des applications dans E d'une partie quelconque de E (*Ens.*, R, § 3, no 5) l'application $(f, g) \rightarrow f \circ g$ est une loi de composition interne qui n'est définie que pour les couples (f, g) tels que, si A et B sont les parties de E où sont définies respectivement f et g , on ait $g(B) \subset A$.

6) Soit E un ensemble ordonné réticulé (*Ens.*, R, § 6, no 8): si on désigne par $\sup(x, y)$ la borne supérieure de l'ensemble $\{x, y\}$, l'application $(x, y) \rightarrow \sup(x, y)$ est une loi de composition partout définie entre éléments de E . De même pour la borne inférieure $\inf(x, y)$. L'exemple 1 ci-dessus rentre dans celui-ci, en considérant $\mathfrak{P}(E)$ comme ordonné par inclusion.

Soit $(x, y) \rightarrow x \tau y$ une loi de composition entre éléments d'un ensemble E , définie sur une partie A de $E \times E$. Étant données

deux parties quelconques X, Y de E , on désignera par $X \tau Y$ (pourvu que cette notation ne prête pas à confusion (*)) l'ensemble des éléments $x \tau y$ de E , tels que $x \in X, y \in Y$ et $(x, y) \in A$ (autrement dit, l'image par l'application $(x, y) \rightarrow x \tau y$ de la trace de $X \times Y$ sur A).

L'application $(X, Y) \rightarrow X \tau Y$ est donc une loi de composition partout définie entre parties de E (si $(x, y) \notin A$, on a $\{x\} \tau \{y\} = \emptyset$).

Soit $(x, y) \rightarrow x \tau y$ une loi de composition partout définie entre éléments de E ; l'application $(x, y) \rightarrow y \tau x$ est aussi une loi de composition partout définie, qui est dite *opposée* à la précédente. Si la loi $(x, y) \rightarrow x \tau y$ est définie sur une partie A de $E \times E$, la relation $(y, x) \in A$ est équivalente à $(x, y) \in \bar{A}$ (*Ens.*, R, § 3, no 4), donc $(x, y) \rightarrow y \tau x$ est une application de \bar{A} dans E , qui s'appelle encore la loi de composition *opposée* à la précédente. En d'autres termes :

DÉFINITION 2. — *Deux lois de composition* (partout définies ou non) entre éléments de E sont dites *opposées* si chacune d'elles est composée de l'autre et de la symétrie canonique de $E \times E$. Si l'une est partout définie, il en est de même de l'autre.

D'après nos définitions générales (*Ens.*, R, § 8, no 2), la donnée d'une loi de composition entre éléments d'un ensemble E définit une *structure* sur cet ensemble : c'est là une espèce particulière de *structure algébrique* (la définition générale d'une structure algébrique sera donnée au § 4 de ce chapitre). Une telle structure est dite *déterminée* sur E par la loi de composition considérée.

Soient E et E' deux ensembles, munis chacun de la structure déterminée par une loi de composition interne ; nous noterons cette loi par le signe τ sur chacun des deux ensembles ; soit A la partie de $E \times E$, A' la partie de $E' \times E'$ où sont respectivement

(*) Voici un exemple où ce principe de notation prêterait à confusion et ne devra donc pas s'appliquer. Supposons qu'il s'agisse de la loi de composition $A \cup B$ entre parties d'un ensemble E ; on en déduit une loi de composition $(\mathfrak{A}, \mathfrak{B}) \rightarrow F(\mathfrak{A}, \mathfrak{B})$, entre parties de $\mathfrak{P}(E)$, $F(\mathfrak{A}, \mathfrak{B})$ étant l'ensemble des $A \cup B$ pour $A \in \mathfrak{A}, B \in \mathfrak{B}$; mais $F(\mathfrak{A}, \mathfrak{B})$ ne devra pas se noter $\mathfrak{A} \cup \mathfrak{B}$, cette notation ayant déjà un sens différent (réunion de \mathfrak{A} et \mathfrak{B} considérées comme parties de $\mathfrak{P}(E)$).

définies ces deux lois. Conformément aux définitions générales (*Ens. R*, § 8, n° 5), on appelle *isomorphisme* de E sur E' une application *biunivoque* f de E sur E' , dont l'extension à $E \times E$ applique A sur A' , et pour laquelle on a

$$(1) \quad f(x \tau y) = f(x) \tau f(y)$$

chaque fois que $x \tau y$ est défini (c'est-à-dire pour tout couple $(x, y) \in A$). On dit que E et E' sont *isomorphes* (ou qu'il y a *isomorphie* entre leurs structures) s'il existe un isomorphisme de E sur E' .

Plus généralement, on dit qu'une application f de E dans E' est une *représentation* de E dans E' , si, chaque fois que le composé $x \tau y$ est défini, le composé $f(x) \tau f(y)$ est défini et satisfait à la relation (1) (c'est là un cas particulier d'une notion qui sera définie au § 4 pour une structure algébrique quelconque).

Si la loi τ sur E est partout définie, il est immédiat qu'un isomorphisme de E sur E' n'est autre qu'une *représentation biunivoque* de E sur E' . Cette proposition n'est plus exacte si la loi τ n'est pas partout définie sur E , car alors, pour une représentation biunivoque f de E sur E' , il peut se faire que $f(x) \tau f(y)$ soit défini, mais non $x \tau y$.

2. Composé d'une séquence d'éléments.

Rappelons (*Ens. R*, § 2, n° 14) qu'une *famille* d'éléments d'un ensemble E est définie par la donnée d'un ensemble d'indices I et d'une application $i \rightarrow x_i$ de I dans E ; on dit qu'une famille $(x_i)_{i \in I}$ est *finie* si l'ensemble d'indices est *fini*.

L'ensemble d'indices I d'une famille peut éventuellement être muni d'une *structure* (*Ens. R*, § 8); si I et K sont deux ensembles d'indices munis de structures de même espèce, on dira que deux familles $(x_i)_{i \in I}$, $(y_\alpha)_{\alpha \in K}$ d'éléments d'un *même* ensemble E sont *semblables* (relativement aux structures de I et K) s'il existe un *isomorphisme* φ de I sur K tel que $x_i = y_{\varphi(i)}$ pour tout $i \in I$.

Il est commode de désigner d'un nom spécifique les familles dont l'ensemble d'indices est muni d'une structure particulière, notamment lorsque, pour une même famille $(x_i)_{i \in I}$, il y a lieu de considérer des structures différentes sur l'ensemble d'indices I . C'est ce qui se présente en Algèbre, où nous allons devoir consi-

dérer particulièrement le cas d'une famille *finie* $(x_i)_{i \in I}$, dont l'ensemble d'indices I est muni d'une structure d'ensemble *totalement ordonné*; on dit que la donnée de la famille $(x_i)_{i \in I}$ et de la structure d'ensemble totalement ordonné de I définit une *séquence* d'éléments de E ; cette séquence se notera encore $(x_i)_{i \in I}$, mais cette notation ne détermine la séquence que si on a précisé la structure d'ensemble totalement ordonné de I .

Étant donnée une famille finie $(x_\alpha)_{\alpha \in A}$ d'éléments d'un ensemble E , il lui correspond autant de séquences que de structures d'ensemble totalement ordonné sur A (c'est-à-dire $p!$ si A est un ensemble de p éléments); toutes ces séquences doivent être considérées comme distinctes. Si on considère en particulier une *suite* finie $(x_i)_{i \in H}$, où H est une partie finie de l'ensemble N des entiers naturels, il lui correspond une séquence particulière en prenant sur H la structure définie par la relation d'ordre $m \leq n$ entre entiers naturels (*Ens. R*, § 6, n° 2); lorsqu'on considérera la suite comme une séquence, sans préciser la relation d'ordre sur H , il sera convenu qu'il s'agit de cette relation d'ordre particulière. Avec cette convention, on peut dire qu'une séquence quelconque $(x_\alpha)_{\alpha \in A}$ est *semblable* (au sens défini ci-dessus) à une suite finie, car il existe une application biunivoque et croissante de l'ensemble totalement ordonné A sur un intervalle $[0, n]$ de l'ensemble N .

Ces définitions étant posées, soit E un ensemble muni d'une loi de composition interne τ *partout définie*.

DÉFINITION 3. — Soit $(x_\alpha)_{\alpha \in A}$ une séquence d'éléments de E . Pour toute partie non vide B de A (totalement ordonnée par l'ordre induit), on appelle *composé* (pour la loi τ) de la séquence $(x_\alpha)_{\alpha \in B}$ et on note $\prod_{\alpha \in B} x_\alpha$, l'élément de E défini par récurrence sur le nombre d'éléments de B , de la façon suivante :

$$1^\circ \text{ si } B = \{\beta\}, \prod_{\alpha \in B} x_\alpha = x_\beta;$$

2^o si B a $p > 1$ éléments, et si β est le plus petit élément de B , B' l'ensemble des éléments $> \beta$ dans B , $\prod_{\alpha \in B} x_\alpha = x_\beta \tau \left(\prod_{\alpha \in B'} x_\alpha \right)$.

Il est immédiat (par récurrence sur le nombre d'éléments des ensembles d'indices) que les composés de deux séquences *semblables* sont égaux ; en particulier, le composé d'une séquence quelconque est égal au composé d'une suite finie (ce qui permet, si on veut, de se restreindre à ces derniers). Si $A = \{\lambda, \mu\}$ a deux éléments ($\lambda < \mu$) le composé $\prod_{\alpha \in A} x_\alpha$ n'est autre que $x_\lambda \tau x_\mu$.

Du point de vue des notations, le composé d'une séquence $(x_\alpha)_{\alpha \in A}$ s'écrit $\prod_{\alpha \in A} x_\alpha$ pour une loi notée τ ; pour une loi notée additive-

ment, il est d'usage de le désigner par $\sum_{\alpha \in A} x_\alpha$, et de l'appeler la somme de la séquence $(x_\alpha)_{\alpha \in A}$ (les x_α étant appelés les termes de la somme) ; pour une loi notée multiplicativement, on le désigne le plus souvent par la notation $\prod_{\alpha \in A} x_\alpha$, et on l'appelle le produit de la séquence (x_α) (les x_α étant appelés les facteurs du produit) (*).

Lorsqu'il n'y a pas de confusion possible sur l'ensemble d'indices (ni sur sa structure d'ordre) on se dispense souvent de l'écrire dans la notation du composé d'une séquence et on écrit donc, par exemple pour une loi notée additivement, $\sum x_\alpha$ ou même $\sum x_\alpha$, au lieu de $\prod_{\alpha \in A} x_\alpha$; de même pour les autres notations.

Pour une loi notée τ , le composé d'une suite (x_i) ayant pour ensemble d'indices un intervalle $[p, q]$ de N , se note $\prod_{p \leq i \leq q} x_i$, ou $\prod_{i=p}^q x_i$, ou encore $x_p \tau x_{p+1} \tau \dots \tau x_q$; de même pour des lois notées par d'autres signes.

Remarques. — 1) Pour une loi interne τ non partout définie, on peut encore définir le composé d'une séquence comme dans la

(*) L'emploi de ce terme, et de la notation $\prod_{\alpha \in A} x_\alpha$, devra toutefois être évité lorsque les x_α sont des ensembles, afin de ne pas entraîner confusion avec le terme et la notation analogues de la Théorie des Ensembles.

déf. 3, mais cette définition n'aura de sens que pour les séquences satisfaisant à certaines conditions.

2) On notera qu'il y a un certain arbitraire dans la définition du composé d'une séquence ; la récurrence que nous avons introduite procède « de droite à gauche » : pour une suite $(x_i)_{1 \leq i \leq n}$ de n éléments explicités, le composé de la suite n'est autre que $x_1 \tau (x_2 \tau (x_3 \tau (\dots \tau (x_{n-1} \tau x_n) \dots)))$ ($n-2$ parenthèses). Il serait tout aussi légitime de définir le composé en procédant « de gauche à droite » ou de toute autre façon (par un groupement quelconque des parenthèses) ; mais, comme nous allons le voir, cet arbitraire disparaît pour les lois les plus importantes en pratique, les lois associatives.

3. Lois associatives.

DÉFINITION 4. — Une loi de composition $(x, y) \rightarrow x \tau y$ partout définie entre éléments d'un ensemble E , est dite associative si, quels que soient les éléments x, y, z de E , on a

$$(2) \quad (x \tau y) \tau z = x \tau (y \tau z).$$

Un ensemble muni de la structure déterminée par une loi partout définie associative prend le nom de monoïde.

La loi opposée à une loi associative est évidemment associative.

Lorsque la loi $x \tau y$ n'est pas partout définie, on dit parfois qu'elle est associative si la loi de composition $X \tau Y$ qu'on en déduit (n° 1) entre parties de E , et qui, elle, est partout définie, est associative ; d'autres fois, on dit qu'elle est associative si la relation (2) est vérifiée chaque fois que les deux membres sont définis (cette deuxième condition est d'ailleurs une conséquence de la première). Une partie des résultats qui suivent s'étend, avec des modifications convenables, aux lois non partout définies et associatives (à l'un des deux sens précédents).

Exemples. — 1) Parmi les exemples de lois de composition indiqués au n° 1, les suivantes sont associatives : $X \cap Y$ et $X \cup Y$ (ex. 1) ; $x + y$ et xy (ex. 2) ; $X \circ Y$ et $f \circ g$ (ex. 4), $\sup(x, y)$ et $\inf(x, y)$ (ex. 6). Si $x \tau y$ est une loi associative entre éléments de E , $X \tau Y$ est une loi associative entre éléments de $\mathfrak{P}(E)$. En revanche, l'exponentiation des entiers naturels (ex. 2) n'est pas associative ; en effet, $(2^1)^2 \neq 2^{(1^2)}$.

2) *Monoïdes libres.* Soit A un ensemble, E l'ensemble des suites finies non vides d'éléments de A ; la relation « s et s' sont des suites finies semblables » (au sens du n° 2) entre deux éléments s, s' de E est, comme on le voit immédiatement, une relation d'équivalence

R dans E ; désignons par L(A) l'ensemble quotient E/R. On définit sur cet ensemble une loi de composition interne de la manière suivante :

Considérons deux éléments $s = (a_i)_{i \in I}$, $s' = (b_j)_{j \in J}$ de E, tels que les relations $i \in I$, $j \in J$ entraînent $i < j$; si on pose $K = I \cup J$, et, pour tout $k \in K$, $c_k = a_k$ si $k \in I$, $c_k = b_k$ si $k \in J$, la suite $s'' = (c_k)_{k \in K}$ est dite obtenue par *juxtaposition* de la suite s et de la suite s'. On vérifie immédiatement que si $s_1 \equiv s$ (mod. R), $s'_1 \equiv s'$ (mod. R), et si la juxtaposition de s_1 et s'_1 est définie, elle donne une suite $s''_1 \equiv s''$ (mod. R); la classe (mod. R) de s'' ne dépend donc que des classes de s et s'; on dit encore qu'elle est obtenue par *juxtaposition* de la classe de s et de celle de s', et on a bien ainsi une loi de composition dans L(A). Cette loi est *partout définie*, car si $s = (a_i)_{i \in I}$ et $s' = (b_j)_{j \in J}$ sont deux suites quelconques de E, il existe une suite s'_1 telle que $s'_1 \equiv s'$ (mod. R) et telle que la juxtaposition de s et s'_1 soit définie (si h est le plus grand élément de I, il suffit de considérer l'ensemble d'indices K formé des entiers $h+j+1$, où j parcourt J, et de prendre $s'_1 = (b_{k-h-1})_{k \in K}$). En outre, on vérifie aisément que cette loi est *associative*.

L'ensemble L(A), muni de cette loi de composition, prend le nom de *monoïde libre* déduit de A ; les éléments de L(A) sont appelés les *mots* formés avec les éléments de A. Dans tout mot (c'est-à-dire une classe mod. R), il existe une suite et une seule $(a_i)_{0 \leq i \leq n}$ dont l'ensemble d'indices est un intervalle $[0, n]$ de N ; on identifie souvent cette suite avec le mot dont elle fait partie ; le nombre de termes d'une suite quelconque appartenant à un mot est appelé la *longueur* du mot.

La principale propriété des lois associatives est le théorème suivant, qui donne tout son intérêt à la notion de composé d'une séquence, définie au n° 2 :

THÉORÈME 1 (théorème d'associativité). — *Soit A un ensemble fini non vide, totalement ordonné, réunion de parties non vides B_i ($1 \leq i \leq p$) telles que les relations $\alpha \in B_i$, $\beta \in B_j$, $1 \leq i < j \leq p$ entraînent $\alpha < \beta$; soit $(x_\alpha)_{\alpha \in A}$ une séquence d'éléments de E, ayant A pour ensemble d'indices ; pour toute loi associative τ donnée sur E, on a*

$$(3) \quad \sum_{\alpha \in A} x_\alpha = \sum_{1 \leq i \leq p} \left(\sum_{\alpha \in B_i} x_\alpha \right).$$

On va démontrer le théorème par récurrence sur le nombre n

des éléments de A. Si $n = 1$, les B_i étant non vides, on a nécessairement $p = 1$, et le théorème est évident. Sinon, le théorème étant supposé vrai pour un ensemble d'indices ayant moins de n éléments, distinguons deux cas :

a) B_1 a un seul élément β . Soit $C = B_2 \cup B_3 \cup \dots \cup B_p$. Le premier membre de (3) n'est autre (par définition) que $x_\beta \tau \left(\sum_{\alpha \in C} x_\alpha \right)$; le second membre n'est autre (par définition) que

$$x_\beta \tau \left(\sum_{2 \leq i \leq p} \left(\sum_{\alpha \in B_i} x_\alpha \right) \right);$$

l'égalité résulte de ce que le théorème est supposé vrai pour C et B_2, B_3, \dots, B_p .

b) Sinon, soit β le plus petit élément de A (donc de B_1) ; soit A' l'ensemble des éléments $> \beta$ dans A, et soit $B'_1 = A' \cap B_1$; A' a $n - 1$ éléments, et les conditions du théorème sont satisfaites par A' et ses parties B'_1, B_2, \dots, B_p ; donc, on a par hypothèse

$$\sum_{\alpha \in A'} x_\alpha = \left(\sum_{\alpha \in B'_1} x_\alpha \right) \tau \left(\sum_{2 \leq i \leq p} \left(\sum_{\alpha \in B_i} x_\alpha \right) \right).$$

Formons le composé de x_β et de chacun des deux membres : on aura au premier membre, par définition, $\sum_{\alpha \in A} x_\alpha$; au second, on obtient (en appliquant la définition d'une loi associative)

$$\left(x_\beta \tau \left(\sum_{\alpha \in B'_1} x_\alpha \right) \right) \tau \left(\sum_{2 \leq i \leq p} \left(\sum_{\alpha \in B_i} x_\alpha \right) \right)$$

ce qui n'est autre chose (d'après la déf. 4) que le second membre de la formule (3).

Un cas particulier du th. 1 est la formule

$$x_0 \tau x_1 \tau \dots \tau x_n = (x_0 \tau x_1 \tau \dots \tau x_{n-1}) \tau x_n$$

qui permet de définir le composé d'une suite finie par récurrence en procédant « de gauche à droite » (au lieu que la définition donnée ci-dessus procédait « de droite à gauche ») : les deux définitions sont donc équivalentes pour une loi associative.

Lorsque tous les termes d'une séquence de n termes sont égaux à un même élément $x \in E$, leur composé se notera $\tau^n x$ pour une loi notée τ , $\tau^1 x$ pour une loi notée τ , x^n pour une loi notée multiplicativement, et le plus souvent nx pour une loi notée additivement (sauf certains cas où cette dernière notation pourrait prêter à confusion ; voir § 3, n° 1). Le théorème d'associativité, appliqué à une séquence dont tous les termes sont égaux, donne la formule

$$\tau^{n_1 + n_2 + \dots + n_p} x = (\tau^{n_1} x) \tau (\tau^{n_2} x) \tau \dots \tau (\tau^{n_p} x)$$

donc, en particulier, si $p = 2$,

$$(4) \quad \tau^{m+n} x = (\tau^m x) \tau (\tau^n x)$$

et, si $n_1 = n_2 = \dots = n_p = m$,

$$(5) \quad \tau^{pm} x = \tau^p (\tau^m x).$$

Si X est une partie de E , on désignera, conformément aux notations ci-dessus, par $\tau^p X$ l'ensemble $X_1 \tau X_2 \tau \dots \tau X_p$ où

$$X_1 = X_2 = \dots = X_p = X;$$

c'est donc l'ensemble de tous les composés $x_1 \tau x_2 \tau \dots \tau x_p$, pour $x_1 \in X, x_2 \in X, \dots, x_p \in X$.

N

Il importe de ne pas confondre cet ensemble avec l'ensemble des $\tau^p x$, où x parcourt X .

On posera $\tau^\infty X = \bigcup_{p>0} (\tau^p X)$: c'est l'ensemble des composés de toutes les suites finies dont tous les termes appartiennent à X ; pour une loi associative on a $X \tau (\tau^\infty X) = (\tau^\infty X) \tau X \subset \tau^\infty X$.

4. Parties stables. Lois induites.

DÉFINITION 5. — Une partie A d'un ensemble E est dite stable pour une loi de composition entre éléments de E si le composé de deux éléments de A appartient à A chaque fois qu'il est défini.

Autrement dit, pour que A soit stable pour une loi τ , il faut et il suffit que $A \tau A \subset A$.

L'intersection d'une famille de parties stables de E est évidem-

ment stable, donc en particulier il existe une plus petite partie stable Z de E contenant une partie X donnée (Ens. R, § 6, n° 5), qui est dite engendrée par X ; il est immédiat, par récurrence sur n , que le composé de toute séquence de n termes appartenant à X appartient à Z , autrement dit on a toujours $\tau^n X \subset Z$. En outre :

THÉORÈME 2. — Pour une loi associative τ sur E , la partie stable engendrée par une partie X de E est $\tau^\infty X$.

Il suffit de voir que $\tau^\infty X$ est stable si τ est associative ; or, si u et v sont deux éléments de $\tau^\infty X$, ils sont de la forme $u = x_0 \tau x_1 \tau \dots \tau x_{n-1}$, $v = x_n \tau x_{n+1} \tau \dots \tau x_{n+p}$ avec $x_i \in X$ pour $0 \leq i \leq n+p$; donc (th. 1) $u \tau v = x_0 \tau x_1 \tau \dots \tau x_{n+p}$ appartient à $\tau^\infty X$.

Exemples. — 1) Dans l'ensemble des entiers naturels \mathbb{N} , la partie stable pour l'addition engendrée par l'ensemble formé du seul nombre 1 est l'ensemble des entiers ≥ 1 ; pour la multiplication, l'ensemble $\{1\}$ est stable.

2) Étant donnée une loi partout définie τ entre éléments d'un ensemble E , pour qu'une partie $\{h\}$ réduite à un seul élément soit stable pour la loi τ , il faut et il suffit que $h \tau h = h$; on dit alors que h est idempotent. Par exemple, tout élément d'un ensemble ordonné réticulé est idempotent pour chacune des lois sup(x, y) et inf(x, y).

3) Pour une loi associative τ sur un ensemble E , la partie stable engendrée par un ensemble $\{a\}$ réduit à un seul élément est l'ensemble des éléments $\tau^n a$, où n parcourt l'ensemble des entiers > 0 .

4) D'après les définitions de l'exemple 2 du n° 3, il est clair que toute suite finie $(x_i)_{i \in I}$ d'éléments de A est la juxtaposition des suites à un seul terme $(x_k)_{k=i}$ pour $i \in I$; le monoïde libre $L(A)$ est donc engendré par l'ensemble des mots de longueur 1, qui est équivalent à A et qu'on identifie d'ordinaire à A .

Si τ est une loi de composition partout définie sur E , et F une partie stable de E pour cette loi, la restriction de la fonction $x \tau y$ à $F \times F$ est une loi de composition partout définie sur F ; on dit que c'est la loi induite sur F par la loi τ . Plus généralement :

DÉFINITION 6. — Soit τ une loi de composition entre éléments de E , définie sur une partie A de $E \times E$; on appelle loi induite par la loi τ sur une partie F de E , la loi de composition entre élé-

ments de F , définie sur l'ensemble des $(x, y) \in F \times F$ tels que $(x, y) \in A$ et $x \tau y \in F$, et qui à un tel couple (x, y) fait correspondre le composé $x \tau y$. La structure déterminée par cette loi sur F sera dite induite sur F par la structure déterminée par τ sur E .

La loi induite par τ sur F pourra (par abus de langage) être désignée par le même signe τ , quand cette notation ne prêtera pas à confusion.

Sur une partie stable pour une loi associative τ , la loi induite par τ est associative.

5. Éléments permutables. Lois commutatives.

DÉFINITION 7. — *Etant donnée une loi de composition τ entre éléments d'un ensemble E , deux éléments x, y de E sont dits permutables (ou échangeables) pour la loi τ , si $x \tau y$ et $y \tau x$ sont définis et si $x \tau y = y \tau x$.*

DÉFINITION 8. — *Une loi de composition τ entre éléments de E est dite commutative si, pour tout couple (x, y) d'éléments de E tels que $x \tau y$ soit défini, x et y sont permutables.*

Une loi commutative est identique à son opposée.

Exemples. — 1) L'addition et la multiplication des entiers naturels sont des lois commutatives.

2) Dans un ensemble ordonné réticulé, les lois $\sup(x, y)$ et $\inf(x, y)$ sont commutatives : il en est ainsi, en particulier, des lois \cup et \cap entre parties d'un ensemble E .

3) La loi de composition $(X, Y) \rightarrow X \circ Y$ entre parties de $E \times E$ n'est pas commutative (si E a plus d'un élément) : car si $A = \{(a, b)\}$, $B = \{(b, c)\}$ et $a \neq c$, on a $B \circ A = \{(a, c)\}$ et $A \circ B = \emptyset$. Mais la diagonale Δ de $E \times E$ est permutable avec toute partie de $E \times E$. De même, la loi $f \circ g$ entre applications de E dans E n'est pas commutative (si E a plus d'un élément) comme on voit en prenant pour f et g des applications constantes distinctes, mais l'application identique est permutable avec toute application.

4) Si $x \tau y$ est une loi commutative entre éléments de E , $X \tau Y$ est une loi commutative entre parties de E .

PROPOSITION 1. — *Si un élément x est permutable avec chacun des éléments y et z , pour une loi associative τ , il est permutable avec $y \tau z$.*

En effet, $x \tau (y \tau z)$ s'écrit successivement

$$x \tau (y \tau z) = (x \tau y) \tau z = (y \tau x) \tau z = y \tau (x \tau z) = y \tau (z \tau x) = (y \tau z) \tau x.$$

PROPOSITION 2. — *Si, pour une loi associative τ , tout élément d'une partie X de E est permutable avec tout élément d'une partie Y de E , tout élément de la partie stable engendrée par X est permutable avec tout élément de la partie stable engendrée par Y .*

En effet, il suit de la proposition 1, par récurrence sur n , que si x est permutable avec chacun des termes d'une suite de n termes, il l'est avec le composé de la suite ; donc (th. 2) tout $x \in X$ est permutable avec tout élément de la partie stable Y' engendrée par Y ; il s'ensuit alors, par le même raisonnement, que tout élément de Y' est permutable avec tout élément de la partie stable X' engendrée par X .

Deux cas particuliers de la prop. 2 sont à noter : celui où $X = \{x\}$, $Y = \{y\}$, et celui où $X = Y$:

COROLLAIRE 1. — *Si x et y sont permutables pour la loi associative τ , il en est de même de ${}^m x$ et ${}^n y$, quels que soient les entiers $m > 0$ et $n > 0$; en particulier, ${}^m x$ et ${}^n x$ sont permutables quels que soient x et les entiers $m > 0, n > 0$.*

COROLLAIRE 2. — *Si tous les éléments d'une partie X sont permutables deux à deux pour une loi associative τ , la loi induite par τ sur la partie stable engendrée par X est associative et commutative.*

DÉFINITION 9. — *On appelle élément central de E , pour une loi de composition entre éléments de E , tout élément permutable avec tous les éléments de E . On appelle centre de E l'ensemble des éléments centraux.*

Il résulte de la prop. 1 que, pour une loi associative, le centre E est une partie stable de E ; la loi induite sur le centre est évidemment commutative.

La principale propriété des lois à la fois associatives et commutatives consiste en ce que les composés de toutes les suites ne différant d'une suite finie donnée que par l'ordre des termes, ont même valeur : ce qu'on va maintenant démontrer.

THÉORÈME 3 (théorème de commutativité). — Soit τ une loi de composition associative et commutative sur E ; soit $(x_\alpha)_{\alpha \in A}$ une famille finie non vide d'éléments de E ; quelle que soit la manière dont on ordonne totalement A , le composé $\prod_{\alpha \in A} x_\alpha$ a la même valeur.

Le théorème est vrai si A a un seul élément β , le composé étant alors x_β . Montrons par récurrence sur p qu'il est vrai pour toute partie de A à p éléments : il suffira de montrer qu'il est vrai pour un ensemble d'indices à p éléments s'il est vrai pour toute partie de cet ensemble à moins de p éléments. Soit donc A un ensemble à p éléments, $i \rightarrow \alpha_i$ une application biunivoque de l'intervalle $[0, p-1]$ de N sur A ; on ordonne totalement A en transportant l'ordre de l'intervalle $[0, p-1]$ par cette application, et le composé de la séquence $(x_\alpha)_{\alpha \in A}$ définie par cette relation d'ordre n'est autre que $\prod_{i=0}^{p-1} x_{\alpha_i}$.

Ordonnons totalement A d'une autre manière, et soit α_h le plus petit élément de A pour cet ordre, A' l'ensemble des autres éléments de A (totalement ordonné par l'ordre induit). Supposons d'abord $0 < h < p-1$, et posons $B = \{\alpha_0, \alpha_1, \dots, \alpha_{h-1}\}$, et $C = \{\alpha_{h+1}, \dots, \alpha_{p-1}\}$; le théorème étant supposé vrai pour A' , on a, en appliquant de plus le théorème d'associativité (puisque $A' = B \cup C$)

$$\prod_{\alpha \in A'} x_\alpha = \left(\prod_{i=0}^{h-1} x_{\alpha_i} \right) \tau \left(\prod_{i=h+1}^{p-1} x_{\alpha_i} \right)$$

d'où, en composant x_{α_h} avec les deux membres, et par application répétée de la commutativité et de l'associativité de τ :

$$\begin{aligned} \prod_{\alpha \in A} x_\alpha &= x_{\alpha_h} \tau \left(\prod_{\alpha \in A'} x_\alpha \right) = x_{\alpha_h} \tau \left(\prod_{i=0}^{h-1} x_{\alpha_i} \right) \tau \left(\prod_{i=h+1}^{p-1} x_{\alpha_i} \right) \\ &= \left(\prod_{i=0}^{h-1} x_{\alpha_i} \right) \tau x_{\alpha_h} \tau \left(\prod_{i=h+1}^{p-1} x_{\alpha_i} \right) = \prod_{i=0}^{p-1} x_{\alpha_i}, \end{aligned}$$

ce qui démontre le théorème dans ce cas. Si $h = 0$ ou $h = p-1$, on trouve le même résultat mais d'une manière plus simple, les termes relatifs à B ou bien les termes relatifs à C disparaissant des formules.

Pour une loi associative et commutative sur un ensemble E , le composé d'une famille finie $(x_\alpha)_{\alpha \in A}$ d'éléments de E sera par définition la valeur commune des composés de toutes les séquences obtenues en ordonnant totalement A de toutes les manières possibles.

Ce composé se notera encore $\prod_{\alpha \in A} x_\alpha$ pour une loi notée τ ; de même pour les autres notations.

Les th. 1 et 3 se combinent pour donner le suivant :

THÉORÈME 4. — Soient τ une loi associative et commutative sur E , $(x_\alpha)_{\alpha \in A}$ une famille finie non vide d'éléments de E . Si A est réunion de parties non vides B_1, B_2, \dots, B_p , deux à deux sans élément commun, on a

$$(6) \quad \prod_{\alpha \in A} x_\alpha = \prod_{i=1}^p \left(\prod_{\alpha \in B_i} x_\alpha \right).$$

En effet, cela résulte du th. 3 si on ordonne totalement A de façon que les B_i satisfassent aux conditions du th. 1.

Signalons deux cas particuliers importants de ce théorème. En premier lieu, si $(x_{\alpha\beta})_{(\alpha, \beta) \in A \times B}$ est une famille finie dont l'ensemble d'indices est le produit de deux ensembles finis non vides A, B (« famille double »), on a

$$(7) \quad \prod_{(\alpha, \beta) \in A \times B} x_{\alpha\beta} = \prod_{\alpha \in A} \left(\prod_{\beta \in B} x_{\alpha\beta} \right) = \prod_{\beta \in B} \left(\prod_{\alpha \in A} x_{\alpha\beta} \right)$$

comme il résulte du th. 4 en considérant $A \times B$ comme réunion des ensembles $\{\alpha\} \times B$ d'une part, des ensembles $A \times \{\beta\}$ de l'autre.

En particulier, si B a n éléments, et si, pour chaque $\alpha \in A$, tous les $x_{\alpha\beta}$ ont une même valeur x_α , on a

$$(8) \quad \prod_{\alpha \in A} \left(\prod_{\beta=1}^n x_\alpha \right) = \prod_{\alpha \in A} x_\alpha.$$

En raison de la formule (7), le composé d'une suite double (x_{ij}) dont l'ensemble d'indices est le produit de deux intervalles $[p, q]$ et $[r, s]$ de \mathbb{N} , se note souvent, pour une loi associative et commutative écrite additivement

$$\sum_{i=p}^q \sum_{j=r}^s x_{ij} \quad \text{ou} \quad \sum_{j=r}^s \sum_{i=p}^q x_{ij}$$

et de même pour les lois notées par d'autres signes.

En second lieu, soit A l'ensemble des couples d'entiers (i, j) tels que $0 \leq i \leq n$, $0 \leq j \leq n$ et $i < j$; le composé d'une famille $(x_{ij})_{(i,j) \in A}$ (pour une loi associative et commutative), se notera

encore $\prod_{0 \leq i < j \leq n} x_{ij}$ (ou simplement $\prod_{i < j} x_{ij}$ si aucune confusion n'en résulte); le th. 4 donne ici les formules

$$(9) \quad \prod_{0 \leq i < j \leq n} x_{ij} = \prod_{i=0}^{n-1} \left(\prod_{j=i+1}^n x_{ij} \right) = \prod_{j=1}^n \left(\prod_{i=0}^{j-1} x_{ij} \right).$$

On a des formules analogues à (7) pour une famille dont l'ensemble d'indices est le produit de plus de deux ensembles, des formules analogues à (9) pour une famille dont l'ensemble d'indices est l'ensemble S_p des suites strictement croissantes $(i_k)_{1 \leq k \leq p}$ de p entiers tels que $0 \leq i_k \leq n$ ($p \leq n + 1$): dans ce dernier cas, le composé de la famille $(x_{i_1 i_2 \dots i_p})_{(i_1, \dots, i_p) \in S_p}$ se note

$$\prod_{0 \leq i_1 < i_2 < \dots < i_p \leq n} x_{i_1 i_2 \dots i_p}, \text{ ou simplement } \prod_{i_1 < i_2 < \dots < i_p} x_{i_1 i_2 \dots i_p}.$$

Signalons enfin que, d'après le corollaire 2 de la prop. 2, les th. 3 et 4 s'appliquent encore s'il s'agit d'une loi associative et de familles d'éléments deux à deux permutable pour cette loi.

Exercices. — 1) Soit τ une loi de composition (partout définie ou non) sur un ensemble E . Si $(X_\alpha)_{\alpha \in A}$ et $(Y_\beta)_{\beta \in B}$ sont deux familles quelconques de parties de E , on a

$$\left(\bigcup_{\alpha \in A} X_\alpha \right) \tau \left(\bigcup_{\beta \in B} Y_\beta \right) = \bigcup_{(\alpha, \beta) \in A \times B} (X_\alpha \tau Y_\beta).$$

2) Soit τ une loi de composition non partout définie sur un ensemble E . Soit E' la partie de $\mathfrak{P}(E)$ formée des ensembles $\{x\}$, où x parcourt E , et de la partie vide \emptyset de E ; montrer que E' est une partie stable de $\mathfrak{P}(E)$ pour la loi $X \tau Y$; en déduire que, si \bar{E} désigne l'ensemble obtenu par adjonction (Ens. R, § 4, no 5) à E d'un élément ω , on peut prolonger à $\bar{E} \times \bar{E}$ la loi τ , de sorte que la loi τ soit identique à la loi induite sur E par cette loi prolongée.

3) Soit τ une loi de composition non partout définie sur E .

a) Pour que la loi $X \tau Y$ entre parties de E soit associative, il faut et il suffit que, quels que soient $x \in E$, $y \in E$, $z \in E$, si l'un des deux membres de la formule (2) est défini, l'autre soit défini et lui soit égal (utiliser l'exerc. 1 pour montrer que la condition est suffisante).

b) Si cette condition est satisfaite, montrer que le th. 1 se généralise comme suit : si l'un des deux membres de la formule (3) est défini, l'autre est défini et lui est égal.

4) a) Etant donné un ensemble E , soit Φ l'ensemble des applications dans E d'une partie quelconque de E ; si f, g, h sont trois éléments de Φ , montrer que si le composé $(f \circ g) \circ h$ est défini, il en est de même de $f \circ (g \circ h)$, mais que la réciproque est inexacte ; si ces deux composés sont définis, ils sont égaux.

b) Soit \mathfrak{F} une famille de parties non vides de E , sans élément commun deux à deux, et soit Ψ le sous-ensemble de Φ formé des applications biunivoques d'un ensemble de \mathfrak{F} sur un ensemble de \mathfrak{F} . Montrer que, pour la loi induite par la loi $f \circ g$ sur Ψ , la condition de l'exerc. 3a) est satisfaite.

5) Montrer que les seuls triplets (m, n, p) d'entiers naturels $\neq 0$, tels que $(m^n)^p = m^{np}$ sont : $(1, n, p)$, n et p étant quelconques ; $(m, 1, 1)$ et $(m, 2, 2)$ où m est quelconque.

6) Soit τ une loi de composition partout définie entre éléments d'un ensemble E ; soit A la partie de E formée des éléments x tels que $x \tau (y \tau z) = (x \tau y) \tau z$ quels que soient $y \in E$, $z \in E$; montrer que A est une partie stable de E et que la loi induite sur A par τ est associative.

7) Si τ est une loi associative sur E , a et b deux éléments de E , les ensembles $\{a\} \tau E$, $E \tau \{b\}$, $\{a\} \tau E \tau \{b\}$, $E \tau \{a\} \tau E$, sont des parties stables de E pour la loi τ .

8) Soit τ une loi associative sur E , a un élément de E ; quels que soient $x \in E$, $y \in E$, on pose $x \perp y = x \tau a \tau y$; montrer que la loi \perp est associative.

9) Sur un ensemble E , les applications $(x, y) \rightarrow x$ et $(x, y) \rightarrow y$ sont des lois de composition associatives opposées.

10) Soient X et Y deux parties quelconques d'un ensemble E ; on pose $X \tau Y = X \cup Y$ si $X \cap Y = \emptyset$, $X \tau Y = E$ si $X \cap Y \neq \emptyset$;

montrer que la loi de composition ainsi définie sur $\mathfrak{P}(E)$ est associative et commutative.

11) Soit τ une loi associative sur E , A et B deux parties de E stables pour cette loi ; montrer que si $B \tau A \subset A \tau B$, $A \tau B$ est une partie stable de E .

12) Les seuls entiers naturels distincts $\neq 0$ qui sont permutable pour la loi $(x, y) \rightarrow xy$ sont 2 et 4.

13) Montrer que, pour la loi $X \circ Y$ entre parties de $E \times E$, le centre est l'ensemble des parties de la diagonale Δ .

14) Montrer que, pour la loi de composition $f \circ g$ entre applications de E dans E , le centre est réduit à l'application identique.

15) On dit qu'une loi τ sur un ensemble E est *idempotente* si tous les éléments de E sont idempotents (n° 4) pour cette loi, c'est-à-dire si $x \tau x = x$ pour tout $x \in E$. Montrer que, si une loi τ sur E est associative, commutative et idempotente, la relation $x \tau y = y$ est une relation d'ordre dans E ; si on l'écrit $x \leqslant y$, deux éléments quelconques x, y de E admettent une borne supérieure (pour cette relation d'ordre) égale à $x \tau y$. Réciproque.

16) Soit E un monoïde (n° 3), X une partie non vide de E , A la partie stable de E engendrée par X . Si, à tout mot $u = (a_i)_{0 \leqslant i \leqslant n}$ du monoïde libre $L(X)$ déduit de X , on fait correspondre le composé $f(u)$ de la suite (a_i) dans E , montrer que l'application f ainsi définie est une représentation (n° 1) de $L(X)$ sur A .

§ 2. — Élément neutre ; éléments réguliers ; éléments symétriques.

1. Élément neutre.

DÉFINITION 1. — Pour une loi de composition τ entre éléments d'un ensemble E , un élément e de E est dit élément neutre si $e \tau x$ et $x \tau e$ sont définis et égaux à x , pour tout $x \in E$.

Il existe au plus un élément neutre pour une loi donnée τ , car si e et e' sont éléments neutres, on a $e = e \tau e' = e'$. L'élément neutre, s'il existe, est permutable avec tout élément : c'est un élément central.

Exemples. — 1) Dans l'ensemble des parties d'un ensemble E , \emptyset est élément neutre pour la loi \cup , E pour la loi \cap . Plus généralement, dans un ensemble ordonné réticulé, le plus petit élément, s'il existe, est élément neutre pour la loi $\sup(x, y)$; réciproquement, s'il existe un élément neutre pour cette loi, il est le plus petit élément de l'ensemble.

n° 1 ÉLÉMENTS NEUTRE, RÉGULIERS, SYMÉTRIQUES

De même pour le plus grand élément et la loi $\inf(x, y)$.

2) Le nombre 0 est élément neutre pour l'addition des entiers naturels, le nombre 1 pour la multiplication de ces entiers. La loi $(x, y) \rightarrow xy$ n'a pas d'élément neutre.

3) Pour la loi $X \circ Y$ entre parties de $E \times E$, la diagonale Δ est l'élément neutre. Pour la loi $f \circ g$ entre applications de E dans E , l'application identique de E sur E est l'élément neutre.

4) Si e est élément neutre pour une loi τ entre éléments de E , $\{e\}$ est élément neutre pour la loi $(X, Y) \rightarrow X \tau Y$ entre parties de E .

S'il existe un élément neutre e pour une loi τ sur un ensemble E , et si F est une partie de E qui contienne e , e est élément neutre pour la loi induite par τ sur F . Mais il peut se faire que la loi induite par τ sur une partie F ait un élément neutre e' , sans que F contienne e , ou même sans qu'il existe d'élément neutre pour la loi τ sur E .

Par exemple, si τ est associative sur E , et si $h \in E$ est *idempotent* pour la loi τ (§ 1, n° 4) h est élément neutre pour la loi induite par τ sur la partie stable formée des éléments $h \tau x \tau h$, où x parcourt E ; il pourra en être ainsi sans que h soit élément neutre pour τ dans E . En particulier, si τ est la loi $\sup(x, y)$ sur un ensemble ordonné réticulé E , on pourra prendre pour h un élément quelconque de E .

Soient E et F deux ensembles munis chacun d'une loi de composition interne notée τ ; si f est une représentation de E dans F , et si la loi τ sur E admet un élément neutre e , $f(e)$ est élément neutre pour la loi induite par celle de F sur $f(E)$.

DÉFINITION 2. — Si e est élément neutre pour une loi de composition associative entre éléments de E , on appellera composé d'une famille vide d'éléments de E l'élément neutre e .

Si donc \emptyset est la partie vide d'un ensemble d'indices, on écrira dans les conditions de la déf. 2, $\prod_{x \in \emptyset} x = e$; on posera de même $\tau^{\emptyset} x = e$ quel que soit x . Avec ces définitions, les théorèmes 1 et 4 du § 1 restent vrais même si on y supprime l'hypothèse que les ensembles A et B_i sont non vides. De même, les formules $\tau^{m+n} x = (\tau^m x) \tau (\tau^n x)$ et $\tau^{mn} x = \tau^m (\tau^n x)$ sont vraies alors pour $m \geqslant 0, n \geqslant 0$

L'élément neutre, pour une loi notée *additivement*, se notera 0 et s'appellera *zéro* ou *origine* chaque fois que cette notation ne risquera pas d'entrainer confusion (par exemple avec l'entier naturel 0) ; pour une loi notée *multiplicativement*, il se notera 1 et s'appellera *élément unité* (ou *unité*), sous la même réserve.

2. Eléments réguliers.

DÉFINITION 3. — *Etant donnée une loi de composition τ , partout définie, entre éléments de E, on appelle translation à gauche (resp. translation à droite) correspondant à un élément $a \in E$, l'application $x \rightarrow a \tau x$ (resp. $x \rightarrow x \tau a$) de E dans lui-même.*

Les qualificatifs « à gauche » et « à droite » ont leur origine dans la notation habituelle de la plupart des lois de composition. Par passage à la loi opposée, les translations à gauche deviennent translations à droite et réciproquement.

On notera éventuellement γ_a , δ_a les translations à gauche et à droite correspondant à $a \in E$, c'est-à-dire qu'on aura

$$\gamma_a(x) = a \tau x, \quad \delta_a(x) = x \tau a.$$

PROPOSITION 1. — *Pour une loi associative τ , la translation à gauche $\gamma_{x \tau y}$ correspondant au composé de x et de y est l'application $\gamma_x \circ \gamma_y$ composée des translations γ_x, γ_y ; la translation à droite $\delta_{x \tau y}$ est l'application $\delta_y \circ \delta_x$, composée de δ_y, δ_x .*

En effet :

$$\begin{aligned} \gamma_{x \tau y}(z) &= (x \tau y) \tau z = x \tau (y \tau z) = \gamma_x(\gamma_y(z)) \\ \delta_{x \tau y}(z) &= z \tau (x \tau y) = (z \tau x) \tau y = \delta_y(\delta_x(z)). \end{aligned}$$

Autrement dit, l'application $x \rightarrow \gamma_x$ est une *représentation* de l'ensemble E (muni de la loi τ) dans l'ensemble E^{τ} des applications de E dans lui-même, muni de la loi $f \circ g$; l'application $x \rightarrow \delta_x$ est une représentation de E dans l'ensemble E^{τ} , muni de la loi opposée à la loi $f \circ g$.

DÉFINITION 4. — *Etant donnée une loi de composition τ , partout définie, entre éléments d'un ensemble E, un élément $a \in E$ est dit régulier pour la loi τ si les translations à droite et à gauche correspondant à a sont des applications biunivoques de E dans lui-même.*

Autrement dit, pour que a soit régulier, il faut et il suffit que chacune des relations $a \tau x = a \tau y, x \tau a = y \tau a$, entraîne $x = y$ (on dit qu'on peut « simplifier par a » ces égalités). S'il existe un élément neutre e pour la loi τ , il est régulier pour cette loi : les translations γ_e et δ_e sont alors l'application identique de E sur lui-même.

Si X et Y sont des parties de E, et a un élément régulier de E, chacune des relations $\{a\} \tau X = \{a\} \tau Y, X \tau \{a\} = Y \tau \{a\}$ entraîne $X = Y$.

Par contre, même si tous les éléments d'une partie A de E sont réguliers, la relation $A \tau X = A \tau Y$ (ou la relation $X \tau A = Y \tau A$) n'entraîne pas en général $X = Y$.

Exemples. — 1) Tout entier naturel est régulier pour l'addition ; tout entier naturel $\neq 0$ est régulier pour la multiplication ; tout entier naturel autre que 0 et 1 est régulier pour l'exponentiation.

2) Dans un ensemble ordonné réticulé, il ne peut y avoir d'autre élément régulier pour la loi $\sup(x, y)$ que l'élément neutre (plus petit élément) s'il existe ; de même pour $\inf(x, y)$. En particulier, dans l'ensemble des parties d'un ensemble E, Ø est le seul élément régulier pour la loi \cup , E le seul élément régulier pour la loi \cap .

PROPOSITION 2. — *L'ensemble des éléments réguliers pour une loi associative est stable pour cette loi.*

En effet, si γ_y et γ_x sont biunivoques, il en est de même de $\gamma_{x \tau y} = \gamma_x \circ \gamma_y$ (prop. 1). De même pour $\delta_{x \tau y}$.

Si un élément x est régulier pour une loi τ , il l'est aussi pour la loi induite par τ sur toute partie stable A contenant x (mais un élément de A peut être régulier dans A et ne pas l'être dans E) ; en particulier, pour la loi induite par une loi associative τ sur l'ensemble R des éléments réguliers de E, *tous les éléments de R sont réguliers*.

3. Eléments symétriques.

DÉFINITION 5. — *Etant donnée une loi de composition τ entre éléments d'un ensemble E, admettant un élément neutre e, on dit qu'un élément x' est symétrique d'un élément x si $x \tau x' = x' \tau x = e$; on dit qu'un élément x est symétrisable s'il existe un élément symétrique de x.*

Exemples. — 1) L'élément neutre, s'il existe, est son propre symétrique. Il peut arriver qu'il n'existe pas d'autre élément symétrisable dans E : c'est le cas pour l'addition et la multiplication dans \mathbb{N} ; c'est le cas aussi pour la loi $\sup(x, y)$ dans un ensemble réticulé.

2) Dans l'ensemble des applications de E dans E , les éléments symétrisables, pour la loi $f \circ g$, sont les applications *biunivoques* de E sur E (*Ens. R*, § 2, n° 12) ; pour une telle application f , l'application réciproque de f est symétrique de f .

Soient E et F deux ensembles munis chacun d'une loi interne notée τ , et f une représentation de E dans F ; si x et x' sont symétriques dans E , $f(x)$ et $f(x')$ sont symétriques dans $f(E)$.

PROPOSITION 3. — Pour une loi associative τ sur E , tout élément symétrisable x est régulier et admet un seul symétrique ; les translations à gauche et à droite correspondantes γ_x et δ_x sont des applications biunivoques de E sur E .

Soit x' un élément symétrique de x ; si $x \tau y = x \tau z$, on aura $x' \tau (x \tau y) = x' \tau (x \tau z)$, ou (par l'associativité) $e \tau y = e \tau z$, c'est-à-dire $y = z$. De même, si $y \tau x = z \tau x$, on a $(y \tau x) \tau x' = (z \tau x) \tau x'$ d'où $y = z$; donc x est régulier. Si x'' est symétrique de x , on a $x \tau x' = x \tau x'' = e$, donc $x' = x''$: le symétrique de x est unique. Enfin, γ_x est une application de E sur E : autrement dit, quel que soit $y \in E$, il existe z tel que $\gamma_x(z) = y$; car, si $z = x' \tau y$, on a $\gamma_x(z) = x \tau (x' \tau y) = e \tau y = y$; de même pour δ_x .

La prop. 3 admet la réciproque suivante :

PROPOSITION 4. — Etant donnée une loi associative τ sur E , si $x \in E$ est tel que les translations à gauche et à droite γ_x et δ_x soient toutes deux des applications de E sur E , il existe un élément neutre pour τ , et x est symétrisable.

On a $\gamma_x(E) = E$, donc il existe $e \in E$ tel que $\gamma_x(e) = x$, ou $x \tau e = x$; on a $\delta_x(E) = E$, donc, pour tout $y \in E$, il existe $z \in E$ tel que $z \tau x = y$; on a donc $y \tau e = z \tau x \tau e = z \tau x = y$. On voit de même (en échangeant les rôles de γ_x et δ_x) qu'il existe e' tel que $e' \tau y = y$ pour tout y . Mais alors on a d'une part $e' \tau e = e'$, de l'autre $e' \tau e = e$, donc $e = e'$, $y \tau e = e \tau y = y$ quel que soit y ; e est élément neutre. Il existe alors x' et x'' tels que $x \tau x' = e$,

$x'' \tau x = e$; donc $x'' \tau (x \tau x') = x''$, $(x'' \tau x) \tau x' = x'$, d'où $x' = x''$, et x' est symétrique de x .

PROPOSITION 5. — Si, pour une loi associative τ , x' et y' sont symétriques de x et y respectivement, $y' \tau x'$ est symétrique de $x \tau y$.

Cela résulte de la relation $(y' \tau x') \tau (x \tau y) = y' \tau (x' \tau x) \tau y = y' \tau y = e$, et du calcul analogue pour $(x \tau y) \tau (y' \tau x')$.

COROLLAIRE 1. — Etant donnée une loi associative τ sur E , si chacun des éléments x_α d'une séquence $(x_\alpha)_{\alpha \in A}$ d'éléments de E a un symétrique x'_α , le composé $\prod_{\alpha \in A} x_\alpha$ a pour symétrique $\prod_{\alpha \in A'} x'_\alpha$, où A' est l'ensemble totalement ordonné déduit de A en remplaçant l'ordre de A par l'ordre opposé.

On déduit ce corollaire de la prop. 5 en raisonnant par récurrence sur le nombre d'éléments de A .

En particulier, si x et x' sont symétriques, $\tau^n x$ et $\tau^n x'$ sont symétriques, pour tout entier $n \geq 0$.

COROLLAIRE 2. — Pour une loi associative, l'ensemble des éléments symétrisables est stable.

PROPOSITION 6. — Si, pour une loi associative, x et x' sont symétriques, et si x est permutable avec y , il en est de même de x' .

En effet, de $x \tau y = y \tau x$, on tire $x' \tau (x \tau y) \tau x' = x' \tau (y \tau x) \tau x'$ puis $(x' \tau x) \tau (y \tau x') = (x' \tau y) \tau (x \tau x')$, c'est-à-dire $y \tau x' = x' \tau y$.

COROLLAIRE. — Pour une loi associative, le symétrique de tout élément central symétrisable est un élément central.

De la prop. 6, on déduit aussi que la prop. 2 du § 1 peut, lorsqu'il existe un élément neutre, être remplacée par le résultat plus complet suivant :

PROPOSITION 7. — Soit τ une loi associative entre éléments de E , admettant un élément neutre e ; soient X et Y deux parties de E , X'' (resp. Y'') la partie stable de E engendrée par la réunion de X (resp. Y), de $\{e\}$, et de l'ensemble des symétriques des éléments symétrisables de E .

trisables de X (resp. Y). Alors, si tout élément de X est permutable avec tout élément de Y , tout élément de X'' est permutable avec tout élément de Y'' .

4. Symétrisation d'une loi associative et commutative.

Un élément $x \in E$, symétrisable pour une loi associative τ , est régulier pour la loi induite par τ sur toute partie stable de E contenant x . On peut se demander, réciproquement, si, étant donnée une loi associative τ sur un ensemble E , on peut « plonger » E dans un ensemble plus étendu \bar{E} et définir sur \bar{E} une loi de composition qui induise la loi τ sur E , et pour laquelle *tout élément régulier de E soit symétrisable*. Il n'en est pas toujours ainsi (*), mais nous allons voir que le problème admet une solution lorsque la loi τ est commutative.

Plaçons-nous dans ce cas, et désignons par E^* l'ensemble des éléments réguliers de E . Ecartons d'abord le cas sans intérêt où E^* est vide : la question est alors trivialement résolue en prenant pour \bar{E} l'ensemble E lui-même. En supposant désormais $E^* \neq \emptyset$, il s'agit, de façon précise, de définir un ensemble \bar{E} , une loi associative et commutative $\bar{\tau}$ sur \bar{E} , et un isomorphisme f de E sur une partie stable A de \bar{E} (A étant muni de la loi induite par $\bar{\tau}$), de sorte que :

- 1° \bar{E} possède un élément neutre pour la loi $\bar{\tau}$;
- 2° Pour tout élément régulier $x \in E^*$, $f(x)$ soit symétrisable dans \bar{E} .

Supposons d'abord le problème résolu ; soit $A^* = f(E^*)$, et soit A' l'ensemble des symétriques des éléments de A^* . Les ensembles A et A' sont stables pour $\bar{\tau}$, donc il en est de même de $A \bar{\tau} A'$, car $(A \bar{\tau} A') \bar{\tau} (A \bar{\tau} A') = (A \bar{\tau} A) \bar{\tau} (A' \bar{\tau} A') \subset A \bar{\tau} A'$, d'après la commutativité et l'associativité de $\bar{\tau}$. L'ensemble $A \bar{\tau} A'$ contient l'élément neutre de \bar{E} ; il contient A^* , car si $y \in A^*$, et si y' est symétrique de y , on a $y = y \bar{\tau} (y \bar{\tau} y') = (y \bar{\tau} y) \bar{\tau} y' \in A \bar{\tau} A'$; il contient aussi A' , car, avec les mêmes notations, on a

$$y' = (y \bar{\tau} y') \bar{\tau} y' = y \bar{\tau} (y' \bar{\tau} y') \in A \bar{\tau} A'.$$

Ainsi, l'ensemble $A \bar{\tau} A'$, muni de la loi induite par $\bar{\tau}$, satisfait

(*) Voir A. MALCEV, On the immersion of an algebraic ring into a field, *Math. Ann.*, t. CXIII (1936), p. 686.

à toutes les conditions du problème. Donc, si le problème est possible, nous pouvons astreindre \bar{E} à la condition supplémentaire :

3° \bar{E} est engendré par la réunion de l'ensemble $A = f(E)$, et de l'ensemble A' des symétriques des images par f des éléments réguliers de E .

Nous allons voir que les conditions 1°, 2°, 3° entraînent l'*unicité* de \bar{E} (à un isomorphisme près). En effet, le problème étant toujours supposé possible, tout élément de \bar{E} a la forme $x \bar{\tau} y'$, où $x \in A$, et y' est le symétrique d'un élément $y \in A^*$. Pour que $x_1 \bar{\tau} y'_1 = x_2 \bar{\tau} y'_2$, il faut et il suffit (y_1 et y_2 étant réguliers) que

$$(x_1 \bar{\tau} y'_1) \bar{\tau} (y_1 \bar{\tau} y_2) = (x_2 \bar{\tau} y'_2) \bar{\tau} (y_1 \bar{\tau} y_2)$$

c'est-à-dire (puisque $\bar{\tau}$ est commutative), $x_1 \bar{\tau} y_2 = x_2 \bar{\tau} y_1$. Il en résulte aussitôt que cette dernière relation est une *relation d'équivalence* entre les éléments (x_1, y_1) et (x_2, y_2) de l'ensemble produit $A \times A^*$, et qu'il existe une application biunivoque de \bar{E} sur l'ensemble quotient de $A \times A^*$ par cette relation.

En passant de A à \bar{E} par l'isomorphisme réciproque de f , on voit donc que, si le problème est possible, la relation $u_1 \tau v_2 = u_2 \tau v_1$ entre éléments (u_1, v_1) et (u_2, v_2) de l'ensemble produit $E \times E^*$ est une relation d'équivalence, et qu'il existe une application biunivoque de \bar{E} sur l'ensemble quotient de $E \times E^*$ par cette relation. En outre, si on transporte par cette application la structure définie par la loi $\bar{\tau}$ sur \bar{E} , la classe d'équivalence composée des classes de (u_1, v_1) et de (u_2, v_2) est la classe de l'élément $(u_1 \tau u_2, v_1 \tau v_2)$: en effet, si $x_1 \in A$, $x_2 \in A$, $y_1 \in A^*$, $y_2 \in A^*$, on a $(x_1 \bar{\tau} y'_1) \bar{\tau} (x_2 \bar{\tau} y'_2) = (x_1 \bar{\tau} x_2) \bar{\tau} (y'_1 \bar{\tau} y'_2)$, et $y'_1 \bar{\tau} y'_2$ est symétrique de $y_1 \bar{\tau} y_2$. Tout ceci prouve donc que, si on peut définir \bar{E} , la loi $\bar{\tau}$ et l'isomorphisme f de manière à satisfaire aux conditions 1°, 2°, 3°, \bar{E} est déterminé, à une isomorphie près, par la donnée de E et de la loi τ .

De plus, tout élément régulier de \bar{E} est *symétrisable* : en effet, si $x \bar{\tau} y'$ est régulier dans \bar{E} ($x \in A$, $y \in A^*$), il en est de même (prop. 2) de $(x \bar{\tau} y') \bar{\tau} y = x$; *a fortiori* x est régulier dans A , donc symétrisable dans \bar{E} par hypothèse ; par suite $x \bar{\tau} y'$ est également symétrisable. Cette propriété de \bar{E} est donc une conséquence des propriétés 1°, 2°, 3° supposées vérifiées.

Reste à prouver que le problème est effectivement possible. Guidés par ce qui précède, montrons d'abord que la relation

$u_1 \tau v_2 = u_2 \tau v_1$ entre éléments (u_1, v_1) et (u_2, v_2) de $E \times E^*$ est une relation d'équivalence R. En effet, elle est évidemment réflexive et symétrique ; elle est transitive, car les relations $u_1 \tau v_2 = u_2 \tau v_1$, $u_2 \tau v_3 = u_3 \tau v_2$ entraînent $u_1 \tau v_2 \tau v_3 = u_2 \tau v_1 \tau v_3 = u_3 \tau v_2 \tau v_1$, donc (v_2 étant régulier), $u_1 \tau v_3 = u_3 \tau v_1$.

Appelons maintenant \bar{E} l'ensemble quotient de $E \times E^*$ par la relation R. Soient x_1, x_2 deux éléments de \bar{E} , (u_1, v_1) et (u_2, v_2) des éléments des classes d'équivalence x_1, x_2 ; la classe d'équivalence qui contient $(u_1 \tau u_2, v_1 \tau v_2)$ ne dépend que de x_1, x_2 , car si on remplace (u_1, v_1) par un élément équivalent (u_3, v_3) , on a $u_1 \tau v_3 = u_3 \tau v_1$, donc $(u_1 \tau u_2) \tau (v_3 \tau v_1) = (u_3 \tau u_2) \tau (v_1 \tau v_2)$; on a un résultat analogue quand on remplace (u_2, v_2) par un élément équivalent ; on désignera par $x_1 \bar{\tau} x_2$ la classe à laquelle appartient $(u_1 \tau u_2, v_1 \tau v_2)$; $\bar{\tau}$ est une loi de composition entre éléments de \bar{E} , évidemment associative et commutative.

Montrons que \bar{E} possède un élément neutre pour cette loi. En effet, tous les éléments de $E \times E^*$ de la forme (w, w) , où $w \in E^*$, sont équivalents ; et réciproquement, si (u, v) est équivalent à (w, w) , on a $u \tau w = v \tau w$, donc (w étant régulier), $u = v$; soit e la classe formée des éléments (w, w) . Si $(u, v) \in E \times E^*$, et $w \in E^*$, $(u \tau w, v \tau w)$ est équivalent à (u, v) ; e est donc élément neutre pour la loi $\bar{\tau}$, et la condition 1^o est vérifiée.

Étant donné $u \in E$, considérons dans $E \times E^*$ l'ensemble des éléments de la forme $(u \tau v, v)$, où v parcourt E^* ; ils sont tous équivalents, et réciproquement, si (u_1, v_1) est équivalent à un de ces éléments, on a $u_1 \tau v_1 \tau v_1 = u_1 \tau v_1$, donc (v_1 étant régulier) $u_1 = u_1 \tau v_1$; autrement dit, les éléments $(u \tau v, v)$ forment une classe d'équivalence ; si on la désigne par $f(u)$, on définit ainsi une application biunivoque f de E sur une partie A de \bar{E} ; on vérifie aisément que A est stable pour la loi $\bar{\tau}$, et que f est un isomorphisme de E sur A. Enfin, si u est régulier dans E , $f(u)$, qui est la classe de $(u \tau v, v)$, admet un symétrique dans \bar{E} , à savoir la classe de $(v, u \tau v)$ (puisque dans ce cas $u \tau v \in E^*$) ; la condition 2^o est donc satisfaite, et le problème posé est possible. Nous avons ainsi démontré le théorème suivant :

THÉORÈME 1 (théorème de symétrisation). — *Soit τ une loi de composition associative et commutative partout définie entre éléments d'un ensemble E.*

On peut définir un ensemble \bar{E} , une loi de composition $\bar{\tau}$ entre éléments de \bar{E} , associative et commutative, et une partie A de \bar{E} , stable pour la loi $\bar{\tau}$, de manière à satisfaire aux conditions suivantes :

1^o *Il existe un isomorphisme de E (pour la loi τ) sur A (pour la loi induite par $\bar{\tau}$) qui, à tout élément régulier de E, fait correspondre un élément de A symétrisable dans \bar{E} ;*

2^o *\bar{E} est engendré par la réunion de A et de l'ensemble A' des symétriques des éléments réguliers de A.*

En outre, l'ensemble \bar{E} est déterminé d'une manière unique par ces conditions (à une isomorphie près), et tout élément régulier de \bar{E} est symétrisable.

COROLLAIRE. — *Lorsque tous les éléments de E sont réguliers, tous les éléments de \bar{E} sont symétrisables.*

Cela résulte en effet des conditions 1^o et 2^o du th. 1, et de la prop. 5.

La structure déterminée sur \bar{E} par la loi $\bar{\tau}$ rentre alors dans l'espèce des structures de groupe, que nous étudierons au § 6.

L'ensemble \bar{E} construit dans la démonstration du th. 1, muni de la loi $\bar{\tau}$, est appelé l'ensemble *symétrisé* de E (pour la loi τ) ; on dit que la loi $\bar{\tau}$ est obtenue par *symétrisation* de la loi τ . Dans les applications du th. 1, il est le plus souvent commode d'*identifier* (Ens. R, § 8, n° 5) l'ensemble E avec l'ensemble ci-dessus désigné par A ; ce qui permet (par abus de langage) de dire qu'on a « plongé » E dans son symétrisé \bar{E} et que la loi $\bar{\tau}$ est le *prolongement par symétrie* de la loi τ . Cette convention de langage sera appliquée en particulier dans les deux importants exemples qui suivent.

5. Applications : I. Entiers rationnels.

Prenons pour E l'ensemble N des entiers naturels, la loi de composition étant l'*addition* ; tous les éléments de N sont réguliers pour cette loi. Le symétrisé de N se note Z ; ses éléments sont appelés *entiers rationnels* ; la loi obtenue par symétrisation de l'*addition* dans N s'appelle *addition des entiers rationnels* et se note encore +. Les éléments de Z sont, par définition, les classes

d'équivalence déterminées dans $\mathbb{N} \times \mathbb{N}$ par la relation entre (m_1, n_1) et (m_2, n_2) qui s'écrit $m_1 + n_2 = m_2 + n_1$; ils sont tous *symétrisables*; un élément m de \mathbb{N} est identifié avec la classe formée des éléments $(m + n, n)$ où $n \in \mathbb{N}$; il admet pour symétrique dans \mathbb{Z} la classe des éléments $(n, m + n)$. Mais tout élément (p, q) de $\mathbb{N} \times \mathbb{N}$ peut s'écrire sous la forme $(m + n, n)$ si $p \geq q$, sous la forme $(n, m + n)$ si $p \leq q$; il s'ensuit que \mathbb{Z} est la réunion de \mathbb{N} et de l'ensemble des symétriques des éléments de \mathbb{N} . D'ailleurs, l'élément neutre 0 est le seul élément de \mathbb{N} dont le symétrique appartienne à \mathbb{N} .

On note $-m$ l'entier rationnel symétrique de l'entier naturel $m \neq 0$; \mathbb{Z} est réunion de \mathbb{N} et de l'ensemble des éléments $-m$ pour $m \in \mathbb{N}, m \neq 0$; m est identifié à la classe contenant $(m, 0)$, et $-m$ à la classe qui contient $(0, m)$; on en déduit facilement (en tenant compte de ce qui a été dit dans la démonstration du th. 1) l'expression de la somme de deux entiers rationnels; pour $m \in \mathbb{N}, n \in \mathbb{N}, n \neq 0$:

- a) Si $m \geq n$, on a $m + (-n) = p$, p étant l'élément de \mathbb{N} tel que $m = n + p$.
- b) Si $m < n$, on a $m + (-n) = -p$, p étant l'élément de \mathbb{N} tel que $m + p = n$.
- c) Si $m \neq 0$, on a $(-m) + (-n) = -(m + n)$.

Ces relations restent vraies sans la restriction $n \neq 0$, et éventuellement $m \neq 0$, en convenant que -0 désigne encore l'élément 0.

Plus généralement on désignera par $-x$ le symétrique d'un entier rationnel quelconque x , qu'on appelle plus souvent l'*opposé* de x ; le composé $x + (-y)$ se note, de façon abrégée, $x - y$.

La relation d'ordre $m \leq n$ entre entiers naturels (*Ens.*, chap. III) possède la propriété suivante: si $m \leq n$, on a $m + p \leq n + p$ pour tout $p \in \mathbb{N}$; montrons qu'on peut définir sur \mathbb{Z} une relation d'ordre *et une seule*, notée encore $x \leq y$, induisant sur \mathbb{N} la relation précédente, et telle que $x \leq y$ entraîne $x + z \leq y + z$ pour tout $z \in \mathbb{Z}$ (on dit que l'ordre sur \mathbb{Z} est *invariant par translation*; cf. chap. V).

En effet, pour une telle relation, on doit avoir $0 \leq m$ pour tout $m \in \mathbb{N}$, d'où $(-m) \leq m + (-m) = 0$; si x et y sont deux entiers rationnels tels que $x \leq y$, on a $0 = x - x \leq y - x$, donc $y - x = m \in \mathbb{N}$, et on a $y = x + m$; réciproquement, s'il existe

$m \in \mathbb{N}$ tel que $y = x + m$, on a $0 + x \leq m + x$, donc $x \leq y$; s'il existe une relation d'ordre satisfaisant aux conditions ci-dessus, elle est nécessairement équivalente à la relation « il existe $m \in \mathbb{N}$ tel que $y = x + m$ » (ou encore $y - x \in \mathbb{N}$). Inversement, cette dernière relation est bien une relation d'ordre, car elle est évidemment transitive, et si $y = x + m, x = y + n, m \in \mathbb{N}, n \in \mathbb{N}$, on a $m + n = 0$, d'où $m = n = 0, x = y$; en outre, elle satisfait bien aux conditions posées; enfin, \mathbb{Z} est totalement ordonné par cette relation, car on a $x - y = -(y - x)$ et on a toujours, quels que soient x et y dans \mathbb{Z} , $y - x \in \mathbb{N}$ ou $x - y \in \mathbb{N}$, c'est-à-dire $x \leq y$ ou $y \leq x$.

Lorsqu'on considérera désormais \mathbb{Z} comme un ensemble ordonné, il s'agira toujours, sauf mention expresse du contraire, de l'ordre qui vient d'être défini. Les entiers naturels sont identiques aux entiers ≥ 0 : on les appelle encore entiers *positifs*; les entiers ≤ 0 , symétriques des entiers positifs, sont dits entiers *négatifs*; les entiers > 0 (resp. < 0) sont dits *strictement positifs* (*) (resp. *strictement négatifs*); l'ensemble des entiers > 0 se notera \mathbb{N}^* .

6. Applications : II. Nombres rationnels positifs.

Prenons pour E l'ensemble \mathbb{N} des entiers naturels, la loi de composition étant cette fois la *multiplication*; l'ensemble des éléments réguliers de \mathbb{N} pour cette loi est \mathbb{N}^* . Le symétrisé de \mathbb{N} pour la multiplication se note \mathbb{Q}_+ et ses éléments sont appelés *nombres rationnels positifs*; la loi obtenue par symétrisation de la multiplication s'appelle *multiplication des nombres rationnels positifs* et se note multiplicativement. Les éléments de \mathbb{Q}_+ sont les classes d'équivalence déterminées dans $\mathbb{N} \times \mathbb{N}^*$ par la relation entre (p_1, q_1) et (p_2, q_2) qui s'écrit $p_1 q_2 = p_2 q_1$; on convient de désigner par $\frac{p}{q}$ ou par p/q l'élément de \mathbb{Q}_+ qui contient l'élément (p, q) de $\mathbb{N} \times \mathbb{N}^*$; le produit de p_1/q_1 et de p_2/q_2 est donc $p_1 p_2/q_1 q_2$; l'entier naturel m est identifié aux nombres rationnels $\frac{mn}{n}$ ($n \in \mathbb{N}^*$).

(*) On notera que, pour nous conformer au langage général adopté pour les ensembles ordonnés (*Ens.* R, § 6) et les groupes ordonnés (cf. chap. V), nous nous écartons de la terminologie courante (où *positif* signifie > 0); avec notre terminologie, 0 est à la fois *positif* et *négatif* (c'est d'ailleurs le seul entier rationnel ayant cette propriété).

Nous ne pousserons pas davantage ici l'étude de \mathbb{Q}_+ , car on retrouvera cet ensemble plus loin (§ 9, n° 5) comme partie de l'ensemble \mathbb{Q} des *nombres rationnels* (où on définira, non seulement une multiplication induisant sur \mathbb{Q}_+ la multiplication qui vient d'être définie, mais aussi une *addition*).

7. Prolongement d'une représentation par symétrie.

Étant donné un ensemble E , muni d'une loi associative et commutative, le théorème suivant permet de prolonger au symétrisé \bar{E} de E (n° 4) certaines représentations de E dans un ensemble F muni d'une loi associative :

THÉORÈME 2. — Soient \bar{E} un ensemble muni d'une loi associative et commutative, et E une partie stable de \bar{E} telle que : 1^o tout élément régulier de E soit symétrisable dans \bar{E} ; 2^o \bar{E} soit engendré par la réunion de E et de l'ensemble des symétriques des éléments réguliers de E . Soit f une représentation de E dans un ensemble F muni d'une loi associative, qui à tout élément régulier de E fasse correspondre un élément symétrisable de F ; alors f peut, d'une manière et d'une seule, être prolongée en une représentation de \bar{E} dans F .

On supposera notées τ les lois données sur \bar{E} et F ; le symétrique d'un élément symétrisable $x \in \bar{E}$ (resp. $y \in F$) se notera x' (resp. y'). Il est immédiat que la loi induite sur $f(E)$ par la loi τ sur F est commutative. D'autre part, il résulte de la démonstration du th. 1 que tout élément w de \bar{E} est de la forme $x \tau y'$, où $x \in E$ et y est un élément régulier de E ; si $x \tau y' = x_1 \tau y'_1$, on a $x \tau y_1 = x_1 \tau y$, donc $f(x) \tau f(y_1) = f(x_1) \tau f(y)$; comme $f(y)$ et $f(y_1)$ sont symétrisables par hypothèse, et aussi permutable entre eux et avec $f(x)$ et $f(x_1)$, on a $f(x) \tau (f(y))' = f(x_1) \tau (f(y_1))'$ donc $f(x) \tau (f(y))'$ ne dépend que de l'élément w et non de son expression particulière sous la forme $x \tau y'$; en outre, si $w \in E$, on a $x = w \tau y$, donc $f(x) = f(w) \tau f(y)$, et $f(w) = f(x) \tau (f(y))'$. En posant $f(x \tau y') = f(x) \tau (f(y))'$, on prolonge donc à \bar{E} l'application f de E dans F ; et on vérifie, par un calcul analogue aux précédents, que ce prolongement est une représentation de \bar{E} dans F . L'unicité résulte de ce que toute représentation g de \bar{E} dans F satisfait à $g(x \tau y') = g(x) \tau (g(y))'$ pour tout y symétrisable de E .

8. Application : Multiplication des entiers rationnels.

Considérons l'ensemble \mathbb{Z} des entiers rationnels (n° 5) et l'ensemble des entiers naturels $\mathbb{N} \subset \mathbb{Z}$, avec la structure définie sur eux par l'addition seule. Si $m \in \mathbb{N}$, on a (Ens., chap. III) l'identité $m(x + y) = mx + my$ pour $x \in \mathbb{N}$, $y \in \mathbb{N}$, qui exprime que l'application $x \rightarrow mx$ de \mathbb{N} dans lui-même est une représentation. On peut aussi la considérer comme représentation de \mathbb{N} dans \mathbb{Z} , et à ce titre lui appliquer le th. 2 : on peut donc la prolonger en une représentation de \mathbb{Z} dans \mathbb{Z} , qu'on notera encore $x \rightarrow mx$; d'après la démonstration du th. 2, pour $x = -n$, $n \in \mathbb{N}^*$, mx est égal à $-mn$.

Déterminons maintenant toutes les représentations f de \mathbb{Z} dans \mathbb{Z} . Soit $f(1) = a$, et supposons d'abord $a \geqslant 0$. On a $f(x + 1) = f(x) + a$, d'où s'ensuit, par récurrence, que, pour $x \in \mathbb{N}$, $f(x) = ax$; par application du th. 2 à \mathbb{Z} et \mathbb{N} , on a donc $f(x) = ax$ quel que soit $x \in \mathbb{Z}$. Si au contraire $a = -n$, $n \in \mathbb{N}^*$, l'application $x \rightarrow -f(x)$ est composée de $x \rightarrow -x$ (qui est une représentation, l'addition étant commutative) et de f , donc est une représentation qui applique 1 sur $n > 0$, d'où $-f(x) = nx$ et $f(x) = -nx$ quel que soit $x \in \mathbb{Z}$; on posera encore, par définition, $f(x) = ax$, c'est-à-dire qu'on pose $(-n)x = -(nx)$ pour $n \in \mathbb{N}^*$, $x \in \mathbb{Z}$.

On a ainsi défini le produit ab quels que soient $a \in \mathbb{Z}$, $b \in \mathbb{Z}$. Pour $m \in \mathbb{N}$, $n \in \mathbb{N}$, on a $(-m)n = -mn$, $m(-n) = -mn$, $(-m)(-n) = mn$, d'où on conclut immédiatement que la multiplication est associative et commutative dans \mathbb{Z} ; par la manière même dont on a obtenu le produit, on a $x(y + z) = xy + xz$, d'où (par la commutativité) $(x + y)z = xz + yz$ quels que soient x, y, z ; et $x \cdot 0 = 0 \cdot x = 0$, $x \cdot 1 = 1 \cdot x = x$.

Pour la multiplication ainsi définie dans \mathbb{Z} , \mathbb{N} est évidemment une partie stable ; autrement dit, les relations $x \geqslant 0$, $y \geqslant 0$ entraînent $xy \geqslant 0$. Si $x \leqslant y$ et $z \geqslant 0$, on a donc $z(y - x) \geqslant 0$, c'est-à-dire $zx \leqslant zy$.

On verra au § 8 (n° 1) comment le raisonnement qui conduit à définir la multiplication dans \mathbb{Z} permet, convenablement généralisé, de définir l'anneau des endomorphismes d'un groupe abélien quelconque.

9. Notations du symétrique d'un élément.

L'ensemble \mathbf{Z} des entiers rationnels permet de poser une notation qui comprend comme cas particulier la notation ${}^n \tau x$ définie au § 1, n° 3. Rappelons que, pour une loi associative τ admettant un élément neutre e , on pose ${}^0 \tau x = e$ pour tout x ; si de plus x possède un élément symétrique x' , on pose, par définition, ${}^{-n} \tau x = {}^n \tau x'$ quel que soit $n \in \mathbf{N}^*$: alors ${}^a \tau x$ est défini quel que soit $a \in \mathbf{Z}$, et on a en particulier ${}^1 \tau x = x'$. On vérifie immédiatement que l'on a, quels que soient $a \in \mathbf{Z}$, $b \in \mathbf{Z}$

$$(1) \quad {}^{a+b} \tau x = ({}^a \tau x) \tau ({}^b \tau x).$$

$$(2) \quad {}^{ab} \tau x = {}^a \tau ({}^b \tau x).$$

Voici encore quelques observations générales concernant la terminologie et les notations pour les lois de composition écrites, soit additivement, soit multiplicativement :

a) *Sauf indication formelle du contraire*, on n'emploiera le signe $+$ que lorsqu'il s'agira de noter une loi *associative et commutative* entre éléments d'un ensemble E . Pour une loi ainsi notée, on conviendra, si $x \in E$, de considérer $+x$ comme une notation désignant x lui-même; si de plus x est symétrisable, on désignera par $-x$ le symétrique de x , qui sera plus souvent appelé *l'opposé de x* . En outre, on notera le composé $x + (-y)$ sous la forme abrégée $x - y$; de même, des notations telles que

$$x + y - z, \quad x - y - z, \quad x - y + z - t$$

signifieront respectivement

$$(x + y) - z, \quad (x - y) - z, \quad ((x - y) + z) - t.$$

Enfin, dans tous les cas où on notera nx (pour $n \in \mathbf{N}^*$) le composé d'une suite de n éléments tous égaux à x , on conviendra, lorsqu'il existe dans E un élément neutre, que $0x$ désignera cet élément neutre (lui-même le plus souvent noté 0, comme il a été dit); et quand x a un opposé $-x$, on notera $(-n)x$ l'élément $n(-x) = - (nx)$.

b) *Sauf indication formelle du contraire*, on n'emploiera la no-

tation multiplicative que lorsqu'il s'agira de noter une loi *associative*. Pour une loi ainsi notée, si x admet un élément symétrique x' , cet élément sera plus souvent appelé *l'inverse de x* , et x sera dit *inversible*; dans les mêmes conditions, on désignera par x^a , pour $a \in \mathbf{Z}$, l'élément désigné plus haut par ${}^a \tau x$ pour une loi notée τ ; en particulier *l'inverse de x* se notera x^{-1} .

Si de plus la loi multiplicative considérée est *commutative* (et dans ce cas seulement), et si on désigne par 1 l'élément neutre (appelé plus souvent dans ce cas *unité*, comme on l'a vu), on conviendra parfois, lorsque y est inversible, d'écrire $\frac{1}{y}$ l'élément y^{-1} , et $\frac{x}{y}$ l'élément $xy^{-1} = y^{-1}x$; on l'écrira aussi x/y lorsque cette notation ne prêtera pas à confusion. Un élément noté de cette manière s'appelle une *fraction*: x est appelé le *numérateur*, y le *dénominateur* de la fraction.

c) Désormais, dans les raisonnements généraux relatifs aux lois de composition *associatives*, on se servira le plus souvent de la notation multiplicative (ou éventuellement de la notation additive lorsque la loi est aussi commutative).

Exercices. — 1) Soit τ une loi de composition partout définie sur un ensemble E . Désignant par F l'ensemble « somme » (*Ens. R*, § 4, n° 5) de E et d'un ensemble $\{e\}$ à un élément, et identifiant E et $\{e\}$ avec les parties correspondantes de F , montrer qu'on peut, d'une manière et d'une seule, définir sur F une loi de composition $\bar{\tau}$ qui induise sur E la loi τ , et pour laquelle e soit élément neutre; si τ est associative, la loi $\bar{\tau}$ est associative. (S'il n'y a pas d'élément neutre pour τ dans E , on dit que F se déduit de E « par adjonction d'un élément neutre »).

2) Soit τ une loi partout définie sur E . Pour que τ soit associative, il faut et il suffit que toute translation à gauche γ_x soit permutable avec toute translation à droite δ_y dans l'ensemble des applications de E dans E (pour la loi $f \circ g$).

3) Dans l'ensemble F des applications de E dans E , pour que la relation $f \circ g = f \circ h$ entraîne $g = h$, il faut et il suffit que f soit une application biunivoque de E dans E ; pour que la relation $g \circ f = h \circ f$ entraîne $g = h$, il faut et il suffit que f soit une application de E sur E ; pour que f soit régulier (pour la loi δ), il faut et il suffit que f soit une application biunivoque de E sur E .

4) Dans un monoïde libre (§ 1, n° 2), tout élément est régulier.

5) Pour $2 \leqslant n \leqslant 5$, déterminer, sur un ensemble E à n élé-

ments, toutes les lois partout définies, admettant un élément neutre et pour lesquelles tous les éléments de E soient réguliers ; pour $n = 5$, montrer qu'il existe des lois non associatives satisfaisant à ces conditions.

(N.-B. Les exercices 6 à 16 inclus se rapportent à des lois associatives sur un ensemble E , notées *multiplicativement* ; e désigne l'élément neutre, lorsqu'il existe, γ_a et δ_a les translations correspondant à $a \in E$; pour une partie X de E , on posera $\gamma_a(X) = aX$, $\delta_a(X) = Xa$).

6) Pour une loi associative sur un ensemble *fini*, tout élément régulier est inversible (utiliser la prop. 4).

7) Étant donnée une loi associative sur un ensemble E , et un élément $x \in E$, soit A l'ensemble des x^n pour $n \in \mathbb{N}^*$; s'il existe un élément neutre, soit B l'ensemble des x^n pour $n \in \mathbb{N}$; si de plus x est inversible, soit C l'ensemble des x^a pour $a \in \mathbb{Z}$. Montrer que, si A (resp. B, C) est infini, il est isomorphe (pour la loi induite par la loi donnée sur E) à \mathbb{N}^* (resp. \mathbb{N}, \mathbb{Z}) muni de l'addition.

8) Avec les notations de l'exerc. 7, on suppose A fini ; montrer que A contient un idempotent h (§ 1, n° 4) et un seul (on observera que si x^p et x^q sont idempotents, on a $x^p = x^q, x^q = x^p$, donc $x^p = x^q$) ; si $h = x^p$, l'ensemble des x^n pour $n \geq p$ est une partie stable D de E telle que, pour la loi induite sur D , h soit élément neutre, et tous les éléments de D inversibles.

¶ 9) Pour une loi multiplicative sur un ensemble E , soit a un élément de E tel que la translation à gauche γ_a soit une application biunivoque de E dans E .

a) S'il existe un élément u tel que $au = a$, montrer que $ux = x$ pour tout $x \in E$; en particulier, si $xu = x$ pour tout $x \in E$, u est élément neutre.

b) S'il existe $u \in E$ tel que $au = a$, et $b \in E$ tel que $ab = u$, montrer que $ba = u$ (former aba) ; en particulier, s'il existe un élément neutre e , et un élément b tel que $ab = e$, b est inverse de a .

10) Si a et b sont deux éléments de E tels que γ_{ba} soit une application biunivoque de E dans E , montrer que γ_a est une application biunivoque de E dans E . En déduire que, pour une loi associative et commutative sur E , l'ensemble S des éléments non réguliers de E est tel que $ES \subset S$ (et en particulier est stable).

¶ 11) On dit que E est un *semi-groupe à gauche* si, pour tout $x \in E$, γ_x est une application biunivoque de E dans E .

a) Si u est un idempotent (§ 1, n° 4), on a $ux = x$ pour tout $x \in E$ (utiliser l'exerc. 9a)) ; u est élément neutre pour la loi induite sur Eu .

b) Si u et v sont deux idempotents distincts de E , on a $Eu \cap Ev = \emptyset$ (montrer que la relation $xu = yv$ entraîne $xu = xv$), et les ensembles Eu et Ev (munis des lois induites par celle de E) sont isomorphes.

c) Soit R le complémentaire de la réunion des ensembles Eu , où u parcourt l'ensemble des idempotents de E . Montrer que $ER \subset R$ (prouver que si $x \in E, y \in R$, on ne peut avoir $xy = xyu$ pour un idempotent u) ; il en résulte que R est une partie stable de E . Si R n'est pas vide, on a $aR \neq R$ pour tout $a \in R$ (utiliser l'exerc. 9a) pour prouver que, dans le cas contraire, R contiendrait un idempotent) ; en particulier, R est alors infini. On dit que R est le *résidu* du semi-groupe à gauche E .

d) Si R n'est pas vide, et s'il existe au moins un idempotent u dans E (c'est-à-dire si $E \neq R$), pour tout $x \in REu$, on a $xEu \neq Eu$ (en supposant le contraire, montrer qu'il existerait $a \in R$ tel que $aR = R$) ; en particulier, aucun élément de REu n'est inversible dans Eu , et REu est un ensemble infini (utiliser l'exerc. 8).

e) Si E possède un élément neutre e , e est le seul idempotent de E , et R est vide (remarquer que $E = Ee$).

f) S'il existe $a \in E$ tel que la translation à droite δ_a soit une application *biunivoque* de E dans E (en particulier si la loi donnée sur E est commutative), ou bien E possède un élément neutre, ou bien $E = R$ (remarquer que s'il existe un idempotent u , on a $xa = xua$ pour tout $x \in E$).

g) S'il existe $a \in E$ tel que δ_a soit une application de E sur E , ou bien E possède un élément neutre, ou bien $E = R$ (examiner séparément le cas où $a \in R$ et le cas où $a \in Eu$, pour un idempotent u).

¶ 12) Pour une loi multiplicative sur E , soit $a \in E$ tel que γ_a soit une application de E sur E .

a) Montrer que, s'il existe u tel que $ua = a$, on a $ux = x$ pour tout $x \in E$.

b) Pour qu'un élément $b \in E$ soit tel que γ_{ba} soit une application biunivoque de E dans E , il faut et il suffit que γ_a soit une application biunivoque de E sur E et γ_b une application biunivoque de E dans E .

¶ 13) On suppose que, pour tout $x \in E$, γ_x est une application de E sur E . Montrer que si, pour un élément $a \in E$, γ_a est une application biunivoque de E sur E , γ_x est une application biunivoque de E sur E pour tout $x \in E$ (utiliser l'exerc. 12 b)) ; il en est ainsi en particulier s'il existe deux éléments a, b , de E tels que $ab = b$ (utiliser l'exerc. 12a)). E est alors un semi-groupe à gauche, dont le résidu R est vide ; en outre, pour tout idempotent u , tout élément de Eu est inversible dans Eu .

¶ 14) Pour une loi associative sur un ensemble *fini* E , il existe des parties *minimales* de la forme aE (c'est-à-dire des éléments minimaux de l'ensemble des parties de E de cette forme, ordonné par inclusion).

a) Si $M = aE$ est minimale, on a $xM = xE = M$ pour tout $x \in M$; muni de la loi induite par celle de E , M est un semi-groupe à

gauche (exerc. 11) dans lequel toute translation à gauche est une application biunivoque de M sur lui-même (cf. exerc. 13).

b) Si $M = aE$ et $M' = a'E$ sont minimales et distinctes, on a $M \cap M' = \emptyset$: pour tout $b \in M$, l'application $x' \rightarrow bx'$ de M' dans M est une application biunivoque de M' sur M . En déduire qu'il existe un idempotent $u' \in M'$ tel que $bu' = b$, et un idempotent $u \in M$ tel que $uu' = u$ (prendre pour u l'idempotent tel que $bu = b$). Montrer que $u'u = u'$ (considérer $uu'u$), et que tout $y' \in M'$ tel que $y'u = y'$ appartient à $M'u'$.

c) Montrer que l'application $x' \rightarrow ux'$ de $M'u'$ dans M est un isomorphisme de $M'u'$ sur Mu ; en déduire que M et M' sont des semi-groupes à gauche isomorphes.

d) Soient $M_i (1 \leq i \leq r)$ les parties minimales distinctes de la forme aE : déduire de b) qu'on peut ranger les idempotents de chaque semi-groupe à gauche M_i en une suite $(u_{ij}) (1 \leq j \leq s)$ de sorte qu'on ait $u_{ij} u_{kj} = u_{ij}$ quels que soient i, j, k . Si K est la réunion des M_i , montrer que $Eu_{ij} \subset K$ (remarquer que pour tout $x \in E$, $xu_{ij}E$ est une partie minimale de la forme aE); en déduire que Eu_{ij} est la réunion des $u_{kj}Eu_{kj}$ pour $1 \leq k \leq r$ (montrer que $(Eu_{ij}) \cap M_k = u_{kj}Eu_{kj}$), et que $Eu_{ij}E = K$. Prouver enfin que toute partie minimale de la forme Eb est identique à un des s ensembles Eu_{ij} (remarquer, à l'aide de a), que $Ebu_{ij}b = Eb$, et en déduire que $Eb \subset K$.

15) Soit $(x_i)_{1 \leq i \leq n}$ une suite finie d'éléments tels que les translations à gauche γ_{x_i} soient des applications biunivoques de E dans E .

a) Montrer que la relation $x_1 x_2 \dots x_n = e$ entraîne toutes les relations $x_{i+1} \dots x_n x_1 x_2 \dots x_i = e$ qui s'en déduisent par « permutation circulaire » pour $1 \leq i \leq n$.

b) En déduire que si le composé de la suite (x_i) est inversible, chacun des x_i est inversible.

16) Si x et y sont inversibles, on appelle *commutateur* de x et y , et on désigne par $x \circ y$, l'élément $y^{-1}x^{-1}yx$. Montrer que, pour que x et y (supposés inversibles) soient permutable, il faut et il suffit que $x \circ y = e$. Démontrer les identités :

$$\begin{aligned} y \circ x &= (x \circ y)^{-1} \\ x \circ (yz) &= (x \circ y)(z \circ (x \circ y))(x \circ z) \\ (x \circ y)(z \circ (x \circ y))(z \circ x)^{-1}(y \circ z)(x \circ (y \circ z))(x \circ y)^{-1}(z \circ x)(y \circ (z \circ x))(y \circ z)^{-1} &= e \end{aligned}$$

(la troisième se déduit de la seconde en permutant circulairement x, y, z , et multipliant membre à membre les trois identités obtenues).

17) Étendre la démonstration du théorème de symétrisation (th. 1) au cas où la loi τ est associative et où tout élément régulier pour cette loi est un élément *central*.

¶ 18) Soit τ une loi associative sur un ensemble E , E^* l'ensemble des éléments réguliers de E ; on suppose que E^* n'est pas vide, et que tout élément régulier est un élément central. On désigne par \mathfrak{F} l'ensemble des parties X de E ayant la propriété suivante : il existe $y \in E^*$ tel que $\delta_y(E) \subset X$.

a) Montrer que l'intersection de deux ensembles de \mathfrak{F} appartient à \mathfrak{F} .

b) Soit Φ l'ensemble des fonctions définies sur un ensemble de \mathfrak{F} , prenant leurs valeurs dans E , et telles que, pour $f \in \Phi$ et $X \in \mathfrak{F}$,

$f(X)$ appartienne à \mathfrak{F} . On désigne par R la relation entre éléments f et g de Φ : « il existe un ensemble $X \in \mathfrak{F}$ tel que les restrictions de f et g à X soient identiques ». Montrer que R est une relation d'équivalence ; soit $\Psi = \Phi/R$ l'ensemble quotient de Φ par cette relation.

c) Soient f et g deux éléments de Φ , $A \in \mathfrak{F}$ et $B \in \mathfrak{F}$ les ensembles où f et g sont respectivement définies ; il existe $X \subset B$ et appartenant à \mathfrak{F} , tel que $g(X) \subset A$; si g_X est la restriction de g à X , montrer que l'application $f \circ g_X$ appartient à Φ , et que sa classe (mod. R) ne dépend que des classes de f et g (et non de X); cette classe est dite composée de celle de f et de celle de g ; montrer que la loi de composition ainsi définie dans Ψ est associative et possède un élément neutre.

d) Pour tout $a \in E$, montrer que la translation à gauche γ_a appartient à Φ ; soit φ_a sa classe (mod. R). Montrer que l'application $x \rightarrow \varphi_x$ est un isomorphisme de E dans Ψ , et que si $x \in E^*$, φ_x est inversible dans Ψ (considérer l'application réciproque de γ_x , montrer qu'elle appartient à Φ , et que sa classe (mod. R) est symétrique de φ_x). En déduire une nouvelle démonstration du th. 1 et de sa généralisation énoncée dans l'exerc. 17.

§ 3. — Lois de composition externes.

1. Lois de composition externes.

DÉFINITION 1. — On appelle *loi de composition externe* entre éléments d'un ensemble Ω , dit *ensemble des opérateurs* (ou *domaine d'opérateurs*) de la loi, et éléments d'un ensemble E , une application f d'une partie A de $\Omega \times E$ dans E . La valeur $f(\alpha, x)$ de f pour un $(\alpha, x) \in A$ s'appelle le *composé de α et de x* pour cette loi. Les éléments de Ω sont appelés les *opérateurs de la loi*.

Comme pour les lois internes, on dit, par abus de langage, qu'une loi externe est donnée (ou définie) sur E . Le cas de beau-

coup le plus important est celui des lois *partout définies*, c'est-à-dire définies sur $A = \Omega \times E$; ce sont celles que nous considérons le plus souvent par la suite.

Parmi les notations les plus fréquemment adoptées pour le composé de α et de x , citons les notations multiplicative à gauche $\alpha \cdot x$ (le point pouvant s'omettre à volonté), multiplicative à droite $x \cdot \alpha$, et exponentielle x^α ; dans les raisonnements des §§ 3 à 5, on se servira ordinairement du signe \perp pour noter des lois externes quelconques.

Exemples. — 1) Étant donnée une loi interne associative entre éléments d'un ensemble E , notée multiplicativement, $(n, x) \rightarrow x^n$ est une loi de composition externe partout définie entre éléments de N^* et éléments de E ; pour $\alpha \in \mathbb{Z}$, $(\alpha, x) \rightarrow x^\alpha$ est une loi entre \mathbb{Z} et E , qui n'est partout définie que si tous les éléments de E sont inversibles. Ce qui précède s'applique aux lois $(n, x) \rightarrow nx$ et $(a, x) \rightarrow ax$ pour une loi interne notée additivement (*).

2) Étant donnés deux ensembles E et F , l'application $(X, Y) \rightarrow X \circ Y$ est une loi de composition (partout définie) entre parties X de $E \times E$ et parties Y de $E \times F$, les premières étant les opérateurs; l'application $(Z, Y) \rightarrow Y \circ Z$ est une loi entre parties Z de $F \times F$ (opérateurs) et parties Y de $E \times F$.

3) Une loi de composition interne τ étant donnée sur E , on note encore $x \tau A$, pour $x \in E$, $A \subset E$, l'ensemble des $x \tau y$ pour $y \in A$ (c'est-à-dire l'ensemble $\{x\} \tau A$): on définit ainsi une loi de composition entre éléments de E (opérateurs) et parties de E .

Étant donné une loi externe \perp entre opérateurs $\alpha \in \Omega$ et éléments $x \in E$, définie sur une partie A de $\Omega \times E$, on désigne par $\Xi \perp X$, pour toute partie $\Xi \subset \Omega$ et toute partie $X \subset E$, l'ensemble des $\alpha \perp x$ pour $\alpha \in \Xi$, $x \in X$, $(\alpha, x) \in A$; lorsque Ξ est réduit à un élément α , on écrit $\alpha \perp X$ au lieu de $\{\alpha\} \perp X$.

L'application $(\Xi, X) \rightarrow \Xi \perp X$ est une loi de composition *partout définie* entre parties de Ω et parties de E .

(*) Il pourra se faire qu'en plus de cette loi interne, on se donne sur E une loi externe, notée multiplicativement, dont le domaine d'opérateurs contienne l'ensemble des entiers naturels N (ou une partie de N); il y aura lieu, dans ce cas, pour éviter toute confusion, d'utiliser une autre notation que $n \cdot x$ pour la somme d'une suite de n termes égaux à x (sauf dans le cas où cette somme serait toujours égale au composé de n et de x pour la loi externe donnée).

Une loi de composition externe $\alpha \perp x$ étant donnée entre $\alpha \in \Omega$ et $x \in E$, $x \rightarrow f_\alpha(x) = \alpha \perp x$ est une application dans E d'une partie de E , à savoir de l'ensemble des x pour lesquels $\alpha \perp x$ est défini. On dit que c'est l'*application produite* par l'opérateur α .

Réciproquement, soit $(f_\alpha)_{\alpha \in \Omega}$ une famille d'applications de parties de E dans E , ayant Ω comme ensemble d'indices: l'application $(\alpha, x) \rightarrow f_\alpha(x)$ est une loi de composition entre Ω et E . Il est donc complètement équivalent de se donner une telle famille (f_α) , ou de se donner une loi de composition entre Ω et E . Pour une loi de composition externe \perp entre Ω et E , un élément $x \in E$ est dit *invariant* pour un opérateur $\alpha \in \Omega$ si $\alpha \perp x$ est défini et égal à x ; un élément $\varepsilon \in \Omega$ est appelé *opérateur neutre* si tous les éléments de E sont invariants pour ε .

2. Dédoublement d'une loi interne.

L'ensemble Ω des opérateurs d'une loi externe sur un ensemble E peut ne pas être distinct de E lui-même: si $\Omega = E$, on se trouve en présence d'une application dans E d'une partie A de $E \times E$, qui peut également être considérée comme définissant une loi interne entre éléments de E . Plus précisément, une application $(x, y) \rightarrow f(x, y)$ de $A \subset E \times E$ dans E peut être considérée comme définissant les lois suivantes, *qu'il importe de bien distinguer*:

- 1^o Une loi interne τ pour laquelle le composé de x et de y est $x \tau y = f(x, y)$;
- 2^o la loi interne $\bar{\tau}$ opposée à la précédente (§ 1, n° 1), pour laquelle le composé de x et de y est $x \bar{\tau} y = y \tau x = f(y, x)$;
- 3^o une loi externe \perp entre opérateurs $x \in E$ et éléments $y \in E$, pour laquelle le composé de x et de y est $x \perp y = f(x, y)$; on dit que cette loi est la *loi externe à gauche* déduite de la loi τ ;
- 4^o une loi externe \perp entre opérateurs $x \in E$ et éléments $y \in E$, pour laquelle le composé de x et de y est $x \perp y = f(y, x)$; on dit que cette loi est la *loi externe à droite* déduite de τ ; c'est aussi la loi externe à gauche déduite de $\bar{\tau}$.

Lorsqu'aucune confusion n'est à craindre, on utilise, pour les lois externes déduites d'une loi interne τ , le même symbole τ : le composé de x et de y se notant $x \tau y$ pour la loi externe à gauche, $y \tau x$ pour la loi externe à droite.

Pour une loi τ partout définie sur E , la loi externe à gauche déduite de τ est celle qui correspond (de la manière dite plus haut) à la famille des translations à gauche $(\gamma_x)_{x \in E}$; la loi externe à droite est celle qui correspond à la famille des translations à droite δ_x . Dire qu'un élément $e \in E$ est élément neutre pour la loi τ équivaut à dire qu'il est opérateur neutre pour la loi externe à gauche et la loi externe à droite déduites de τ .

On dira que les deux lois externes déduites d'une loi interne sont obtenues par *dédoubllement* de cette loi. Chaque fois que le domaine d'opérateurs d'une loi externe sur E sera identique à E , et qu'il risquera d'en résulter des confusions, on le remplacera par un ensemble E' en correspondance biunivoque avec E , et on définira le composé de $x' \in E'$ et de $y \in E$ comme égal au composé de l'opérateur $x \in E$ et de l'élément $y \in E$ pour la loi donnée, x étant l'élément de E qui correspond à $x' \in E'$. Naturellement, on transportera en même temps à E' , le cas échéant, toutes les structures qu'on se sera données sur E (*Ens. R.*, § 8, n° 5).

3. Parties stables. Lois induites.

DÉFINITION 2. — Une partie A d'un ensemble E est dite stable pour une loi de composition externe $\alpha \perp x$ entre opérateurs $\alpha \in \Omega$ et éléments $x \in E$, si le composé $\alpha \perp x$ appartient à A chaque fois que $x \in A$ et que $\alpha \perp x$ est défini.

Autrement dit, A est stable si $\Omega \perp A \subset A$.

L'intersection d'une famille de parties stables de E est évidemment stable, donc il existe une plus petite partie stable de E contenant une partie X donnée, qui est dite *engendrée* par X .

Exemple. — Pour la loi externe déduite par dédoublement de la multiplication des entiers naturels, la partie stable engendrée par l'ensemble $\{1\}$ contient $n \cdot 1 = n$ pour tout $n \in \mathbb{N}$, donc est identique à \mathbb{N} . On voit sur cet exemple la nécessité de bien distinguer une loi interne d'avec les lois externes qu'on en déduit par dédoublement, puisque, pour la multiplication des entiers naturels, $\{1\}$ est une partie stable. De façon générale, si une partie A de E est stable pour la loi externe à gauche (ou la loi externe à droite) déduite d'une loi interne τ , elle est aussi stable pour la loi τ ; mais la réciproque est inexacte, comme le prouve l'exemple précédent.

Si \perp est une loi externe partout définie entre opérateurs $\alpha \in \Omega$ et éléments $x \in E$, et si A est une partie stable de E pour cette loi, Φ une partie quelconque de Ω , la restriction de la fonction $\alpha \perp x$ à $\Phi \times A$ est une loi externe partout définie entre opérateurs $\alpha \in \Phi$ et éléments $x \in A$; on dit que c'est la loi *induite* par la loi \perp sur les ensembles Φ et A . Plus généralement :

DÉFINITION 3. — Soit \perp une loi de composition externe entre opérateurs $\alpha \in \Omega$ et éléments $x \in E$, définie sur $A \subset \Omega \times E$; on appelle loi induite par \perp entre opérateurs $\alpha \in \Phi$ et éléments $x \in F$, pour $\Phi \subset \Omega$ et $F \subset E$, la loi définie sur l'ensemble des $(\alpha, x) \in \Phi \times F$ tels que $(\alpha, x) \in A$ et $\alpha \perp x \in F$, et qui, à un tel couple (α, x) , fait correspondre le composé $\alpha \perp x$.

Si aucune confusion n'est à craindre, la loi induite par \perp pourra (par abus de langage) être désignée par le même signe. Lorsqu'on parle (sans autre indication) de la loi induite par \perp sur une partie F de E , on sous-entend toujours que $\Phi = \Omega$.

Lorsqu'on considère au contraire le cas où $F = E$, et $\Phi \subset \Omega$, on dit encore que la loi induite sur Φ et E est obtenue par *restriction* à l'ensemble Φ du domaine d'opérateurs de la loi donnée.

Exercice. — Soit \perp une loi externe partout définie entre opérateurs $\alpha \in \Omega$ et éléments $x \in E$. Soit F l'ensemble des applications de E dans E , G la partie de F formée des applications f_α produites par les opérateurs de la loi \perp , H la partie de F , stable pour la loi $f \circ g$, engendrée par G .

a) Montrer que toute partie de E , stable pour la loi \perp , est stable pour la loi $(f, x) \rightarrow f(x)$ entre opérateurs $f \in H$ et éléments $x \in E$, et réciproquement.

b) La partie stable pour la loi \perp , engendrée par une partie $X \subset E$, est identique à l'ensemble des $f(x)$, où f parcourt H et x parcourt X .

§ 4. — Structures algébriques.

1. Définition d'une structure algébrique.

L'objet de l'Algèbre est l'étude des structures déterminées par la donnée d'une ou plusieurs lois de composition, internes ou externes, entre les éléments d'un ou plusieurs ensembles. Le plus

souvent, tous ces ensembles, sauf un, sont considérés comme ensembles auxiliaires (*Ens. R*, § 8, n° 2), ce qui conduit à poser la définition suivante :

DÉFINITION 1. — *On appelle structure algébrique sur un ensemble E, toute structure déterminée sur E par une ou plusieurs lois de composition internes entre éléments de E, et une ou plusieurs lois de composition externes entre des domaines d'opérateurs Ω, Θ, \dots , et E, ces lois pouvant être assujetties à satisfaire à certaines conditions (par exemple l'associativité, la commutativité, etc.) ou à avoir entre elles certaines relations (voir § 5).*

Le nombre des lois internes et des lois externes d'une structure algébrique, ainsi que les conditions et relations auxquelles elles sont assujetties (et qui constituent les *axiomes* de la structure (*Ens. R*, § 8, n° 2)) caractérisent l'*espèce* (*Ens. R*, § 8, n° 2) de structure envisagée. On définira ainsi, dans ce chapitre et les suivants, les structures de groupe, de groupe à opérateurs, d'anneau, de corps, de module, etc..

Lorsqu'une structure algébrique \mathcal{G} est définie sur un ensemble E par la donnée de plusieurs lois de composition, les structures algébriques obtenues en ne considérant sur E que certaines des lois qui définissent \mathcal{G} sont dites *sous-jacentes* à \mathcal{G} .

Étant données deux structures algébriques de même espèce sur deux ensembles E et E', toute loi de composition interne de l'une des structures est associée à une loi de composition interne de l'autre, d'une manière bien déterminée par le schéma commun de formation des structures de l'espèce considérée ; il en est de même pour les lois externes. Inversement, si deux structures algébriques sont telles qu'il existe une correspondance biunivoque (explicitée) entre les lois de composition qui les déterminent, associant à toute loi interne de l'une une loi interne de l'autre et à toute loi externe de l'une une loi externe de l'autre, on peut toujours considérer ces deux structures comme étant de *même espèce* (à savoir, l'espèce des structures dont les lois internes et externes sont en nombre déterminé, mais ne sont assujetties à *aucune* autre condition). Deux lois externes associées sur E et E' peuvent avoir, ou non, le même domaine d'opérateurs ; lorsque pour tout couple de lois

externes associées sur E et E', les domaines d'opérateurs des deux lois sont les mêmes, on dit que les deux structures de même espèce considérées sont *homologues*.

La définition d'une structure algébrique entraîne naturellement une notion d'*isomorphisme* (*Ens. R*, § 8, n° 5) pour ces structures :

Étant données deux structures algébriques *homologues* sur E et E', un *isomorphisme* de E sur E' est une application biunivoque f de E sur E' telle que les lois internes sur E', et les lois externes entre les domaines d'opérateurs Ω, Θ, \dots (communs aux deux structures) et E', se déduisent des lois correspondantes sur E par *transport de structure* (*Ens. R*, § 8, n° 5) au moyen de l'application f et de l'application identique de chacun des domaines d'opérateurs sur lui-même.

Plus rarement, étant données deux structures de même espèce sur E et E', on aura affaire à un *transport de structure* au moyen d'une application biunivoque f de E sur E', et d'applications biunivoques quelconques ω, θ, \dots , des domaines d'opérateurs Ω, Θ, \dots , des lois externes de E sur les domaines d'opérateurs Ω', Θ', \dots , des lois externes correspondantes de E' (qui pourront, ou non, être identiques à Ω, Θ, \dots , respectivement) ; on dira alors qu'il s'agit d'un *poly-isomorphisme* de E, Ω, Θ, \dots , sur E', Ω', Θ', \dots , (*di-isomorphisme* s'il n'y a qu'un seul ensemble d'opérateurs pour l'espèce de structure envisagée).

Un isomorphisme de E sur lui-même s'appellera, comme toujours, un *automorphisme* de E ; un poly-isomorphisme de E, Ω, Θ, \dots , sur eux-mêmes s'appellera *poly-automorphisme* (*di-automorphisme* s'il n'y a qu'un seul domaine d'opérateurs).

2. Parties stables. Structure algébrique induite.

DÉFINITION 2. — *Etant donné un ensemble E muni d'une structure algébrique, une partie A de E sera dite stable (par rapport à la structure de E) si elle est stable par rapport à chacune des lois internes ou externes qui déterminent la structure de E.*

L'intersection d'une famille quelconque de parties stables de E est encore une partie stable ; en particulier, il existe une plus petite

partie stable contenant une partie donnée X de E , qui sera dite engendrée par X .

DÉFINITION 3. — *Etant donné un ensemble E muni d'une structure algébrique, on appelle structure induite par cette structure sur une partie F de E la structure déterminée sur F par les lois internes et externes induites sur F par les lois qui déterminent la structure de E .*

On dira souvent que la structure donnée sur E prolonge la structure qu'elle induit sur une partie de E .

Une structure algébrique sur E et la structure qu'elle induit sur une partie F de E peuvent toujours être considérées comme homologues (n° 1) ; mais, si la structure de E est d'une espèce déterminée, la structure induite ne sera pas nécessairement de cette espèce, même si F est une partie stable de E .

On verra par exemple au § 6 que la structure induite sur une partie stable F d'un groupe E par la structure de groupe de E , n'est pas en général une structure de groupe.

3. Structures quotients.

On considérera dans ce qui suit des relations d'équivalence R , S, \dots , entre éléments d'ensembles pourvus de structures algébriques. Comme il a été dit (*Ens. R*, § 5, n° 2), la relation R entre éléments x, y , s'écrira souvent $x \equiv y$ (mod. R) ou simplement $x \equiv y$ quand on n'a pas de confusion à craindre avec une autre relation.

DÉFINITION 4. — *Une loi de composition interne τ étant définie entre éléments d'un ensemble E , on dira qu'une relation d'équivalence R est compatible avec la loi τ si, chaque fois qu'on a $x \equiv x'$ (mod. R), $y \equiv y'$ (mod. R), et que les composés $x \tau y$ et $x' \tau y'$ sont définis, on a $x \tau y \equiv x' \tau y'$ (mod. R) ; la loi qui, aux classes d'équivalence de x et de y , fait correspondre la classe de $x \tau y$, est une loi de composition interne entre éléments de l'ensemble quotient E/R , qui s'appelle quotient de la loi τ par R .*

Si τ est partout définie, il en est de même de la loi quotient de τ par R ; si τ est associative, la loi quotient est associative ; si

τ est commutative, la loi quotient est commutative (on dit pour abréger que l'associativité et la commutativité se conservent en passant aux quotients). Si τ a un élément neutre e , la loi quotient a un élément neutre (à savoir la classe d'équivalence à laquelle appartient e) ; à deux éléments symétriques pour τ correspondent dans E/R des éléments symétriques pour la loi quotient, donc à un élément symétrisable de E correspond un élément symétrisable dans E/R . En revanche, à un élément régulier dans E ne correspond pas nécessairement un élément régulier dans E/R (voir l'exemple ci-dessous).

DÉFINITION 5. — *Une loi de composition externe \perp étant définie entre des opérateurs $\alpha \in \Omega$ et les éléments d'un ensemble E , on dira qu'une relation d'équivalence R entre éléments de E est compatible avec la loi \perp si, chaque fois qu'on a $x \equiv x'$ (mod. R) et que les composés $\alpha \perp x$ et $\alpha \perp x'$ sont définis, on a $\alpha \perp x \equiv \alpha \perp x'$ (mod. R) ; la loi qui, à α et à la classe d'équivalence de x , fait correspondre la classe d'équivalence de $\alpha \perp x$, est une loi externe entre opérateurs $\alpha \in \Omega$ et éléments de E/R , qui s'appelle quotient de la loi \perp par R .*

Si une relation R est compatible avec une loi interne τ , elle est compatible aussi, d'une part avec la loi opposée, d'autre part avec les deux lois externes qui se déduisent de τ par dédoublement. Par passage au quotient pour ces quatre lois, on obtient deux lois internes, opposées l'une de l'autre, entre éléments de E/R , et deux lois externes, entre opérateurs qui sont les éléments de E , et éléments de E/R .

Réciproquement, étant donnée une loi interne partout définie τ , soit R une relation d'équivalence compatible avec chacune des lois externes qui se déduisent de τ ; alors, les relations $x \equiv x'$ (mod. R), $y \equiv y'$ (mod. R) entraînent d'une part $x' \perp y \equiv x \perp y$ (mod. R), d'autre part $x' \perp y \equiv x' \perp y'$ (mod. R), donc $x \perp y \equiv x' \perp y'$ (mod. R) ; R est compatible avec τ .

On dira pour abréger qu'une relation R est compatible à gauche (resp. à droite) avec une loi interne τ , si elle est compatible avec la loi externe à gauche (resp. à droite) déduite de τ . On voit donc que :

PROPOSITION 1. — Pour qu'une relation d'équivalence soit compatible avec une loi interne partout définie, il faut et il suffit qu'elle soit compatible à gauche et à droite avec cette loi.

DÉFINITION 6. — Soit E un ensemble muni d'une structure algébrique définie par des lois de composition internes ou externes ; on dira qu'une relation d'équivalence R entre éléments de E est compatible avec la structure de E si elle l'est avec toutes ces lois ; la structure définie sur le quotient E/R par les quotients de ces lois par R s'appelle la structure quotient par R de celle de E : et E/R muni de cette structure s'appelle le quotient par R de l'ensemble E muni de la structure donnée.

Ici encore, la structure quotient sur E/R peut toujours être considérée comme *homologue* de la structure donnée sur E ; mais, si cette dernière est d'une espèce déterminée, il y aura lieu dans chaque cas de vérifier si la structure quotient est aussi de cette même espèce (il en est bien ainsi, en particulier, pour les groupes quotients, anneaux quotients, etc., qui seront définis dans la suite de ce chapitre).

Exemple : Congruences dans \mathbf{Z} .

Soit $a \in \mathbf{Z}$; la relation entre éléments x, y de \mathbf{Z} qui s'énonce « il existe $z \in \mathbf{Z}$ tel que $x - y = az$ » est une relation d'équivalence, que l'on convient, une fois pour toutes, d'écrire $x \equiv y \pmod{a}$ ou plus brièvement $x \equiv y (a)$, et qui s'appelle une *congruence modulo a*. En remplaçant a par $-a$, on obtient une relation équivalente, donc on pourra supposer $a \geq 0$; pour $a = 0$, $x \equiv y (0)$ signifie $x = y$, donc on n'aura de relation distincte de l'égalité que si $a \neq 0$: aussi supposerons-nous par la suite que $a > 0$ sauf indication formelle du contraire.

Pour $a > 0$, le quotient de \mathbf{Z} par la congruence $x \equiv y (a)$ est un *ensemble fini de a éléments*, appelé *ensemble des entiers rationnels modulo a* ; cela va résulter de la propriété suivante, qui généralise aux entiers rationnels la *division euclidienne* des entiers naturels (*Ens.*, chap. III) :

Si $a \in \mathbf{N}^$ et $x \in \mathbf{Z}$, il existe deux entiers rationnels bien déterminés q et r, tels que $x = qa + r$ et $0 \leq r \leq a - 1$.*

En effet, si $x = qa + r$ et $0 \leq r \leq a - 1$, on a $qa \leq x < (q + 1)a$,

d'où $ma \leq x$ pour $m \leq q$ et $ma > x$ pour $m > q$; par suite, q (s'il existe) est bien déterminé comme le plus grand élément de l'ensemble des $m \in \mathbf{Z}$ tels que $ma \leq x$. Or l'existence de q a été démontrée lorsque $x \geq 0$ (*Ens.*, chap. III) ; dans le cas contraire, il existe $q' \in \mathbf{Z}$ tel que $q'a \leq -x < (q' + 1)a$; on aura donc $qa \leq x < (q + 1)a$ en prenant $q = -q'$ si $-x = q'a$, $q = -(q' + 1)$ si $q'a < -x$.

Le nombre r ainsi déterminé s'appelle le *reste de x modulo a* ; pour que $x \equiv y (a)$, il faut et il suffit que x et y aient même reste modulo a , car deux entiers naturels appartenant à l'intervalle $[0, a - 1]$ ne peuvent être congrus (mod. a) que s'ils sont égaux. Il s'ensuit que le quotient de \mathbf{Z} par la relation $x \equiv y (a)$ est en correspondance biunivoque avec l'intervalle $[0, a - 1]$, donc est un ensemble de a éléments, qu'on identifie souvent avec cet intervalle.

Quel que soit $a \in \mathbf{Z}$, la relation $x \equiv y (a)$ est *compatible* avec l'addition et avec la multiplication dans \mathbf{Z} , comme on le vérifie immédiatement ; par passage au quotient, on obtient donc pour $a > 0$ des lois de composition associatives et commutatives qui s'appellent *addition* et *multiplication modulo a*. Quand on identifie l'ensemble quotient de \mathbf{Z} par la congruence modulo a avec l'intervalle $[0, a - 1]$, la somme modulo a (resp. le produit modulo a) de deux éléments r, s de cet intervalle est le reste modulo a de leur somme $r + s$ dans \mathbf{Z} (resp. de leur produit rs dans \mathbf{Z}).

La relation $x \equiv 0 \pmod{a}$ s'énonce aussi « x est multiple de a », « a est diviseur de x », « a divise x ».

On notera que si x est un multiple $\neq 0$ de a , x est régulier pour la multiplication dans \mathbf{Z} , mais sa classe (mod. a) n'est pas un élément régulier pour la multiplication modulo a .

Il est immédiat que le quotient de \mathbf{N} par la relation induite sur \mathbf{N} par $x \equiv y (a)$, est identique à l'ensemble des entiers rationnels modulo a ; l'addition et la multiplication modulo a s'obtiennent également en prenant les lois quotients, par cette relation induite, de l'addition et de la multiplication dans \mathbf{N} .

Au § 6, nous verrons que les relations de congruence $x \equiv y (a)$ sont les *seules* relations d'équivalence dans \mathbf{Z} compatibles avec l'addition.

4. Représentations ; homomorphismes.

DÉFINITION 7. — Soient E et F deux ensembles munis de structures algébriques homologues, et f une application de E dans F . Les lois de composition correspondantes sur E et F étant notées par un même signe, f s'appellera une représentation de E dans F si :

1^o Pour chacune des lois de composition internes τ données sur E et F , chaque fois que $x \tau y$ est défini, $f(x) \tau f(y)$ est défini et on a $f(x \tau y) = f(x) \tau f(y)$;

2^o Pour chacune des lois externes α données sur E et F , chaque fois que $\alpha \alpha x$ est défini, $\alpha \alpha f(x)$ est défini et on a $f(\alpha \alpha x) = \alpha \alpha f(x)$.

La déf. 7 implique en particulier que, pour chacune des lois internes τ données sur E et F , f est une représentation de E dans F pour les structures déterminées par ces seules lois (§ 1, n° 1) ; il en résulte que si une loi τ sur E admet un élément neutre e , $f(e)$ est élément neutre pour la loi induite par τ sur $f(E)$; si x et x' sont symétriques dans E pour la loi τ , $f(x)$ et $f(x')$ sont symétriques dans $f(E)$ pour la loi induite par τ (§ 2, n°s 1 et 3). Si les lois τ sont partout définies sur E et F , on a, pour toute séquence $(x_\lambda)_{\lambda \in L}$ d'éléments de E , l'identité

$$(1) \quad f\left(\bigcap_{\lambda \in L} x_\lambda\right) = \bigcap_{\lambda \in L} f(x_\lambda)$$

comme on le voit immédiatement par récurrence sur le nombre d'éléments de L .

Soient X et Y deux parties quelconques de E . Si toutes les lois de composition sur E et F sont partout définies, on a, pour chacune des lois internes τ sur E et F , $f(X \tau Y) = f(X) \tau f(Y)$, et pour chacune des lois externes α et pour un opérateur quelconque α de cette loi, $f(\alpha \alpha X) = \alpha \alpha f(X)$. Autrement dit, l'extension de f aux ensembles de parties (*Ens. R*, § 2, n° 4) est une représentation de $\mathfrak{P}(E)$ dans $\mathfrak{P}(F)$.

Lorsque toutes les lois de composition qui déterminent la structure de E sont partout définies, une représentation f de E dans F s'appelle encore un *homomorphisme* (*) de E dans F ; on dit que

(*) Lorsque E et F sont munis de certaines structures algébriques et en outre de topologies satisfaisant à certaines conditions, le terme « homomorphisme »

c'est un homomorphisme de E sur F si $f(E) = F$; un homomorphisme de E dans lui-même s'appelle un *endomorphisme* de E .

Lorsqu'il existe un homomorphisme de E sur F , on dit que la structure de F est *homomorphe* à celle de E (ou en *homomorphie* avec celle de E). Les structures homomorphes à une structure donnée sont caractérisées par le théorème suivant, dont la démonstration est immédiate à partir des définitions :

THÉORÈME 1 (théorème d'homomorphie). — Soient E et F deux ensembles munis de structures algébriques homologues, les lois de composition de E étant partout définies. Si f est un homomorphisme de E dans F , l'image $f(E)$ est une partie stable de F , qui, munie de la structure induite par celle de F , est isomorphe au quotient de E par la relation d'équivalence $f(x) = f(y)$ (relation qui est compatible avec la structure de E).

Le théorème peut être en défaut si les lois de composition de E ne sont pas partout définies, car le composé de $f(x)$ et $f(y)$ pour une loi interne sur F peut alors être défini sans que le composé de x et y pour la loi correspondante sur E le soit, et de même pour les lois externes.

Si un homomorphisme f de E dans F est biunivoque, $f(E)$ est isomorphe à E d'après le th. 1 : on dit alors que f est un *isomorphisme* de E dans F . Pour toute partie stable A d'un ensemble E dont toutes les lois de composition sont partout définies, l'application canonique de A dans E est un isomorphisme de A (munie de la structure induite par celle de E) dans E , qu'on appelle *isomorphisme canonique* de A dans E .

Si R est une relation d'équivalence compatible avec une structure algébrique sur un ensemble E , l'application canonique de E sur E/R est une représentation, dite *représentation canonique* de E sur E/R (ou *homomorphisme canonique* de E sur E/R lorsque toutes les lois de composition de E sont partout définies).

En se bornant au cas où les lois de composition de E et F sont partout définies, le th. 1 montre que la *décomposition canonique* (*Ens. R*, § 5, n° 3) d'un homomorphisme f de E dans F donne, en désignant par R la relation d'équivalence $f(x) = f(y)$:

4

sera employé dans une acception plus restreinte, et ne sera plus synonyme de « représentation » (cf. *Top. gén.*, chap. III, § 2) ; mais tant qu'il n'intervient aucune structure topologique, cette synonymie ne présente aucun inconvénient.

- 1^o l'isomorphisme canonique de $f(E)$ dans F ;
- 2^o un isomorphisme de E/R sur $f(E)$, qu'on appelle *représentation biunivoque associée à f* ;
- 3^o l'homomorphisme canonique de E sur E/R .

PROPOSITION 2. — Soient E, F, G , trois ensembles munis de structures algébriques homologues, f une représentation de E dans F , g une représentation de F dans G ; l'application composée $g \circ f$ est une représentation de E dans G .

La proposition résulte immédiatement de la déf. 7.

PROPOSITION 3. — Soient E un ensemble muni d'une structure algébrique, R une relation d'équivalence compatible avec cette structure, f la représentation canonique de E sur E/R . Pour qu'une application g de E/R dans un ensemble F muni d'une structure homologue à celle de E , soit une représentation, il faut et il suffit que $g \circ f$ soit une représentation de E dans F .

La nécessité de la condition résulte de la prop. 2; on vérifie aisément que la condition est suffisante; pour une loi interne τ , si le composé $u \tau v$ de deux éléments de E/R est défini, il existe dans E un élément x de la classe u , et un élément y de la classe v tels que $x \tau y$ soit défini; donc $g(f(x)) \tau g(f(y))$ est défini et égal à $g(f(x \tau y))$, c'est-à-dire que $g(u) \tau g(v)$ est défini et égal à $g(u \tau v)$; raisonnement analogue pour les lois externes.

Dans le reste de ce n°, nous considérerons un ensemble E muni d'une structure algébrique déterminée par des lois de composition *partout définies*. En conservant les notations de la prop. 3, désignons par S la relation $g(x') = g(y')$ dans E/R , par T la relation $g(f(x)) = g(f(y))$ dans E ; S est le quotient T/R de T par R

Ens. R, § 5, n° 9; d'après le th. 1, l'image de E/R par g est isomorphe au quotient $(E/R)/S$; mais cette image est aussi l'image de E par $g \circ f$, et le th. 1 montre qu'elle est isomorphe au quotient E/T . En prenant pour g l'homomorphisme canonique de E/R sur $(E/R)/S$, on a donc le théorème suivant :

THÉORÈME 2 (Premier théorème d'isomorphie). — Soit E/R le quotient d'un ensemble E , muni d'une structure algébrique, par une relation d'équivalence R compatible avec cette structure. Toute

relation d'équivalence S dans E/R , compatible avec la structure quotient de E/R , est de la forme T/R , où T est une relation d'équivalence dans E , entraînée par R et compatible avec la structure de E ; et réciproquement. En outre, l'application canonique de E/T sur $(E/R)/(T/R)$ est un isomorphisme.

Désignons toujours par f l'homomorphisme canonique de E sur E/R ; soit A une partie stable de E , munie de la structure induite par celle de E ; la restriction de f à A est une représentation de A dans E/R , et, d'après le th. 1, $f(A)$ est isomorphe au quotient A/R_A de A par la relation R_A induite par R dans A (*Ens. R, § 5, n° 5*). Soit B la partie de E obtenue en saturant A pour la relation R (*Ens. R, § 5, n° 6*); B est encore une partie stable de E . En effet, soient $x \in B$, $y \in B$; il existe par définition $x' \in A$ et $y' \in A$ tels que $x \equiv x'$ et $y \equiv y'$ (mod. R); pour l'une des lois internes τ qui définissent la structure de E , on aura $x' \tau y' \in A$ et $x \tau y \equiv x' \tau y'$ (mod. R), donc $x \tau y \in B$; de même pour les lois externes. Comme B/R_B est isomorphe à $f(B)$, et que $f(B) = f(A)$, on voit que :

THÉORÈME 3 (Second théorème d'isomorphie). — Soient E un ensemble muni d'une structure algébrique, A une partie stable de E , R une relation d'équivalence dans E compatible avec la structure de E . L'ensemble B déduit de A en le saturant pour R est stable; si R_A et R_B sont les relations induites par R sur A et sur B par celle de E , et l'application canonique (*) de A/R_A sur B/R_B est un isomorphisme.

5. Produits de structures algébriques.

DÉFINITION 8 — Soit $(E_i)_{i \in I}$ une famille d'ensembles, pour tous tous de structures algébriques homologues, et soit $E = \prod_{i \in I} E_i$ leur produit. On suppose que chacune des lois (internes ou externes)

(*) Cette application canonique (composée de l'application canonique de $f(B) = f(A)$ sur B/R_B , et de l'application canonique de A/R_A sur $f(A)$) fait donc correspondre à toute classe (mod. R_A) dans A , la classe (mod. R) dans E qui la contient.

caractéristique de l'espèce de structure envisagée, est notée par un même signe sur tous les E_i .

1^o Pour une loi interne notée τ sur les E_i , et pour $x = (x_i), y = (y_i)$ on pose $x \tau y = (x_i \tau y_i)$ chaque fois que $x_i \tau y_i$ est défini pour tout $i \in I$; la loi de composition interne ainsi définie sur E s'appelle produit des lois τ sur les E_i .

2^o Pour une loi externe notée \perp sur les E_i , un opérateur α relatif à ces lois, et $x = (x_i)$, on pose $\alpha \perp x = (\alpha \perp x_i)$ chaque fois que $\alpha \perp x_i$ est défini pour tout $i \in I$; la loi de composition externe ainsi définie sur E s'appelle produit des lois \perp sur les E_i .

3^o Si, pour chacune des lois caractéristiques de l'espèce de structure envisagée, on forme sur E le produit des lois correspondantes sur les E_i , la structure déterminée sur E par toutes ces lois produits s'appelle le produit des structures des E_i ; et E , muni de cette structure, s'appelle le produit des E_i munis des structures données.

La structure produit est évidemment homologue aux structures données sur les E_i ; mais si celles-ci appartiennent toutes à une même espèce déterminée, il y aura lieu d'examiner dans chaque cas si la structure produit est ou non de cette espèce.

On verra par la suite des exemples pour lesquels il en est toujours ainsi (structures de groupe, d'anneau, etc.), et aussi des exemples du contraire (structure de corps).

Avec les notations de la déf. 8, si A_i est une partie stable de E_i , $A = \prod_{i \in I} A_i$ est une partie stable de E , et la structure induite sur A par celle de E est le produit de celles qui sont induites sur les A_i par celles des E_i . L'application pr_i de E dans E_i est une représentation de E sur E_i ; de même la projection sur un produit partiel $\prod_{i \in J} E_i$ quelconque. Si $(I_x)_{x \in K}$ est une partition

de I , et si on pose $F_x = \prod_{i \in I_x} E_i$, l'application canonique (Ens.

R, § 4, n° 11) de E sur $\prod_{x \in K} F_x$ est un isomorphisme.

Si f_i est une représentation d'un ensemble F (muni d'une structure homologue à celles des E_i) dans E_i , $f = (f_i)$ est une représentation de F dans E .

Soit $(F_i)_{i \in I}$ une seconde famille d'ensembles munis de structures algébriques homologues à celles des E_i , ayant même ensemble d'indices; si, pour chaque i , f_i est une représentation de E_i dans F_i , l'application $(x_i) \rightarrow (f_i(x_i))$ est une représentation de $\prod_{i \in I} E_i$ dans $\prod_{i \in I} F_i$.

En particulier, si I est un ensemble à deux éléments, et les f_i les représentations canoniques sur des quotients, on a la proposition suivante :

PROPOSITION 4. — Soient E et F deux ensembles munis de structures algébriques homologues, R une relation d'équivalence compatible avec la structure de E , S une relation d'équivalence compatible avec la structure de F . L'application canonique de $(E/R) \times (F/S)$ sur $(E \times F)/(R \times S)$ (Ens. R, § 5, n° 10) est un isomorphisme.

S'il s'agit de structures déterminées sur chacun des E_i par une seule loi interne (notée τ pour tous les E_i), et si les lois τ sont toutes associatives, leur produit l'est aussi; pour que deux éléments $(x_i), (y_i)$ soient permutables pour la loi produit, il faut et il suffit que, pour tout i , x_i et y_i soient permutables; en particulier, si toutes les lois τ sont commutatives, leur produit l'est aussi; on dira encore, pour abréger, que l'associativité et la commutativité se conservent en passant aux produits. Pour que la loi produit ait un élément neutre $e = (e_i)$, il faut et il suffit que, pour tout i , e_i soit élément neutre dans E_i ; pour que $x = (x_i)$ soit régulier pour la loi produit, il faut et il suffit que chacun des x_i soit régulier dans E_i ; pour que $x = (x_i)$ et $y = (y_i)$ soient symétriques, il faut et il suffit que, pour tout i , x_i et y_i soient symétriques.

Enfin, considérons le cas où tous les E_i sont identiques à un même ensemble F , muni d'une structure algébrique quelconque; E est alors l'ensemble F^I des applications $i \rightarrow f(i)$ de I dans F ; pour chaque loi interne τ sur F , le composé $f \tau g$ de deux telles applications est l'application $i \rightarrow f(i) \tau g(i)$; et pour chaque

loi externe \perp sur F , le composé $\alpha \perp f$ de l'opérateur α et de l'application f est l'application $\iota \rightarrow \alpha \perp f(\iota)$.

Z

Lorsque $I = F$, il importe de distinguer soigneusement les lois de composition $f \tau g$ entre applications de F dans F , et la loi $(f, g) \rightarrow f \circ g$.

Exercices. — 1) On considère sur un ensemble E une structure algébrique déterminée par la donnée de plusieurs lois externes. Montrer qu'on peut (à un poly-isomorphisme près), considérer ces lois comme les lois obtenues par *restriction d'une seule loi externe* à certaines parties du domaine d'opérateurs de \perp (considérer un ensemble « somme » (*Ens. R*, § 4, no 5) des ensembles d'opérateurs des diverses lois externes données sur E). Les parties stables de E sont les mêmes pour la structure donnée et celle déterminée par la seule loi \perp ; toute relation d'équivalence compatible avec la structure donnée est compatible avec la loi \perp , et réciproquement.

2) On rappelle qu'en identifiant (par abus de langage) les relations d'équivalence dans un ensemble E et les parties de $E \times E$ définies par ces relations (*Ens.*, chap. II), on dit qu'une relation d'équivalence R contient une relation d'équivalence S si la partie de $E \times E$ définie par R contient la partie définie par S (ce qui revient à dire que S entraîne R) ; on parle de même d'*intersection* d'une famille de relations d'équivalence.

a) Étant donnée une structure algébrique sur un ensemble E , montrer que l'intersection d'une famille de relations d'équivalence compatibles avec la structure de E est une relation d'équivalence compatible avec cette structure.

b) Étant donnés deux éléments a, b de E , parmi toutes les relations d'équivalence R compatibles avec la structure de E , et telles que $a \equiv b$ (mod. R), il en existe une contenue dans toutes les autres ; on dit que cette relation $R_{a, b}$ est la relation d'équivalence obtenue en *identifiant* a et b , et que l'ensemble quotient $E/R_{a, b}$ est l'ensemble quotient obtenu en identifiant a et b .

c) Si R est une relation d'équivalence compatible avec la structure de E , il existe une famille de couples (a_i, b_i) d'éléments de E , telle que R soit la plus petite relation d'équivalence contenant toutes les relations R_{a_i, b_i} ; on dit que E/R est l'ensemble quotient obtenu en identifiant a_i et b_i pour tout i .

¶ 3) Soit E un monoïde (§ 1, no 2) noté multiplicativement.

a) Si A est une partie quelconque de E , la relation $\gamma_x^{-1}(A) = \gamma_y^{-1}(A)$ entre éléments x et y de E est une relation d'équivalence compatible à droite avec la loi de E , qu'on notera $R_d(A)$.

b) Si R est une relation d'équivalence compatible à droite

avec la loi de E , et A une classe quelconque (mod. R), montrer que R entraîne $R_d(A)$, et que l'intersection (exerc. 2) des relations $R_d(A)$, où A parcourt l'ensemble des classes mod. R , est la relation d'équivalence (entre éléments x et y de E) : « quel que soit z , $xz \equiv yz$ (mod. R) ».

c) On dit qu'une partie A de E est un ensemble *séparateur* si la relation $\gamma_x^{-1}(A) \cap \gamma_y^{-1}(A) \neq \emptyset$ entraîne $\gamma_x^{-1}(A) = \gamma_y^{-1}(A)$. Montrer que si A est séparateur, la relation $\delta_x^{-1}(A) \cap \delta_y^{-1}(A) \neq \emptyset$ entraîne $\delta_x^{-1}(A) = \delta_y^{-1}(A)$, et que les classes d'équivalence mod. $R_d(A)$ sont les ensembles $\delta_x^{-1}(A)$, où x parcourt E , et l'ensemble $W(A)$ des $x \in E$ tels que $\gamma_x^{-1}(A) = \emptyset$. Soit F le complémentaire de $W(A)$ dans E ; dans les mêmes conditions, prouver que les relations $xz \in F$, $yz \in F$, $xz \equiv yz$ (mod. $R_d(A)$) entraînent $x \equiv y$ (mod. $R_d(A)$).

d) Soit R une relation d'équivalence compatible à droite avec la loi de E , et telle que la relation $xz \equiv yz$ (mod. R) entraîne $x \equiv y$ (mod. R). Montrer que toute classe mod. R est un ensemble séparateur ; avec les notations précédentes, si A est une classe mod. R , les relations induites sur le complémentaire F de $W(A)$ par R et $R_d(A)$ sont équivalentes.

4) Montrer que toute relation d'équivalence dans Z , compatible avec l'addition, est de la forme $x \equiv y (a)$, avec $a \in Z$ (montrer que la classe de 0 pour une telle relation, est de la forme $a \cdot Z$, en considérant le plus petit élément > 0 de cette classe, s'il existe). En déduire qu'avec les notations de l'exerc. 7 du § 2, si l'ensemble C est un ensemble fini de p éléments, il est isomorphe à l'ensemble des entiers modulo p (muni de l'addition modulo p) ; il en est de même de l'ensemble désigné par D dans l'exerc. 8 du § 2, s'il a p éléments.

5) Soient E et E' deux ensembles munis de structures algébriques homologues, et f une représentation de E dans E' . Montrer que, si A' est une partie stable de E' , $f(A')$ est une partie stable de E .

6) Dans le monoïde libre $L(A)$ déduit d'un ensemble A , on considère la relation R entre deux mots $u = (a_i)_{0 \leq i \leq n}$, $v = (b_i)_{0 \leq i \leq n}$: « il existe une permutation π de l'intervalle $[0, n]$ telle que $b_i = a_{\pi(i)}$ » (autrement dit, les suites (a_i) et (b_i) ne diffèrent que par l'ordre des termes). Montrer que R est une relation d'équivalence compatible avec la juxtaposition dans $L(A)$; l'ensemble quotient $L(A)/R$ est appelé le *monoïde abélien libre* déduit de A ; montrer qu'il est isomorphe à la partie stable de l'ensemble produit N^A (muni du produit des lois additives des facteurs N) formée

des familles $(n_\alpha)_{\alpha \in A}$ d'entiers naturels telles que $n_\alpha = 0$ sauf pour un nombre fini d'indices α .

§ 5. — Relations entre lois de composition.

Dans la définition de la plupart des structures algébriques figurent plusieurs lois de composition, assujetties à avoir entre elles certaines relations ; les types de relations dont il s'agit sont assez variés : nous allons énumérer ici les principaux, et indiquer comment il est d'usage de les mettre en évidence dans les notations.

1. Distributivité.

DÉFINITION 1. — Une loi externe partout définie \perp entre opérateurs $\alpha \in \Omega$ et éléments d'un ensemble E , est dite distributive par rapport à une loi interne τ entre éléments de E , si, chaque fois que le composé $x \tau y$ est défini, le composé $(\alpha \perp x) \tau (\alpha \perp y)$ est défini pour tout $\alpha \in \Omega$, et satisfait à

$$(1) \quad \alpha \perp (x \tau y) = (\alpha \perp x) \tau (\alpha \perp y).$$

Cette définition équivaut à dire que, pour tout $\alpha \in \Omega$, l'application $x \rightarrow \alpha \perp x$ est une *représentation* de Ω dans E , relativement à la structure déterminée sur E par la seule loi interne τ .

Nous nous bornerons à considérer dans ce qui suit le cas où la loi τ est partout définie. La remarque précédente, et l'identité (1) du § 4, montrent alors que, pour toute séquence $(x_\lambda)_{\lambda \in L}$ d'éléments de E , on a

$$(2) \quad \alpha \perp \left(\bigcap_{\lambda \in L} x_\lambda \right) = \bigcap_{\lambda \in L} (\alpha \perp x_\lambda).$$

Lorsque la loi interne considérée est écrite multiplicativement, on emploie fréquemment la notation exponentielle x^z pour une loi externe distributive par rapport à cette multiplication, de sorte que la distributivité s'exprime par l'identité $(xy)^z = x^z y^z$. Si la loi interne est notée additivement, on emploie fréquemment la notation additive à gauche $\alpha \cdot x$, ou à droite $x \cdot \alpha$, pour une loi externe distributive par rapport à cette addition, la distributivité s'exprimant respectivement par les identités $\alpha(x + y) = \alpha x + \alpha y$, $(x + y)\alpha = x\alpha + y\alpha$.

DÉFINITION 2. — Soient \perp une loi externe partout définie entre opérateurs $\alpha \in \Omega$ et éléments de E , τ une loi interne entre éléments de E , $\bar{\tau}$ une loi interne entre éléments de Ω . On dit que la loi \perp est distributive par rapport à l'ensemble des deux lois τ , $\bar{\tau}$, si, chaque fois que le composé $\alpha \bar{\tau} \beta$ est défini, le composé $(\alpha \perp x) \tau (\beta \perp x)$ est défini pour tout $x \in E$, et satisfait à

$$(3) \quad (\alpha \bar{\tau} \beta) \perp x = (\alpha \perp x) \tau (\beta \perp x).$$

On aura soin de distinguer cette distributivité de celle définie plus haut : la distributivité de \perp par rapport à l'ensemble des deux lois τ , $\bar{\tau}$, n'entraîne nullement la distributivité de \perp par rapport à la loi τ (voir les exemples ci-après).

La déf. 2 équivaut à dire que pour tout $x \in E$, l'application $\alpha \rightarrow \alpha \perp x$ est une *représentation* de Ω dans E (pour les structures déterminées par $\bar{\tau}$ et τ respectivement).

Nous ne considérerons encore dans ce qui suit que le cas où les lois τ et $\bar{\tau}$ sont partout définies. Le plus souvent, les lois internes considérées sur Ω et E seront notées additivement (donc (§ 2, n° 7) seront associatives et commutatives) ; on emploiera alors pour une loi externe distributive par rapport à l'ensemble des deux lois internes, la notation multiplicative, soit à gauche, soit à droite, la distributivité s'exprimant respectivement par les identités $(\alpha + \beta)x = \alpha x + \beta x$, $x(\alpha + \beta) = x\alpha + x\beta$.

Avec la notation multiplicative à gauche $\alpha \cdot x$, on dit en général que la loi externe est *distributive à gauche* si on a l'identité $(\alpha + \beta)x = \alpha x + \beta x$, l'identité $\alpha(x + y) = \alpha x + \alpha y$ exprimant ce qu'on appelle la *distributivité à droite* (c'est-à-dire la distributivité de la loi externe par rapport à l'addition dans E) ; ces dénominations s'échangent pour une loi notée $x \cdot \alpha$. Avec les mêmes notations, la loi externe est dite *doublement distributive* (par rapport aux deux lois internes) si elle est distributive à gauche et à droite. Alors, si $(x_\lambda)_{\lambda \in L}$ est une famille finie d'éléments de E , $(\alpha_i)_{i \in I}$ une famille finie d'éléments de Ω , on a

$$(4) \quad \left(\sum_{i \in I} \alpha_i \right) \cdot \left(\sum_{\lambda \in L} x_\lambda \right) = \sum_{(i, \lambda) \in I \times L} (\alpha_i \cdot x_\lambda)$$

(et la formule analogue pour la notation à droite), comme on le voit par récurrence sur le nombre des éléments de I et L .

DÉFINITION 3. — *Etant données deux lois internes τ , \perp sur un ensemble E, on dit que la loi \perp est doublement distributive par rapport à la loi τ si elle est partout définie et si chacune des lois externes, déduites de \perp par dédoublement, est distributive par rapport à τ .*

Le plus souvent, il s'agit de lois internes dont l'une est notée additivement (donc est associative et commutative), et l'autre multiplicativement (donc est associative) ; avec ces notations, la double distributivité de la multiplication par rapport à l'addition s'exprime par les identités $x(y+z) = xy + xz$ et $(y+z)x = yx + zx$.

Lorsque la multiplication est *commutative*, ces deux identités sont équivalentes ; si elles sont satisfaites, on dit alors simplement (par abus de langage) que la multiplication est *distributive* par rapport à l'addition. Dans les mêmes conditions, si $(S_\alpha)_{\alpha \in A}$ est une famille finie dont les éléments sont des familles finies $S_\alpha = (x_{\alpha\lambda})_{\lambda \in L_\alpha}$ d'éléments de E, on a l'identité dite « formule générale de distributivité » :

$$(5) \quad \prod_{\alpha \in A} \left(\sum_{\lambda \in L_\alpha} x_{\alpha\lambda} \right) = \sum_{\lambda(\alpha) \in \prod L_\alpha} \left(\prod_{\alpha \in A} x_{\alpha, \lambda(\alpha)} \right)$$

qu'on vérifie par récurrence sur le nombre d'éléments de A.

Exemples. — 1) Si une loi notée multiplicativement est associative et commutative dans E, la loi $(n, x) \rightarrow x^n$ entre opérateurs $n \in N^*$ et éléments $x \in E$ est distributive par rapport à la multiplication dans E (§ 1, formule (8)) : il n'en sera pas ainsi en général si la multiplication n'est pas commutative. Si la multiplication, associative et commutative, admet de plus un élément neutre, la loi x^n sera distributive pour $n \in N$; elle le sera pour $n \in Z$ si de plus tout élément de E est inversible.

Les mêmes résultats subsistent pour une loi interne associative et commutative, notée additivement, la notation x^n étant remplacée par $n.x$.

2) Si une loi notée multiplicativement est associative dans E, la loi $(n, x) \rightarrow x^n$ est distributive par rapport à l'ensemble formé de l'addition dans N^* et de la multiplication dans E, puisque $x^{m+n} = x^m x^n$. Si la multiplication considérée est commutative, la loi x^n est donc doublement distributive. Ces résultats s'étendent pour $n \in Z$, lorsque tout élément de E est inversible.

2

3) Pour $X \subset E$, $K \subset E \times E$, la loi de composition externe $(K, X) \rightarrow K(X)$ entre opérateurs K et éléments X de $\mathfrak{P}(E)$ est distributive par rapport à la loi interne \cup dans $\mathfrak{P}(E)$, mais non par rapport à \cap (Ens. R, § 3, no 8) ; elle est aussi distributive par rapport à l'ensemble des deux lois internes \cup dans $\mathfrak{P}(E)$ et $\mathfrak{P}(E \times E)$, c'est-à-dire que, si $K = K' \cup K''$,

$$K(X) = K'(X) \cup K''(X).$$

On a des résultats analogues pour la loi externe $A \circ X$ entre opérateurs $A \subset F \times F$ et éléments X de $\mathfrak{P}(E \times F)$.

4) Dans $\mathfrak{P}(E)$, chacune des lois internes \cup , \cap est (doublement) distributive par rapport à l'autre.

5) Dans Z , la multiplication est distributive par rapport à l'addition ; l'addition est distributive par rapport à $\sup(x, y)$ et $\inf(x, y)$, et chacune des deux dernières lois est distributive par rapport à l'autre et par rapport à elle-même. Dans N , la multiplication est aussi distributive par rapport à $\sup(x, y)$ et $\inf(x, y)$.

6) Soit τ une loi interne sur un ensemble E ; la loi externe à droite déduite de la loi $f \circ g$ est distributive par rapport à la loi $f \tau g$ entre applications de E dans E, c'est-à-dire que $(f \tau g) \circ h = (f \circ h) \tau (g \circ h)$; il n'en est pas de même pour la loi externe à gauche déduite de $f \circ g$.

Comme l'associativité et la commutativité, les diverses sortes de distributivité définies ci-dessus se conservent en passant aux quotients ou aux produits. De façon précise, si par exemple, sur un ensemble E, une loi interne \perp est doublement distributive par rapport à une loi interne τ , et si R est une relation d'équivalence compatible avec les lois \perp et τ , la loi quotient par R de la loi \perp est doublement distributive par rapport à la loi quotient par R de la loi τ ; de même pour les autres sortes de distributivité, et le passage aux produits.

2

Remarque. — Si \perp est une loi externe distributive par rapport à une loi interne τ sur E, A et B deux parties de E, Φ une partie de l'ensemble Ω des opérateurs de la loi \perp , on n'a pas en général $\Phi \perp (A \tau B) = (\Phi \perp A) \tau (\Phi \perp B)$ (autrement dit, l'extension de la loi \perp aux ensembles de parties n'est pas distributive par rapport à l'extension de la loi τ) : en effet, $\Phi \perp (A \tau B)$ est l'ensemble des éléments $\alpha \perp (x \tau y) = (\alpha \perp x) \tau (\alpha \perp y)$ pour $\alpha \in \Phi$, $x \in A$, $y \in B$; tandis que $(\Phi \perp A) \tau (\Phi \perp B)$ est l'ensemble des éléments $(\alpha \perp x) \tau (\beta \perp y)$ pour $\alpha \in \Phi$, $\beta \in \Phi$, $x \in A$, $y \in B$; on peut seulement écrire, en général, $\Phi \perp (A \tau B) \subset (\Phi \perp A) \tau (\Phi \perp B)$. En outre, pour tout $\alpha \in \Omega$, on a évidemment

$$\alpha \perp (A \tau B) = (\alpha \perp A) \tau (\alpha \perp B).$$

2. Associativité.

DÉFINITION 4. — Soient \perp une loi externe partout définie entre opérateurs $\alpha \in \Omega$ et éléments d'un ensemble E , τ une loi interne associative partout définie entre éléments de Ω ; on dit que la loi \perp est associative par rapport à la loi τ si on a l'identité

$$(6) \quad (\alpha \tau \beta) \perp x = \alpha \perp (\beta \perp x).$$

En d'autres termes, si on pose $f_\alpha(x) = \alpha \perp x$ (f_α) $_{\alpha \in \Omega}$ étant donc la famille des applications de E dans E produites par les opérateurs de la loi \perp) on doit avoir $f_{\alpha \tau \beta} = f_\alpha \circ f_\beta$, c'est-à-dire que l'application $\alpha \rightarrow f_\alpha$ est une *représentation* de Ω (avec la loi τ) dans l'ensemble des applications de E dans E (muni de la loi $f \circ g$).

Si une loi externe est associative par rapport à une loi interne (sur son domaine d'opérateurs), et si cette dernière est notée multiplicativement, on adoptera le plus souvent la notation multiplicative à gauche $\alpha \cdot x$ pour la loi externe considérée, l'associativité s'exprimant par l'identité $(\alpha\beta)x = \alpha(\beta x)$; on notera ce composé $\alpha\beta x$; de même (en vertu de l'associativité de la multiplication dans Ω) on a $(\alpha\beta\gamma)x = \alpha(\beta\gamma x) = (\alpha\beta)(\gamma x) = \alpha(\beta(\gamma x))$, et la valeur commune de ces composés se note $\alpha\beta\gamma x$; on a des formules analogues pour le produit d'un nombre quelconque d'opérateurs.

Si une loi externe est associative par rapport à l'*opposée* d'une loi multiplicative sur son domaine d'opérateurs, on adoptera pour cette loi externe, soit la notation multiplicative à droite $x \cdot \alpha$, soit la notation exponentielle x^α , l'associativité s'exprimant respectivement par les identités $x(\beta\alpha) = (x\beta)\alpha$ et $x^{\beta\alpha} = (x^\beta)^\alpha$.

Exemples. — 1) Etant donnée une loi associative, notée multiplicativement, sur un ensemble E , la loi externe $(n, x) \rightarrow x^n$ est associative par rapport à la multiplication dans N^* , puisque $(x^m)^n = x^{mn}$ (la multiplication dans N^* étant commutative, il n'y a pas de distinction à faire entre elle et son opposée). De même pour $n \in N$ lorsqu'il y a un élément neutre dans E , et pour $n \in Z$ lorsque tous les éléments de E sont inversibles.

2) Etant donnée une loi associative τ sur un ensemble E , la loi externe $(a, X) \rightarrow a \tau X$ entre éléments de E (opérateurs) et parties X de E , est associative par rapport à la loi τ sur E ; la loi externe $(a, X) \rightarrow X \tau a$ est associative par rapport à l'*opposée* de la loi τ .

3) La loi externe $(f, x) \rightarrow f(x)$ entre applications f de E dans E (opérateurs) et éléments de E , est associative par rapport à la loi interne $f \circ g$; de même la loi $(A, X) \rightarrow A(X)$ entre parties A de $E \times E$ (opérateurs) et parties X de E est associative par rapport à la loi interne $A \circ B$.

4) La loi externe $(A, X) \rightarrow A \circ X$ entre opérateurs $A \subset F \times F$ et parties $X \subset E \times F$, est associative par rapport à la loi $A \circ B$ entre opérateurs; la loi externe $(B, Y) \rightarrow Y \circ B$ entre opérateurs $B \subset E \times E$ et parties $Y \subset E \times F$ est associative par rapport à la loi opposée à la loi $B \circ C$ entre opérateurs.

On vérifie immédiatement que l'associativité d'une loi externe par rapport à une loi interne sur le domaine d'opérateurs *se conserve en passant aux quotients et aux produits*.

3. Permutabilité.

DÉFINITION 5. — Soient τ une loi externe partout définie entre opérateurs $\alpha \in \Omega$ et éléments de E , \perp une loi externe partout définie entre opérateurs $\beta \in \Theta$ et éléments de E . On dit que ces deux lois sont permutable si on a l'identité

$$(7) \quad \alpha \tau (\beta \perp x) = \beta \perp (\alpha \tau x).$$

Autrement dit, si $(f_\alpha)_{\alpha \in \Omega}$ et $(g_\beta)_{\beta \in \Theta}$ sont les familles d'applications de E dans E produites par les opérateurs des lois τ et \perp respectivement, f_α doit être permutable avec g_β pour la loi $f \circ g$, quels que soient α et β . En général les lois externes dont il s'agira seront notées multiplicativement; si elles sont toutes deux notées multiplicativement à gauche, la permutabilité des deux lois s'exprime par l'identité $\alpha(\beta x) = \beta(\alpha x)$; si l'une est notée multiplicativement à gauche, l'autre à droite, la permutabilité s'exprime par l'identité $\alpha(x\beta) = (xx)\beta$, et la valeur commune des deux membres se note simplement $\alpha x \beta$; cette écriture justifie le nom de *double associativité* des deux lois externes, qu'on considère dans ce cas comme synonyme de « permutabilité ».

La permutabilité de deux lois externes *se conserve en passant aux quotients et aux produits*.

Exemples. — 1) Si τ est une loi associative sur un ensemble E , les lois externes $(a, X) \rightarrow a \tau X$ et $(b, X) \rightarrow X \tau b$ entre opérateurs de E et parties de E , sont permutable.

2) La loi externe $(A, X) \rightarrow A \circ X$ entre opérateurs $A \subset F \times F$

et parties $X \subset E \times F$, est permutable avec la loi externe $(B, X) \rightarrow X \circ B$ entre opérateurs $B \subset E \times E$ et parties $X \subset E \times F$.

Exercices. — 1) Soit \perp une loi interne partout définie sur E , doublement distributive par rapport à une loi interne associative τ ; montrer que, si $x \perp x'$ et $y \perp y'$ sont réguliers pour la loi τ , $x \perp y'$ est permutable avec $y \perp x'$ pour la loi τ (calculer le composé $(x \tau y) \perp (x' \tau y')$ de deux manières différentes). En particulier, si la loi \perp possède un élément neutre, deux éléments réguliers pour la loi τ sont permutables pour cette loi; si tous les éléments de E sont réguliers pour la loi τ , cette loi est commutative.

2) Soient τ et \perp deux lois internes partout définies sur un ensemble E , telles que la loi externe à gauche déduite de \perp soit distributive par rapport à τ .

a) Si la loi τ possède un élément neutre e , $x \perp e$ est idempotent pour la loi τ , quel que soit $x \in E$; si en outre il existe y tel que $x \perp y$ soit régulier pour la loi τ , on a $x \perp e = e$.

b) Si la loi \perp possède un élément neutre u , et s'il existe $z \in E$ régulier à la fois pour les deux lois \perp et τ , u est régulier pour la loi τ .

¶ 3) Soient τ et \perp deux lois internes partout définies sur E , ayant chacune un élément neutre; si la loi externe à gauche déduite de chacune de ces lois est distributive par rapport à l'autre, tout élément de E est idempotent pour ces deux lois (si e est élément neutre pour τ , u élément neutre pour \perp , prouver d'abord que $e \perp e = e$, en remarquant que $e = e \perp (u \tau e)$).

4) Sur un ensemble E , on suppose données trois lois de composition internes partout définies : une addition (non nécessairement associative ni commutative), une multiplication (non nécessairement associative) et une loi notée τ . On suppose que la multiplication possède un élément neutre e , que la loi externe à gauche déduite de τ est distributive par rapport à la multiplication, et la loi externe à droite déduite de τ distributive par rapport à l'addition. Montrer que, s'il existe x, y, z tels que $x \tau z, y \tau z$ et $(x + y) \tau z$ soient réguliers pour la multiplication, on a $e + e = e$ (utiliser l'exercice 2a)).

¶ 5) On dit qu'une loi de composition interne partout définie τ sur E détermine sur E une structure de *quasi-groupe*, si pour tout $x \in E$, les translations à gauche et à droite γ_x et δ_x sont des applications biunivoques de E sur lui-même. Un quasi-groupe est dit *distributif* si la loi τ est doublement distributive par rapport à elle-même.

a) Déterminer toutes les structures de quasi-groupe distributif sur un ensemble de n éléments, pour $2 \leq n \leq 6$.

b)* Montrer que l'ensemble \mathbb{Q} des nombres rationnels, muni

de la loi de composition $(x, y) \rightarrow \frac{1}{2}(x + y)$, est un quasi-groupe distributif.*

c) Dans un quasi-groupe distributif E , tout élément est idempotent. En déduire que, si E a plus d'un élément, la loi τ ne peut posséder d'élément neutre ni être associative.

d) Les translations à gauche et à droite dans E sont des automorphismes de E .

e) Si E est fini, la structure induite sur toute partie stable de E est une structure de quasi-groupe distributif.

f) Si R est une relation d'équivalence compatible à gauche (resp. à droite) avec la loi τ , les classes mod. R sont des parties stables de E . Si E est fini, toutes ces classes se déduisent de l'une d'elles par translation à gauche (resp. à droite); dans les mêmes conditions, si R est compatible avec la loi τ , la structure quotient sur E/R est une structure de quasi-groupe distributif.

g) L'ensemble A_a des éléments de E permutables avec un élément donné a est stable; si E est fini, pour tout $x \in A_a$, on a $A_x = A_a$ (remarquer, en utilisant e), qu'il existe $y \in A_a$ tel que $x = a \tau y$, et lorsque x parcourt E , les ensembles A_x sont identiques aux classes d'équivalence suivant une relation compatible avec la loi τ .

h) Si E est fini, et la loi τ commutative, le nombre d'éléments de E est impair (considérer les couples (x, y) d'éléments de E tels que $x \tau y = y \tau x = a$, où a est donné).

6) On suppose données, sur un ensemble E , une addition (associative et commutative) pour laquelle tous les éléments de E sont symétrisables* (autrement dit, une loi de groupe abélien additif)*, et une multiplication (associative), doublement distributive par rapport à l'addition; on pose $x \circ y = xy - yx$; la loi $x \circ y$ est doublement distributive par rapport à l'addition. Pour que x et y soient permutables pour la multiplication, il faut et il suffit que $x \circ y = 0$; et on a les identités

$$x \circ y = -y \circ x; \quad x \circ (y \circ z) + y \circ (z \circ x) + z \circ (x \circ y) = 0$$

(la seconde est connue sous le nom d'*« identité de Jacobi »*). La seconde identité s'écrit aussi

$$x \circ (y \circ z) - (x \circ y) \circ z = (z \circ x) \circ y$$

ce qui exprime la « déviation de l'associativité » de la loi $x \circ y$.

7) Les hypothèses étant les mêmes que dans l'exerc. 6, on pose $x \tau y = xy + yx$; la loi τ est alors commutative, doublement distributive par rapport à l'addition, mais non associative en général.

a) Quel que soit $x \in E$, montrer que $\tau^m x = (\tau^m x) \tau^n (\tau^m x)$.

b) Si on pose $[x, y, z] = (x \tau y) \tau z - x \tau (y \tau z)$ (déviation de l'associativité de la loi τ), prouver les identités

$$[x, y, z] + [z, y, x] = 0$$

$$[x, y, z] + [y, z, x] + [z, x, y] = 0$$

$$[x \tau y, u, z] = u \circ ((x \tau y) \circ z)$$

(la notation $x \circ y$ ayant le même sens que dans l'exerc. 6)

$$[x \tau y, u, z] + [y \tau z, u, x] + [z \tau x, u, y] = 0.$$

¶ 8) On suppose données sur E une addition (associative et commutative) pour laquelle tous les éléments de E sont symétrisables, et une multiplication, *non associative*, mais commutative et doublement distributive par rapport à l'addition. Montrer que si, en posant $[x, y, z] = (xy)z - x(yz)$, on a l'identité

$$[xy, u, z] + [yz, u, x] + [zx, u, y] = 0,$$

on a $x^{m+n} = x^m x^n$ quel que soit x (montrer, par récurrence sur p , qu'on a l'identité $[x^q, y, x^{p-q}] = 0$ pour $1 \leq q < p$).^(*)

§ 6. — Groupes et groupes à opérateurs.

1. Groupes.

DÉFINITION 1. — Sur un ensemble G , on dit qu'une loi de composition interne partout définie détermine une structure de groupe si : 1° elle est associative ; 2° elle possède un élément neutre ; 3° tout élément de G admet un symétrique pour cette loi. Un ensemble muni d'une structure de groupe prend le nom de groupe.

D'après les prop. 3 et 4 du § 2, il revient au même de dire qu'un groupe G est un monoïde (§ 1, n° 3) tel que, pour tout $x \in G$, les translations à gauche et à droite γ_x, δ_x , soient des applications de G sur G : ce sont alors des applications biunivoques de G sur G (cf. exerc. 2).

Exemples. — 1) Dans un monoïde quelconque E ayant un élément neutre, l'ensemble des éléments symétrisables, muni de la structure induite par celle de E , est un groupe. En particulier, l'ensemble des applications biunivoques d'un ensemble F sur lui-même (ou ensemble des permutations de F) est un groupe pour la

(*) Pour une étude plus approfondie des structures de cette espèce, voir P. JORDAN, J. v. NEUMANN and E. WIGNER, *Ann. of Math.*, t. XXXV, (1934), p. 29.

loi $f \circ g$, qu'on appelle *groupe symétrique* de l'ensemble F ; nous reviendrons plus en détail sur ce groupe au § 7.

2) Si E est un ensemble muni d'une loi associative et commutative τ , \bar{E} le symétrisé (§ 2, n° 4) de E pour la loi τ , l'ensemble des éléments réguliers de \bar{E} forme un groupe pour la loi induite par celle de \bar{E} . En particulier, l'ensemble Z , muni de l'addition, est un groupe, qui s'appelle le *groupe additif des entiers rationnels* ; de même, l'ensemble Q^* des nombres rationnels > 0 , muni de la multiplication, est un groupe.

Un groupe G est dit *fini* si l'ensemble de ses éléments est fini, sinon il est dit *infini* ; le nombre des éléments d'un groupe fini est appelé *l'ordre* du groupe.

Si une loi de composition sur G détermine sur G une structure de groupe, il en est de même de la loi opposée : les deux groupes ainsi définis sont dits *opposés*. L'application d'un groupe G sur lui-même qui, à tout $x \in G$, fait correspondre le *symétrique* de x , est un *isomorphisme* de G sur le groupe opposé (§ 2, prop. 5), qu'on appelle la *symétrie* ou l'*application symétrique* de G sur lui-même ; c'est une permutation involutive de G .

Dans ce paragraphe, sauf indication contraire, nous noterons toujours *multiplicativement* la loi de composition d'un groupe, et nous désignerons par e l'élément neutre d'une loi de groupe ainsi notée (rappelons que, dans ce cas, e s'appelle souvent *l'élément unité* du groupe) ; la symétrie d'un groupe G sur lui-même s'écrit alors $x \rightarrow x^{-1}$.

Suivant nos conventions générales (*Ens. R*, § 2, n° 4), nous désignerons par A^{-1} l'image d'une partie A de G par la symétrie $x \rightarrow x^{-1}$. Mais il importe de noter que, malgré l'analogie des notations, A^{-1} n'est pas du tout élément inverse de A pour la loi de composition $(X, Y) \rightarrow XY$ entre parties de G (rappelons que XY est l'ensemble des xy pour $x \in X, y \in Y$) : en effet, l'élément neutre pour cette loi est $\{e\}$, et les seuls éléments de $\mathfrak{P}(G)$, inversibles pour cette loi, sont les ensembles $A = \{a\}$ réduits à un seul élément (un tel A , d'ailleurs, a bien pour inverse A^{-1}). On a l'identité $(AB)^{-1} = B^{-1}A^{-1}$ pour $A \subset G, B \subset G$. On dit que A est une partie *symétrique* de G si $A = A^{-1}$. Quel que soit $A \subset G$, $A \cup A^{-1}, A \cap A^{-1}$ et AA^{-1} sont symétriques.

2. Sous-groupes.

DÉFINITION 2. — On appelle sous-groupe d'un groupe G , une partie non vide H de G , telle que la structure induite sur H par celle de G soit une structure de groupe.

PROPOSITION 1. — Soit H une partie non vide d'un groupe G ; les propositions suivantes sont équivalentes :

a) H est un sous-groupe de G .

b) H est une partie stable de G (autrement dit, les relations $x \in H$, $y \in H$ entraînent $xy \in H$), et la relation $x \in H$ entraîne $x^{-1} \in H$.

c) Les relations $x \in H$, $y \in H$, entraînent $xy^{-1} \in H$.

Montrons d'abord que a) entraîne b). Comme la loi de composition induite sur H par celle de G doit être partout définie, H doit être une partie stable de G . En second lieu, cette loi induite doit posséder un élément neutre u , qui satisfait à $u \cdot u = u$; on en conclut que $u = u \cdot u^{-1} = e$, donc H contient e ; si $x \in H$ est inversible dans H , son inverse dans H est par suite identique à son inverse x^{-1} dans G , ce qui achève de démontrer b).

Réciproquement, b) entraîne a); en effet, pour tout $x \in H$, on a $x^{-1} \in H$, puis $x \cdot x^{-1} = e \in H$; la loi de composition induite sur H par celle de G est bien une loi de groupe.

Enfin, il est clair que b) entraîne c); réciproquement, si c) est vérifiée, la relation $x \in H$ entraîne $x \cdot x^{-1} = e \in H$, puis $e \cdot x^{-1} = x^{-1} \in H$; donc, les relations $x \in H$, $y \in H$ entraînent $x(y^{-1})^{-1} = xy \in H$, ce qui prouve que c) entraîne b).

Remarques. — 1) On prouve de même que la proposition b) de l'énoncé est équivalente à la proposition :

c') Les relations $x \in H$, $y \in H$ entraînent $y^{-1}x \in H$.

2) La proposition b) peut encore s'écrire : $H \cdot H \subset H$ et $H^{-1} \subset H$. Pour une partie non vide H de G , ces relations entraînent donc que H est un sous-groupe; par suite $e \in H$, d'où $X \subset H \cdot X$ pour toute partie X de G , et en particulier $H \subset H \cdot H$; d'autre part, la symétrie de G transforme l'inclusion $H^{-1} \subset H$ en $H \subset H^{-1}$. Donc, pour tout sous-groupe H de G , on a les relations

$$(1) \quad H \cdot H = H, \quad H^{-1} = H.$$

La proposition c) s'écrit de même : $H \cdot H^{-1} \subset H$; pour une partie non vide H de G , cette relation équivaut donc aux relations (1); il en est de même de la relation $H^{-1} \cdot H \subset H$.

Si H est un sous-groupe de G , et K un sous-groupe de H , il est clair que K est un sous-groupe de G .

L'ensemble $\{e\}$ est un sous-groupe de G ; c'est évidemment le plus petit (il est contenu dans tous les sous-groupes de G). L'intersection H d'une famille de sous-groupes (H_i) est un sous-groupe, car elle est non vide (on a $e \in H_i$ quel que soit i), et les relations $x \in H$, $y \in H$ entraînent $xy^{-1} \in H_i$ pour tout i , donc $xy^{-1} \in H$.

Il y a donc un plus petit sous-groupe de G contenant une partie donnée X de G ; on l'appelle le *sous-groupe engendré par X* , et X est appelé un *système de générateurs* de ce sous-groupe.

Exemple. — Cherchons les sous-groupes du groupe additif \mathbb{Z} des entiers rationnels. Si H est un tel sous-groupe, et n'est pas réduit au seul élément 0, soit $x \in H$ tel que $x \neq 0$: ou bien $x > 0$, ou bien $x < 0$, et alors $x' = -x > 0$ et $x' \in H$, donc l'ensemble des éléments > 0 de H n'est pas vide : soit a le plus petit. Par récurrence sur $m \in \mathbb{N}^*$, on voit que $ma \in H$; donc aussi $-ma \in H$ pour $m \in \mathbb{N}^*$, et comme $0 \in H$, il suit que $na \in H$ quel que soit $n \in \mathbb{Z}$. Si $x \in H$, on a (§ 4, n° 3) $x = qa + r$, avec $q \in \mathbb{Z}$, $0 \leq r < a$; on a $qa \in H$, donc $r = x - qa \in H$; mais, d'après la définition de a , $0 < r < a$ entraîne $r \notin H$, donc $r = 0$, $x = qa$: H est donc l'ensemble des na pour $n \in \mathbb{Z}$, autrement dit $H = a\mathbb{Z}$. Réciproquement, $a\mathbb{Z}$ est évidemment un sous-groupe de \mathbb{Z} pour $a \in \mathbb{N}^*$; si $a = 0$, $a\mathbb{Z} = \{0\}$; si $a < 0$ et $a' = -a$, on a $a' > 0$ et $a\mathbb{Z} = a'\mathbb{Z}$; il résulte d'ailleurs de la démonstration ci-dessus que $a\mathbb{Z}$ est le sous-groupe engendré par $\{a\}$, et que la partie stable de \mathbb{Z} engendrée par $\{a\}$ est l'ensemble $a\mathbb{N}^*$ des ma pour $m \in \mathbb{N}^*$.

Comme le montre cet exemple, il faut se garder de confondre la partie stable d'un groupe G engendrée par une partie X de G avec le sous-groupe engendré par X : celui-ci contient toujours celle-là, mais en est distinct en général. La formation du sous-groupe engendré par X est précisée par la proposition suivante :

PROPOSITION 2. — Si X est une partie non vide d'un groupe G , le sous-groupe engendré par X est la partie stable Y^∞ engendrée par l'ensemble $Y = X \cup X^{-1}$.

En effet, Y^∞ est l'ensemble des composés des suites dont tous les termes sont des éléments de X ou des inverses d'éléments de X : l'inverse d'un tel composé est un composé de même forme (§ 2, prop. 5), donc (prop. 1) Y^∞ est un sous-groupe de G ; réciproquement, tout sous-groupe contenant X contient évidemment Y , donc Y^∞ .

3. Groupes quotients.

Cherchons quelles sont les relations d'équivalence compatibles avec la loi de composition d'un groupe. D'après la prop. 1 du § 4, il y a lieu d'examiner séparément la compatibilité à gauche et la compatibilité à droite ; la question est résolue par le théorème suivant :

THÉORÈME 1. — Soit R une relation d'équivalence dans un groupe G ; si R est compatible à gauche (resp. à droite) avec la loi du groupe, elle est équivalente à une relation de la forme $x^{-1}y \in H$ (resp. $yx^{-1} \in H$), où H est un sous-groupe de G . Réciproquement, si H est un sous-groupe quelconque de G , la relation $x^{-1}y \in H$ (resp. $yx^{-1} \in H$) est une relation d'équivalence compatible à gauche (resp. à droite) avec la loi du groupe G .

Bornons-nous à considérer le cas d'une relation R compatible à gauche avec la loi de G (le cas d'une relation compatible à droite s'en déduit par passage de G au groupe opposé). La relation $y \equiv x$ (mod. R) équivaut à $x^{-1}y \equiv e$ (mod. R), car $y \equiv x$ entraîne $y^{-1} \equiv x^{-1}$, et réciproquement $x^{-1}y \equiv e$ entraîne $x(x^{-1}y) \equiv x$. Si H désigne la classe formée des $x \equiv e$, la relation R est donc équivalente à $x^{-1}y \in H$. Montrons que H est un sous-groupe de G : il faut établir (prop. 1) que $x \in H$ et $y \in H$ entraînent $x^{-1}y \in H$, c'est-à-dire que $x \equiv e$ et $y \equiv e$ entraînent $x \equiv y$, ce qui est une conséquence de la transitivité de R .

Réciproquement, soit H un sous-groupe de G ; la relation $x^{-1}y \in H$ est réflexive, puisque $x^{-1}x = e \in H$; elle est symétrique, puisque $x^{-1}y \in H$ entraîne $y^{-1}x = (x^{-1}y)^{-1} \in H$; elle est transitive, car $x^{-1}y \in H$ et $y^{-1}z \in H$ entraînent $x^{-1}z = (x^{-1}y)(y^{-1}z) \in H$; enfin, elle est compatible à gauche avec la loi de composition de G , car on peut écrire $x^{-1}y = (zx)^{-1}(zy)$ pour tout $z \in G$.

La relation $x^{-1}y \in H$ (resp. $yx^{-1} \in H$) s'écrit aussi sous la forme équivalente $y \in xH$ (resp. $y \in Hx$). Tout sous-groupe H de G définit ainsi deux relations d'équivalence dans G , à savoir $y \in xH$ et $y \in Hx$: les classes d'équivalence pour ces relations sont respectivement les ensembles xH , qu'on appelle *classes à gauche suivant*

H (ou *modulo* H), et les ensembles Hx , qu'on appelle *classes à droite suivant* H (ou *modulo* H). En saturant une partie $A \subset G$ pour ces relations (*Ens. R*, § 5, n° 6), on obtient respectivement les ensembles AH et HA . Par passage au groupe opposé, tout sous-groupe H reste sous-groupe, les classes à gauche deviennent classes à droite et vice-versa ; par la symétrie de G , tout sous-groupe H est appliqué sur lui-même, les classes à gauche sont transformées en classes à droite et réciproquement.

Lorsque le nombre des classes à gauche distinctes (mod. H) est fini, on l'appelle l'*indice* du sous-groupe H par rapport à G , et on le désigne par la notation $(G : H)$; il est aussi égal au nombre des classes à droite. S'il existe une infinité de classes à gauche distinctes, on dit que H est un sous-groupe de G d'*indice infini*.

Si un sous-groupe K de G contient H , il est réunion de classes à gauche (ou à droite) suivant H ; si K est réunion d'un nombre fini de classes à gauche distinctes suivant H (c'est-à-dire si l'*indice* $(K : H)$ est fini), toute classe à gauche suivant K est réunion du même nombre de classes à gauche distinctes suivant H , puisqu'une classe à gauche suivant K se déduit de K par une translation à gauche. En particulier :

PROPOSITION 3. — Soient H et K deux sous-groupes d'un groupe G , tels que $H \subset K$. Si l'*indice* $(G : H)$ est fini, il en est de même de $(G : K)$ et $(K : H)$, et on a

$$(2) \quad (G : H) = (G : K)(K : H).$$

Réciproquement, si $(G : K)$ et $(K : H)$ sont finis, $(G : H)$ est fini et on a la formule (2).

COROLLAIRE. — Si G est un groupe fini d'ordre g , H un sous-groupe de G d'ordre h , on a

$$(3) \quad (G : H) = \frac{g}{h}$$

(en particulier, l'ordre et l'*indice* de H sont des *diviseurs* de l'ordre de G).

Le th. 1 permet de déterminer les relations d'équivalence compatibles avec la loi d'un groupe G : si R est une telle relation, elle est à la fois compatible à droite et à gauche avec la loi du

groupe, donc, si H est la classe de e (mod. R), H est un sous-groupe tel que les relations $y \in xH$ et $y \in Hx$ soient équivalentes (puisque toutes deux sont équivalentes à R) ; on a donc $xH = Hx$ quel que soit $x \in G$. Réciproquement, s'il en est ainsi, l'une ou l'autre des relations équivalentes $y \in xH$, $y \in Hx$, est compatible avec la loi du groupe, puisqu'elle est à la fois compatible à gauche et à droite avec cette loi (§ 4, prop. 1). L'égalité $xH = Hx$ étant équivalente à $xHx^{-1} = H$, on pose la définition suivante :

DÉFINITION 3. — *Un sous-groupe H de G s'appelle sous-groupe distingué (ou invariant) de G si on a $xHx^{-1} = H$ pour tout $x \in G$.*

Pour vérifier qu'un sous-groupe H est distingué, il suffit de montrer que $xHx^{-1} \subset H$ pour tout $x \in G$; en effet, s'il en est ainsi on a aussi $x^{-1}Hx \subset H$ pour tout $x \in G$, c'est-à-dire $H \subset xHx^{-1}$, et, par suite $H = xHx^{-1}$.

Soit H un sous-groupe distingué de G , R la relation d'équivalence $y \in xH$ définie par H ; sur l'ensemble quotient G/R , la loi quotient par R de la loi du groupe G est associative ; la classe de e est l'élément neutre pour cette loi quotient, et les classes de deux éléments inverses dans G sont inverses pour la loi quotient (§ 4, n° 3). Donc, en résumant les résultats obtenus :

THÉORÈME 2. — *Les relations d'équivalence compatibles avec la loi d'un groupe G sont les relations de la forme $y \in xH$, où H est un sous-groupe distingué de G (la relation $y \in xH$ étant d'ailleurs équivalente à $y \in Hx$ pour un tel sous-groupe H) ; la structure quotient de celle de G par une telle relation est une structure de groupe.*

DÉFINITION 4. — *Le quotient d'un groupe G par la relation d'équivalence définie par un sous-groupe distingué H de G s'appelle le groupe quotient de G par H et se note G/H .*

On note parfois $x \equiv y$ (mod. H) ou $x \equiv y$ (H) la relation d'équivalence définie par un sous-groupe distingué H de G ; la loi quotient de la loi de G par cette relation est souvent appelée, de façon abrégée, la loi quotient de celle de G par le sous-groupe distingué H .

Remarques. — 1) Si A est une partie quelconque de G , et H un sous-groupe distingué de G , on a $AH = HA$; cet ensemble est obtenu en saturant A pour la relation $x \equiv y$ (mod. H).

2) Si xH et yH sont deux éléments quelconques du groupe quotient G/H , le composé de xH et yH est xyH ; il est égal au composé $(xH)(yH)$ dans $\mathfrak{P}(G)$, car on a $HyH = y(y^{-1}Hy)H = y(H.H) = yH$. De même, l'inverse de xH dans G/H est $x^{-1}H$; il est égal à $(xH)^{-1}$, puisque cet ensemble n'est autre que

$$H^{-1}x^{-1} = Hx^{-1}.$$

3) Si H est un sous-groupe distingué d'indice fini, le groupe quotient G/H est un groupe fini d'ordre $(G : H)$.

Exemple. — Si la loi de composition d'un groupe G est commutative, on a $xyx^{-1} = y$ quels que soient x, y , donc tout sous-groupe de G est distingué ; c'est le cas par exemple pour le groupe additif \mathbb{Z} des entiers rationnels. Les sous-groupes de \mathbb{Z} ont été déterminés (n° 2) : ce sont les ensembles $a.\mathbb{Z}$, pour $a \in \mathbb{Z}$; la relation d'équivalence définie par le sous-groupe $a.\mathbb{Z}$ n'est autre que $x - y \in a.\mathbb{Z}$, c'est-à-dire $x \equiv y$ (mod. a) (§ 4, n° 3) : les congruences sont les seules relations d'équivalence compatibles avec l'addition sur \mathbb{Z} . Pour $a > 0$, le quotient du groupe additif \mathbb{Z} par la congruence modulo a s'appelle le *groupe additif des entiers rationnels modulo a* ; c'est un groupe fini d'ordre a .

Dans un groupe G , les sous-groupes G et $\{e\}$ sont distingués (les quotients G/G et $G/\{e\}$ étant isomorphes respectivement à $\{e\}$ et à G) ; si ce sont les seuls, G est dit *simple*. L'intersection de toute famille de sous-groupes distingués de G est un sous-groupe distingué de G : on peut donc parler du plus petit sous-groupe distingué de G contenant une partie X de G .

On notera que, si H est sous-groupe distingué de G , et K sous-groupe distingué de H , K n'est pas toujours sous-groupe distingué de G (on en verra des exemples).

4. Représentations.

La définition générale d'une représentation (§ 4, n° 4, déf. 7) donne en particulier, pour les groupes, la définition suivante :

DÉFINITION 5. — *Soit G un groupe, G' un ensemble muni d'une loi de composition interne. Une application f de G dans G' s'appelle une représentation (ou un homomorphisme) de G dans G' si (les*

lois de G et G' étant notées multiplicativement), quels que soient $x \in G$, $y \in G$, $f(x)f(y)$ est défini et on a

$$(4) \quad f(xy) = f(x)f(y).$$

Si H est un sous-groupe distingué de G , l'application canonique de G sur le groupe quotient G/H est un homomorphisme, dit *homomorphisme canonique* de G sur G/H .

Si f est un homomorphisme de G dans G' , la relation $f(x) = f(y)$ est équivalente à $f(x^{-1}y) = f(e)$: le th. général d'homomorphie (§ 4, th. 1) donne donc, en utilisant le th. 2 ci-dessus, le théorème suivant :

THÉORÈME 3. — Soit f une représentation d'un groupe G dans un ensemble G' muni d'une loi de composition interne. L'image $f(G)$ est un groupe (pour la loi induite par celle de G'), ayant pour élément neutre $e' = f(e)$. L'image réciproque $H = f^{-1}(e')$ de l'élément neutre de $f(G)$ est un sous-groupe distingué de G ; le groupe $f(G)$ est isomorphe au groupe quotient G/H , et la représentation f est composée d'un isomorphisme de G/H dans G' et de l'homomorphisme canonique de G sur G/H .

En d'autres termes, la décomposition canonique de f (Ens. R, § 5, n° 3) donne : 1° l'isomorphisme canonique de $f(G)$ dans G' ; 2° un isomorphisme de G/H sur $f(G)$, dit *représentation biunivoque associée à f*; 3° l'homomorphisme canonique de G sur G/H (cf. § 4, n° 4).

Suivant encore le § 4, on appelle *endomorphisme* d'un groupe G une représentation de G dans G ; comme toujours, un *automorphisme* de G est un isomorphisme de G sur lui-même. Le composé de deux endomorphismes de G pour la loi $f \circ g$ est encore un endomorphisme de G ; le composé pour la même loi de deux automorphismes de G est un automorphisme de G , ainsi que l'application réciproque d'un automorphisme de G .

Autrement dit, les automorphismes d'un groupe G forment un groupe pour la loi $f \circ g$ (cf. § 7).

PROPOSITION 4. — Pour tout élément x d'un groupe G , l'application α_x de G dans G , définie par $\alpha_x(y) = xyx^{-1}$, est un automorphisme de G .

En effet, α_x est un endomorphisme de G , car

$$x \cdot yz \cdot x^{-1} = (xyx^{-1})(zxz^{-1}).$$

D'autre part, la relation $xyx^{-1} = u$ équivaut à $y = x^{-1}ux$, donc pour tout $u \in G$ il existe un y et un seul tel que $\alpha_x(y) = u$, autrement dit α_x est une application biunivoque de G sur lui-même, donc un automorphisme de G .

Les automorphismes α_x s'appellent les *automorphismes intérieurs du groupe G*.

Le groupe G étant noté multiplicativement, on pose parfois

$$y^x = \alpha_{x^{-1}}(y) = x^{-1}yx$$

cette notation étant justifiée (d'après les conventions du § 5) par le fait que y^x , considérée comme loi de composition *externe* entre opérateurs $x \in G$ et éléments $y \in G$, est distributive par rapport à la loi du groupe entre éléments y , et associative par rapport à la loi opposée entre opérateurs x , propriétés qui s'expriment par les identités

$$(xy)^u = x^u y^u, \quad x^{uv} = (x^u)^v.$$

On n'utilisera toutefois cette notation exponentielle que lorsqu'elle ne risquera pas d'entrainer des confusions, et en rappelant chaque fois sa signification.

Un automorphisme de G , et en particulier un automorphisme intérieur, transforme évidemment tout sous-groupe de G en un sous-groupe isomorphe; la déf. 3 signifie qu'un sous-groupe est distingué s'il est transformé en lui-même par tous les automorphismes intérieurs de G .

5. Produits de groupes.

Les remarques du § 4, n° 5, prouvent qu'un produit de structures de groupes est une structure de groupe, ce qui permet de poser la définition suivante :

DÉFINITION 6. — On appelle *groupe produit* d'une famille de groupes $(G_i)_{i \in I}$, l'ensemble produit $G = \prod_{i \in I} G_i$, muni de la structure de groupe déterminée sur lui par la loi qui, à $x = (x_i)$ et $y = (y_i)$, fait correspondre $xy = (x_i y_i)$.

Si H_i est un sous-groupe (resp. sous-groupe distingué) de G_i , $\prod_{i \in I} H_i$, muni de la structure induite par G , est un sous-groupe (resp. sous-groupe distingué) de G , isomorphe au produit des groupes H_i . En particulier, soit J une partie de I , et $K = \complement J$; le groupe produit $G_J = \prod_{i \in J} G_i$ est isomorphe au sous-groupe distingué $G'_J = \left(\prod_{i \in J} G_i \right) \times \left(\prod_{i \in K} \{e_i\} \right)$ de G , avec lequel on l'identifie souvent. La projection pr_J de G sur G_J est un homomorphisme de G sur G_J ; l'image réciproque de l'élément neutre de G_J par cet homomorphisme n'est autre que G'_K , donc G_J est isomorphe à G/G'_K , et G est isomorphe au produit $G'_J \times (G/G'_K)$. Si J_1 et J_2 sont deux parties de I sans élément commun, il résulte de la déf. 6 que tout élément de G'_{J_1} est permutable avec tout élément de G'_{J_2} .

La prop. 4 du § 4 donne ici la suivante :

PROPOSITION 5. — Soient G_1, G_2 deux groupes, H_1 un sous-groupe distingué de G_1 , H_2 un sous-groupe distingué de G_2 . L'application canonique du groupe produit $(G_1/H_1) \times (G_2/H_2)$ sur le groupe quotient $(G_1 \times G_2)/(H_1 \times H_2)$ est un isomorphisme.

Un cas particulier important de produit de groupes est le groupe formé par les applications d'un ensemble E dans un groupe G , le composé de deux applications f et g étant l'application $h = fg$ telle que $h(x) = f(x)g(x)$ pour tout $x \in E$; ce groupe n'est autre que le groupe produit G^E .

6. Produit direct de sous-groupes.

Soit $G = \prod_{1 \leq i \leq n} G_i$ un produit d'une famille finie de groupes G_i ; d'après ce qui précède, G_i est isomorphe au sous-groupe distingué $G'_i = G_i \times \prod_{j \neq i} \{e_j\}$ de G , et, pour $i \neq j$, tout élément de G'_i est permutable avec tout élément de G'_j . Si $x = (x_i) \in G$, et si $u_i = (u_{ij})$ est l'élément de G'_i tel que $u_{ii} = x_i, u_{ij} = e_j$ pour $j \neq i$,

on a $x = u_1 u_2 \cdots u_n$; réciproquement, si $x = v_1 v_2 \cdots v_n, v_i \in G'_i$ ($1 \leq i \leq n$), et si $pr_i(v_i) = y_i$, on a $x = (y_i)$, donc $y_i = x_i$, et $v_i = u_i$: les u_i sont donc déterminés d'une manière unique par x ; d'ailleurs x est aussi le composé de toute suite qui se déduit de la suite $(u_i)_{1 \leq i \leq n}$ par une permutation quelconque (§ 1, th. 3).

Posons la définition suivante :

DÉFINITION 7. — On dit qu'un groupe G , noté multiplicativement, est produit direct d'une famille finie $(H_i)_{1 \leq i \leq n}$ de sous-groupes distincts de G , si tout élément de H_i est permutable avec tout élément de H_j pour $j \neq i$, et si tout $x \in G$ peut se mettre d'une manière et d'une seule sous la forme $x = u_1 u_2 \cdots u_n$, avec $u_i \in H_i$ ($1 \leq i \leq n$). L'élément u_i est appelé le composant de x dans H_i .

On peut donc dire que tout produit $G = \prod_{1 \leq i \leq n} G_i$ d'un nombre fini de groupes, est produit direct des sous-groupes G'_i isomorphes aux G_i .

Inversement, supposons qu'un groupe G soit produit direct d'une famille $(H_i)_{1 \leq i \leq n}$ de ses sous-groupes. Pour tout $x \in G$, la relation $x = u_1 u_2 \cdots u_n, u_i \in H_i$ ($1 \leq i \leq n$) détermine uniquement l'élément u_i par hypothèse; posons $u_i = f_i(x)$. Montrons que f_i est un homomorphisme de G sur H_i ; en effet, $f_i(H_i) = H_i$, donc f_i applique G sur H_i ; d'autre part, si $y \in G, v_i = f_i(y), y = v_1 v_2 \cdots v_n$, la condition de permutabilité des H_i entraîne $xy = (u_1 v_1)(u_2 v_2) \cdots (u_n v_n)$: il suffit de démontrer, par récurrence sur p , que

$$(u_1 u_2 \cdots u_p)(v_1 v_2 \cdots v_p) = (u_1 v_1)(u_2 v_2) \cdots (u_p v_p),$$

ce qui est immédiat en remarquant qu'on a $u_p v_1 v_2 \cdots v_{p-1} = v_1 v_2 \cdots v_{p-1} u_p$ d'après la prop. 2 du § 1. On conclut de là que l'application

$$x \rightarrow (f_i(x))$$

est un isomorphisme de G sur le groupe produit $\prod_{1 \leq i \leq n} H_i$,

qui applique H_i sur le sous-groupe distingué H'_i de ce produit formé

des $u = (u_j)$ tels que $u_j = e$ pour $j \neq i$. En résumé :

PROPOSITION 6. — Si un groupe G est produit direct d'une famille finie $(H_i)_{1 \leq i \leq n}$ de sous-groupes de G , les H_i sont des sous-groupes distingués de G , et l'application qui, à tout élément $u = (u_i)$ du groupe produit $\prod_{1 \leq i \leq n} H_i$, fait correspondre le composé $u_1 u_2 \cdots u_n$

de la suite (u_i) , est un isomorphisme (dit canonique) de $\prod_{1 \leq i \leq n} H_i$ sur G .

En raison de cet isomorphisme, il arrivera souvent qu'on ne fera pas de différence entre les notions de *produit* et de *produit direct* d'une famille finie de sous-groupes d'un groupe donné.

Si G est produit direct des sous-groupes H_i ($1 \leq i \leq n$), il est clair, d'après l'isomorphie précédente, qu'on a

$$(H_1 H_2 \cdots H_{i-1} H_{i+1} \cdots H_n) \cap H_i = \{e\} \text{ pour } 1 \leq i \leq n.$$

Réiproquement :

PROPOSITION 7. — Si une famille finie $(H_i)_{1 \leq i \leq n}$ de sous-groupes distingués d'un groupe G est telle que

$$(H_1 H_2 \cdots H_i) \cap H_{i+1} = \{e\} \text{ pour } 1 \leq i \leq n-1,$$

l'ensemble $H_1 H_2 \cdots H_n$ est un sous-groupe distingué de G , produit direct des sous-groupes H_i .

Par récurrence sur n , on se ramène aussitôt à démontrer la proposition pour $n = 2$. Montrons d'abord que, si $x \in H_1$, $y \in H_2$, x et y sont permutable ; en effet, on a $xyx^{-1}y^{-1} = (xyx^{-1})y^{-1} = x(yx^{-1}y^{-1})$ donc (H_1 et H_2 étant distingués), $xyx^{-1}y^{-1} \in H_1 \cap H_2$, c'est-à-dire $xyx^{-1}y^{-1} = e$, d'après l'hypothèse. Il en résulte (par la prop. 1) que $H_1 H_2$ est un sous-groupe de G , et on vérifie immédiatement que ce sous-groupe est distingué. Supposons enfin qu'on ait $xy = x'y'$, avec $x \in H_1$, $x' \in H_1$, $y \in H_2$, $y' \in H_2$; on en tire $x'^{-1}x = y'y^{-1}$, donc $x'^{-1}x \in H_1 \cap H_2 = \{e\}$, $x' = x$, et de même $y' = y$; $H_1 H_2$ est bien produit direct de H_1 et H_2 .

Pour les groupes notés additivement, on emploiera le terme de *somme directe* au lieu de « *produit direct* ».

7. Groupes abéliens ; groupes monogènes.

DÉFINITION 8. — On dit qu'un groupe est abélien (ou commutatif) si sa loi de composition est commutative.

Un groupe abélien sera souvent noté *additivement*, son élément neutre s'écrivant alors 0 (zéro).

Dans un groupe abélien, tout automorphisme intérieur se réduit à l'automorphisme identique : tout sous-groupe est donc distingué. Tout groupe quotient d'un groupe abélien est abélien ; tout produit de groupes abéliens est abélien.

Dans un groupe quelconque G , soit A une partie de G dont les éléments sont deux à deux permutable ; d'après la prop. 2 ci-dessus, et la prop. 7 du § 2, le sous-groupe de G engendré par A est abélien.

Considérons en particulier le cas où A est réduit à un seul élément x ; alors le sous-groupe X engendré par A , qui est formé des puissances x^n pour $n \in \mathbb{Z}$ (prop. 2), est toujours abélien ; d'après l'identité $x^{m+n} = x^m x^n$, l'application $n \rightarrow x^n$ est un homomorphisme du groupe additif \mathbb{Z} sur X ; donc (th. 3) X est isomorphe, soit à \mathbb{Z} , soit à un groupe quotient de \mathbb{Z} , c'est-à-dire (n° 3) au groupe additif des entiers modulo a , où $a > 0$; dans ce dernier cas X est un groupe fini de a éléments.

DÉFINITION 9. — On dit qu'un groupe est monogène s'il est engendré par un seul de ses éléments ; un groupe monogène fini est encore appelé groupe cyclique.

Nous venons de démontrer que :

PROPOSITION 8. — Un groupe monogène est abélien ; s'il est infini, il est isomorphe au groupe additif \mathbb{Z} des entiers rationnels ; s'il est fini et d'ordre n il est isomorphe au groupe additif des entiers modulo n .

Dans un groupe quelconque G , si le sous-groupe (monogène) engendré par un élément $x \in G$ est d'ordre fini p , on dit que x est un élément d'*ordre p* ; le nombre p est donc le plus petit entier > 0 tel que $x^p = e$; si le sous-groupe engendré par x est infini, on dit que x est d'*ordre infini*. Ces définitions, et la prop. 3, entraînent en particulier que, dans un groupe fini G , l'ordre de tout élément de G est un diviseur de l'ordre de G ; d'où, comme corollaire :

PROPOSITION 9. — Dans un groupe fini G d'ordre n , on a $x^n = e$ pour tout $x \in G$.

En effet, si p est l'ordre de x , on a $n = pq$, q entier, donc $x^n = (x^p)^q = e$.

8. Centre d'un groupe ; groupe des commutateurs.

PROPOSITION 10. — *Le centre Z d'un groupe G est un sous-groupe abélien de G, transformé en lui-même par tout automorphisme de G ; tout sous-groupe de Z est un sous-groupe distingué de G.*

Le fait que Z est un sous-groupe de G résulte de la prop. 1 du § 1 et de la prop. 6 du § 2 ; il est évident que ce sous-groupe est transformé en lui-même par tout automorphisme de G ; enfin, comme $xyx^{-1} = y$ pour tout $x \in G$ et tout $y \in Z$, tout sous-groupe de Z est sous-groupe distingué de G.

Si G est abélien, il est identique à son centre. Pour un groupe non abélien G, le centre peut se réduire à l'élément neutre e (c'est le cas en particulier lorsque G est simple).

On aura soin de noter qu'un sous-groupe abélien d'un groupe G n'est pas nécessairement contenu dans le centre de G : par exemple, si G est simple et non abélien, les groupes monogènes engendrés par les éléments de G sont abéliens et non réduits à e.

Cherchons maintenant à quelle condition doit satisfaire un sous-groupe distingué H d'un groupe G pour que le groupe quotient G/H soit abélien. Quels que soient $x \in G$, $y \in G$, on doit avoir $xy \equiv yx \pmod{H}$, ce qui équivaut à $y^{-1}x^{-1}yx \equiv e \pmod{H}$, c'est-à-dire $y^{-1}x^{-1}yx \in H$; l'élément $y^{-1}x^{-1}yx$ est appelé le *commutateur* de x et de y (et se note parfois $x \circ y$) ; on voit donc que H doit contenir l'ensemble des commutateurs de tous les couples (x, y) d'éléments de G, et par suite aussi le sous-groupe C de G engendré par cet ensemble. Le sous-groupe C est appelé le *groupe des commutateurs* (ou *groupe dérivé*) de G ; il est évidemment transformé en lui-même par tout automorphisme de G, et en particulier c'est un sous-groupe distingué de G ; plus généralement, tout endomorphisme φ de G transforme tout commutateur en un commutateur, donc $\varphi(C) \subset C$. En résumé :

PROPOSITION 11. — *Pour qu'un groupe quotient G/H d'un groupe G soit abélien, il faut et il suffit que le sous-groupe distingué H contienne le groupe des commutateurs C de G.*

Si G est abélien, son groupe des commutateurs se réduit à e ;

pour un groupe G non abélien, le groupe des commutateurs peut être identique à G (c'est le cas par exemple si G est simple).

On notera que l'ensemble des commutateurs d'un groupe G n'est pas identique en général au groupe des commutateurs (qu'il engendre) : le produit de deux commutateurs n'est pas un commutateur en général.

9. Groupes à opérateurs.

DÉFINITION 10. — *On appelle groupe à opérateurs un ensemble G muni d'une structure algébrique déterminée par une loi (interne) de groupe, et une ou plusieurs lois de composition externes distributives par rapport à la loi de groupe.*

Autrement dit, si la loi de groupe sur G est notée multiplicativement, et si \perp est une des lois externes de G, on a, pour tout opérateur α de la loi \perp , l'identité

$$\alpha \perp (xy) = (\alpha \perp x)(\alpha \perp y).$$

Les structures de groupe à opérateurs qu'on rencontrera par la suite sont assez variées, chaque espèce étant caractérisée par la donnée des domaines d'opérateurs correspondants, et le plus souvent par des conditions supplémentaires imposées aux lois de composition dont il s'agit.

Dans un groupe à opérateurs G, chaque opérateur produit un *endomorphisme* de la structure de groupe sous-jacente ; la donnée de chacune des lois externes qui déterminent la structure de groupe à opérateurs revient à la donnée d'une famille d'endomorphismes du groupe G ; ces endomorphismes seront souvent appelés les *homothéties* du groupe à opérateurs G. Dans ce qui suit, la loi de groupe de G étant notée multiplicativement, on notera exponentiellement les homothéties de G (suivant les conventions du § 5, n° 1) : le composé d'un opérateur α et d'un élément $x \in G$ s'écrira donc x^α , la distributivité s'exprimant par l'identité $(xy)^\alpha = x^\alpha y^\alpha$.

On dit qu'un groupe à opérateurs G est *abélien* si sa loi de groupe est commutative ; si cette loi est notée additivement, les lois externes se noteront d'ordinaire multiplicativement, à gauche ou à droite (cf. § 5, n° 1).

Sur un groupe G , on peut toujours considérer une loi externe ayant un domaine d'opérateurs réduit à un seul élément ϵ , et définie par $x^\epsilon = x$ pour tout $x \in G$ (autrement dit, le seul opérateur ϵ est opérateur neutre). Cette loi externe et la loi du groupe déterminent sur G une structure de groupe à opérateurs ; mais il n'y a pas lieu de distinguer cette structure de la structure de groupe donnée sur G , car toutes les notions relatives aux structures algébriques, définies au § 4 (parties stables, relations d'équivalence compatibles avec une structure, représentations), sont *identiques* pour ces deux structures. Cela permet donc de considérer les groupes comme des *cas particuliers* des groupes à opérateurs, et de leur appliquer tous les résultats relatifs à ces derniers que nous allons énoncer.

Dans un groupe abélien G , noté par exemple multiplicativement, on a $(xy)^n = x^n y^n$ quel que soit $n \in \mathbb{Z}$ (§ 1, formule (8)) ; la loi de composition externe $(n, x) \rightarrow x^n$ entre entiers $n \in \mathbb{Z}$ et éléments $x \in G$ définit par suite, avec la loi du groupe, une structure de groupe à opérateurs sur G ; ici encore, il n'y aura pas lieu de distinguer cette structure de la structure de groupe sous-jacente, pour la même raison que ci-dessus.

Plus généralement, si G est un groupe abélien à opérateurs, on ne distingue pas sa structure de celle qu'on obtient en adjoignant la loi externe $(n, x) \rightarrow x^n$ aux lois déjà impliquées par la structure de G .

10. Sous-groupes stables de groupes à opérateurs.

Soit G un groupe à opérateurs ; pour que la structure induite par celle de G sur une partie non vide H de G soit une structure de groupe à opérateurs, il faut et il suffit évidemment que H soit un *sous-groupe* de G , et qu'il soit *stable* pour les lois externes de G ; on pose donc la définition suivante :

DÉFINITION 11. — *On appelle sous-groupe stable d'un groupe à opérateurs G un sous-groupe du groupe G , stable par rapport aux lois externes de G (c'est-à-dire appliqué dans lui-même par les homothéties de G), muni de la structure de groupe à opérateurs induite sur lui par celle de G .*

Dans un groupe à opérateurs G , G et $\{e\}$ sont toujours des sous-groupes stables de G ; le groupe des commutateurs d'un groupe G est stable pour toute structure de groupe à opérateurs ayant même loi de groupe ; il n'en est pas de même en général du centre de G . L'intersection de toute famille de sous-groupes stables d'un groupe à opérateurs G est un sous-groupe stable ; le plus petit sous-groupe stable contenant une partie X de G sera dit *engendré* par G .

Remarques. — 1) Lorsqu'on considère un groupe comme groupe à opérateurs (avec un seul opérateur ϵ tel que $x^\epsilon = x$), la notion de sous-groupe stable se confond avec celle de sous-groupe. De même, si G est un groupe abélien à opérateurs, la notion de sous-groupe stable ne change pas lorsqu'on adjoint aux lois externes données la loi x^n .

2) Un sous-groupe distingué d'un groupe G peut encore être défini comme un groupe stable pour la loi externe $(s, x) \rightarrow s^{-1}xs$, dont G est le domaine d'opérateurs : cette loi, jointe à la loi de groupe de G , induit sur tout sous-groupe distingué de G une structure de groupe à opérateurs, dont G est le domaine d'opérateurs.

11. Groupes quotients de groupes à opérateurs.

Le th. 1 s'étend aux groupes à opérateurs. Il suffira de l'énoncer pour une relation compatible à gauche avec la loi de groupe :

THÉORÈME 4. — *Soit R une relation d'équivalence dans un groupe à opérateurs G ; si R est compatible à gauche avec la loi de groupe de G , et compatible avec les lois externes de G , elle est équivalente à une relation de la forme $x^{-1}y \in H$, où H est un sous-groupe stable de G . Réciproquement, si H est un sous-groupe stable quelconque de G , la relation $x^{-1}y \in H$ est une relation d'équivalence compatible avec les lois externes, et compatible à gauche avec la loi de groupe.*

En effet, R est équivalente à la relation $x^{-1}y \in H$, où H est la classe de e (mod. R), et H est un sous-groupe (th. 1) ; pour tout opérateur α , la relation $x \equiv e$ entraîne $x^\alpha \equiv e^\alpha = e$, donc $H^\alpha \subset H$, H est stable. Réciproquement, si H est un sous-groupe stable, la relation $y \in xH$ entraîne $y^\alpha \in x^\alpha H^\alpha \subset x^\alpha H$, donc la relation d'équivalence $x^{-1}y \in H$ est compatible avec les lois externes de G .

Le th. 2 s'étend alors immédiatement. De même la déf. 4 : si

H est un sous-groupe stable distingué d'un groupe à opérateurs, le quotient de G par la relation d'équivalence définie par H , muni de la structure quotient de celle de G , est un groupe à opérateurs appelé *groupe quotient* de G par H , et noté G/H .

12. Représentations de groupes à opérateurs.

Soit G un groupe à opérateurs ; on pourra définir une *représentation* de G dans un ensemble G' si G' est muni d'une structure algébrique déterminée d'une part par une loi de composition interne, d'autre part par un certain nombre de lois externes, dont chacune est associée à une des lois externes de G et a même domaine d'opérateurs (structure *homologique* à celle de G (§ 4, n° 1)) ; une application f de G dans G' est alors une *représentation* (ou un *homomorphisme*) si, quels que soient $x \in G$, $y \in G$ et l'opérateur α de G , $f(x)f(y)$ et $(f(x))^\alpha$ sont définis, et on a

$$f(xy) = f(x)f(y), \quad f(x^\alpha) = (f(x))^\alpha.$$

On notera en particulier qu'un endomorphisme du *groupe à opérateurs* G n'est pas autre chose qu'un endomorphisme de la structure de *groupe* de G , permutable avec toutes les homothéties de G .

N

Comme deux homothéties d'un groupe à opérateurs G ne sont pas nécessairement permutables, une homothétie ne sera pas en général un endomorphisme de la structure de groupe à opérateurs de G .

Le th. 3 subsiste sans modification essentielle ; nous l'énoncerons explicitement :

THÉORÈME 5. — Soit f une représentation d'un groupe à opérateurs G dans un ensemble G' muni d'une structure homologique. L'image $f(G)$ est un groupe à opérateurs (pour la structure induite par celle de G') ayant pour élément neutre $e' = f(e)$. L'image réciproque $H = f^{-1}(e')$ de l'élément neutre de $f(G)$ est un sous-groupe stable distingué de G ; le groupe à opérateurs $f(G)$ est isomorphe au groupe quotient G/H , et la représentation f est composée d'un isomorphisme de G/H dans G' et de l'homomorphisme canonique de G sur G/H .

13. Sous-groupes d'un groupe quotient.

Les théorèmes généraux d'isomorphie (§ 4, th. 2 et 3) s'appliquent naturellement aux groupes à opérateurs (et à plus forte raison aux groupes) ; ils permettent (en utilisant aussi le th. 5 ci-dessus) de caractériser les sous-groupes stables et les groupes quotients de tout groupe quotient d'un groupe à opérateurs donné :

THÉORÈME 6. — Soient G un groupe à opérateurs, H un sous-groupe stable distingué de G , f l'homomorphisme canonique de G sur le groupe quotient $G' = G/H$.

a) L'image réciproque $K = f^{-1}(K')$ d'un sous-groupe stable K' de G' est un sous-groupe stable de G , contenant H ; on a $K' = f(K)$, et K' est isomorphe à K/H .

b) La relation $K = f^{-1}(K')$ établit une correspondance biunivoque entre les sous-groupes stables de G' et les sous-groupes stables de G contenant H .

c) Si K' est un sous-groupe stable distingué de G' , $K = f^{-1}(K')$ est un sous-groupe stable distingué de G , contenant H , et réciproquement ; en outre, G/K est isomorphe à G'/K' .

d) Si L est un sous-groupe stable quelconque (resp. sous-groupe stable distingué) de G , il en est de même de $L.H = H.L$; $H \cap L$ est sous-groupe stable distingué de L , et $L/(H \cap L)$ est isomorphe à H/L .

Démontrons d'abord a) ; si K' est un sous-groupe stable de G' , les relations $f(x) \in K'$, $f(y) \in K'$ entraînent $f(xy^{-1}) = f(x)(f(y))^{-1} \in K'$ et $f(x^\alpha) = (f(x))^\alpha \in K'$ pour tout opérateur α de G , donc $K = f^{-1}(K')$ est sous-groupe stable de G , contenant évidemment H ; comme f applique G sur G' , il applique K sur K' , qui, dans ces conditions, est isomorphe à K/H d'après le th. 5.

Inversement, si K est un sous-groupe stable de G contenant H , K est saturé pour la relation $y \in xH$, donc, si $K' = f(K)$, on a $K = f^{-1}(K')$, ce qui prouve b).

Établissons ensuite d). Si L est un sous-groupe stable de G , la restriction de f à L est une représentation de L dans G' ; d'après le th. 5, l'image réciproque $H \cap L$ de l'élément neutre par cette représentation est sous-groupe stable distingué de L , et $f(L)$ est

isomorphe à $L/(H \cap L)$; en saturant L pour la relation $y \in xH$, on obtient la partie $HL = LH = \bar{f}(f(L))$, qui est donc un sous-groupe stable de G ; et le second th. d'isomorphie (§ 4, th. 3) montre que $f(L)$ est isomorphe à HL/H . On vérifie immédiatement que, si L est sous-groupe stable distingué de G , il en est de même de HL .

Enfin, c) n'est autre que la traduction, pour les groupes à opérateurs, du premier th. d'isomorphie (§ 4, th. 2).

Pour tout sous-groupe stable $K \supset H$ de G , on identifiera en général $f(K)$ avec le groupe quotient K/H ; l'énoncé c) du th. 4 s'exprime alors en disant que le groupe quotient $(G/H)/(K/H)$ est isomorphe à G/K (pour tout sous-groupe stable distingué $K \supset H$).

Remarque. — Le fait que l'image réciproque $\bar{f}(K')$ d'un sous-groupe de G' est un sous-groupe de G , est une conséquence de la proposition plus générale suivante :

Si A' et B' sont deux parties quelconques de G' , on a

$$\bar{f}(A'B') = \bar{f}(A')\bar{f}(B'), \quad \bar{f}(A'^{-1}) = (\bar{f}(A'))^{-1}.$$

En effet, on a évidemment $\bar{f}(A')\bar{f}(B') \subset \bar{f}(A'B')$; d'autre part, si $z \in \bar{f}(A'B')$, il existe $x \in \bar{f}(A')$ et $y \in \bar{f}(B')$ tels que $f(z) = f(x)f(y) = f(xy)$, donc $z \in xyH \subset \bar{f}(A')\bar{f}(B')$. De même, la relation $z \in \bar{f}(A'^{-1})$ équivaut à $f(z) \in A'^{-1}$, donc à $f(z^{-1}) \in A'$ ou $z^{-1} \in \bar{f}(A')$, et finalement à $z \in (\bar{f}(A'))^{-1}$.

COROLLAIRE. — Soient f une représentation d'un groupe à opérateurs G dans un groupe à opérateurs G' , L un sous-groupe stable de G , K un sous-groupe stable distingué de L . Si $H = \bar{f}(e')$, KH est sous-groupe stable distingué de LH , $K \cdot (L \cap H)$ sous-groupe stable distingué de L , $f(K)$ sous-groupe stable distingué de $f(L)$, et les trois groupes quotients LH/KH , $L/(K \cdot (L \cap H))$ et $f(L)/f(K)$ sont isomorphes.

En effet, soit g la restriction de f à L ; g est un homomorphisme de L sur $f(L)$, et on a $g(K) = f(K)$, $\bar{g}(e') = L \cap H$; donc (th. 6), $\bar{g}(f(K)) = K \cdot (L \cap H)$ est sous-groupe stable distingué de L ,

et $f(L)/f(K)$ est isomorphe à $L/(K \cdot (L \cap H))$. D'autre part $\bar{f}(f(L)) = LH$, $\bar{f}(f(K)) = KH$; en considérant la restriction de f à LH , le même raisonnement prouve que KH est distingué dans LH , et que LH/KH est isomorphe à $f(L)/f(K)$.

14. Le théorème de Jordan-Hölder.

L'une des conséquences importantes du th. 6 est le théorème connu sous le nom de théorème de Jordan-Hölder : il énonce une propriété *invariante par isomorphie* de la structure de certains groupes (notamment des groupes *finis*) et, à ce titre, joue un rôle fondamental en Algèbre (voir notamment les chap. II et VII).

DÉFINITION 12. — On appelle *suite de composition* d'un groupe à opérateurs G une suite finie $(G_i)_{0 \leq i \leq n}$ de sous-groupes stables de G , ayant pour premier terme $G_0 = G$, pour dernier terme $G_n = \{e\}$ et telle que G_{i+1} soit sous-groupe distingué de G_i pour $0 \leq i \leq n-1$. Les quotients G_i/G_{i+1} s'appellent les *quotients* de la suite. Une suite de composition Σ' est dite plus fine qu'une suite de composition Σ si Σ est une suite extraite de Σ' .

Si $(G_i)_{0 \leq i \leq n}$ et $(H_j)_{0 \leq j \leq m}$ sont respectivement des suites de composition de deux groupes à opérateurs G et H (ayant des structures homologues) on dit qu'elles sont équivalentes si $m = n$ et s'il existe une application biunivoque φ de l'intervalle $[0, n-1]$ de \mathbb{N} sur lui-même, telle que G_i/G_{i+1} soit isomorphe à $H_{\varphi(i)}/H_{\varphi(i)+1}$ quel que soit i .

On notera qu'en général, une suite extraite d'une suite de composition (G_i) n'est pas une suite de composition, car pour $j > i+1$, G_j n'est pas en général sous-groupe distingué de G_i .

THÉORÈME 7 (Schreier). — *Etant données deux suites de composition Σ_1 , Σ_2 d'un groupe à opérateurs G , il existe deux suites de composition équivalentes Σ'_1 , Σ'_2 , plus fines respectivement que Σ_1 et Σ_2 .*

Soient $\Sigma_1 = (G_i)_{0 \leq i \leq n}$, $\Sigma_2 = (H_j)_{0 \leq j \leq m}$ les deux suites de composition données, ayant respectivement $n+1$ et $m+1$ termes; nous allons voir qu'on peut former la suite de composition Σ'_1 en *intercalant* $m-1$ sous-groupes G'_{ij} ($1 \leq j \leq m-1$) entre

G_i et G_{i+1} pour $0 \leq i \leq n-1$, et la suite Σ'_2 en intercalant $n-1$ sous-groupes H'_{ji} ($1 \leq i \leq n-1$) entre H_j et H_{j+1} pour $0 \leq j \leq m-1$; on obtiendra ainsi deux suites de $mn+1$ sous-groupes de G ; en choisissant convenablement les sous-groupes intercalés, nous allons montrer que ces suites sont des suites de composition équivalentes.

Remarquons pour cela que $G_i \cap H_j$ est sous-groupe de G_i et de H_j , donc (th. 6) $G_{i+1} \cdot (G_i \cap H_j)$ est sous-groupe de G_i contenant G_{i+1} , $H_{j+1} \cdot (G_i \cap H_j)$ sous-groupe de H_j , contenant H_{j+1} ; si on prend $G'_{ij} = G_{i+1} \cdot (G_i \cap H_j)$ ($1 \leq j \leq m-1$) et $H'_{ji} = H_{j+1} \cdot (G_i \cap H_j)$ ($1 \leq i \leq n-1$), $G'_{i,j+1}$ est sous-groupe de G'_{ij} , $H'_{j,i+1}$ sous-groupe de H'_{ji} ; avec les mêmes notations, on a d'ailleurs $G'_{i,0} = G_i$, $G'_{in} = G_{i+1}$, $H'_{j,0} = H_j$, $H'_{jn} = H_{j+1}$; le théorème sera alors une conséquence immédiate du lemme suivant :

LEMME (Zassenhaus). — *Soient H et K deux sous-groupes stables d'un groupe à opérateurs G , H' et K' des sous-groupes stables distingués de H et K respectivement; alors $H' \cdot (H \cap K')$ est sous-groupe distingué de $H' \cdot (H \cap K)$, $K' \cdot (K \cap H')$ est sous-groupe distingué de $K' \cdot (K \cap H)$, et les groupes quotients $(H' \cdot (H \cap K)) / (H' \cdot (H \cap K'))$ et $(K' \cdot (K \cap H)) / (K' \cdot (K \cap H'))$ sont isomorphes.*

D'après le th. 6 appliqué au groupe H , $H' \cap K = H' \cap (H \cap K)$ est sous-groupe distingué de $H \cap K$; de même $K' \cap H$ est sous-groupe distingué de $K \cap H$; donc (th. 6) $(H' \cap K)(K' \cap H)$ est sous-groupe distingué de $H \cap K$. D'après le corollaire du th. 6, appliqué au groupe H , $H' \cdot (H' \cap K) \cdot (K' \cap H) = H' \cdot (H \cap K')$ est sous-groupe distingué de $H' \cdot (H \cap K)$, et le groupe quotient $(H' \cdot (H \cap K)) / (H' \cdot (H \cap K'))$ est isomorphe à

$$(H \cap K) / ((H' \cap K) \cdot (K' \cap H)).$$

Dans ce dernier quotient, H et H' d'une part, K et K' de l'autre, figurent symétriquement; en les permutant, on obtient le résultat annoncé.

C. Q. F. D.

DÉFINITION 13. — *On appelle suite de Jordan-Hölder d'un groupe à opérateurs G une suite de composition Σ strictement décroissante, telle qu'il n'existe aucune suite de composition strictement décroissante, distincte de Σ et plus fine que Σ .*

DÉFINITION 14. — *Un groupe à opérateurs G est dit simple s'il n'existe aucun sous-groupe stable distingué de G autre que G et $\{e\}$.*

PROPOSITION 12. — *Pour qu'une suite de composition strictement décroissante de G soit suite de Jordan-Hölder de G , il faut et il suffit que tous les quotients de la suite soient simples.*

En effet, si la suite de composition strictement décroissante Σ n'est pas suite de Jordan-Hölder, il existe une suite de composition strictement décroissante Σ' plus fine que Σ et distincte de Σ . Il y a donc deux termes consécutifs G_i, G_{i+1} de Σ qui ne sont pas consécutifs dans Σ' ; soit H le premier terme qui suit G_i dans Σ' ; H est un sous-groupe stable distingué de G_i , contenant G_{i+1} et distinct de ce dernier; donc H/G_{i+1} est sous-groupe stable distingué de G_i/G_{i+1} , distinct de celui-ci et de l'élément neutre; G_i/G_{i+1} n'est pas simple. Réciproquement, si Σ est une suite de composition strictement décroissante dont un des quotients G_i/G_{i+1} n'est pas simple, ce quotient contient un sous-groupe stable distingué autre que lui-même et l'élément neutre, dont l'image réciproque dans G_i sera un sous-groupe stable distingué H de G_i , distinct de G_i et de G_{i+1} (th. 6); il suffit d'insérer H entre G_i et G_{i+1} pour avoir une suite de composition strictement décroissante, distincte de Σ et plus fine que Σ .

THÉORÈME 8 (Jordan-Hölder). — *Deux suites de Jordan-Hölder d'un groupe à opérateurs sont équivalentes.*

Soient Σ_1, Σ_2 deux suites de Jordan-Hölder d'un groupe à opérateurs G ; en appliquant le th. 7, on en déduit deux suites de composition équivalentes Σ'_1, Σ'_2 , respectivement plus fines que Σ_1 et Σ_2 ; celles-ci étant des suites de Jordan-Hölder, Σ'_1 est identique à Σ_1 ou s'en déduit en répétant certains termes; la suite des quotients de Σ'_1 se déduit de celle de Σ_1 en insérant un certain nombre de termes isomorphes au groupe $\{e\}$; Σ_1 étant strictement décroissante, la suite des quotients de Σ_1 se déduit de celle de Σ'_1 en supprimant dans cette dernière tous les termes isomorphes à $\{e\}$. De même pour Σ_2 et Σ'_2 . Comme les suites des quotients de Σ'_1 et Σ'_2 ne diffèrent (à des isomorphismes près) que par l'ordre des termes, il en est de même de celles de Σ_1 et Σ_2 ; le théorème est démontré.

COROLLAIRE. — Soit G un groupe à opérateurs dans lequel il existe une suite de Jordan-Hölder. Si Σ est une suite de composition strictement décroissante quelconque de G , il existe une suite de Jordan-Hölder plus fine que Σ .

En effet, soit Σ_0 une suite de Jordan-Hölder de G ; d'après le th. 7, il existe deux suites de composition équivalentes, Σ' et Σ'_0 plus fines respectivement que Σ et Σ_0 ; le raisonnement du th. 8 montre qu'en supprimant de Σ' les termes répétés, on obtient une suite Σ'' équivalente à Σ_0 , donc une suite de Jordan-Hölder, puisque tous ses quotients sont simples (prop. 12); d'ailleurs, comme Σ est strictement décroissante, Σ'' est plus fine que Σ , d'où le corollaire.

Remarque. — Un groupe à opérateurs quelconque G ne possède pas toujours de suite de Jordan-Hölder; un exemple est fourni par le groupe additif \mathbb{Z} des entiers rationnels; la suite $(2^n \cdot \mathbb{Z})_{n \geq 0}$ est une suite infinie strictement décroissante de sous-groupes (distingués) de \mathbb{Z} ; quel que soit p , les p premiers termes de cette suite forment, avec le groupe $\{0\}$, une suite de composition strictement décroissante; s'il existait une suite de Jordan-Hölder pour \mathbb{Z} , elle aurait au moins $p+1$ termes, d'après le corollaire du th. 8; conclusion absurde, puisque p est arbitraire.

Par contre, il existe une suite de Jordan-Hölder dans tout groupe à opérateurs fini G : en effet, parmi les sous-groupes stables distingués de G , distincts de G , soit H_1 un sous-groupe maximal; définissons de même par récurrence H_{n+1} comme un élément maximal de l'ensemble des sous-groupes distingués de H_n , distincts de H_n ; la suite des ordres des H_n est strictement décroissante, donc il existe n tel que $H_n = \{e\}$, et la suite formée de G et des H_i ($1 \leq i \leq n$) est, d'après sa formation, une suite de Jordan-Hölder.

Scholie. — Si un groupe à opérateurs G possède une suite de Jordan-Hölder, le nombre des quotients de cette suite s'appelle la *longueur* de G ; un groupe simple est donc un groupe de longueur 1. Si G et G' sont deux groupes à opérateurs isomorphes, et si G possède une suite de Jordan-Hölder, il en est de même de G' et les suites de Jordan-Hölder de G et G' sont équivalentes; en particulier, les longueurs de G et G' sont égales. Il faut observer que la donnée de la suite des quotients d'une suite de Jordan-Hölder d'un groupe G ne caractérise pas en général ce groupe à une isomorphie près, s'il est de longueur > 1 (voir exerc. 1); mais ce qui

précède montre que le th. de Jordan-Hölder fournit une condition nécessaire d'isomorphie, qu'on utilise fréquemment pour montrer que deux groupes donnés ne sont pas isomorphes.

15. Produits de groupes à opérateurs. Groupes semi-simples.

Tout ce qui a été dit des produits de groupes et des produits directs de sous-groupes (n°s 5 et 6) s'étend aussitôt aux groupes à opérateurs en remplaçant partout « groupe » par « groupe à opérateurs », et « sous-groupe » par « sous-groupe stable ».

DÉFINITION 15. — On dit qu'un groupe à opérateurs G est semi-simple s'il est produit direct d'un nombre fini de sous-groupes simples.

Si G est un groupe semi-simple, produit direct d'une suite $(H_i)_{1 \leq i \leq n}$ de sous-groupes simples, il suit aussitôt des propriétés des produits (n° 5) que, si on pose $K_i = H_1 H_2 \cdots H_i$, K_{i+1} est produit direct de K_i et H_{i+1} pour $1 \leq i \leq n-1$, et $K_n = G$; K_i étant sous-groupe distingué de K_{i+1} , et K_{i+1}/K_i isomorphe à H_i , donc simple par hypothèse, la suite $G, K_{n-1}, \dots, K_1, \{e\}$ est une suite de Jordan-Hölder de G ; le th. de Jordan-Hölder entraîne donc la proposition suivante :

PROPOSITION 13. — Si un groupe semi-simple G est produit direct de deux familles finies $(G_i)_{1 \leq i \leq n}$ et $(H_j)_{1 \leq j \leq m}$ de sous-groupes simples, on a $m = n$, et il existe une application biunivoque φ de l'intervalle $[1, n]$ sur lui-même, telle que $H_{\varphi(i)}$ soit isomorphe à G_i pour $1 \leq i \leq n$.

Le nombre n des sous-groupes simples dont G est le produit direct est la *longueur* de G .

Le raisonnement de la prop. 13 prouve plus généralement que, si G est produit direct de n sous-groupes H_i ($1 \leq i \leq n$), et si chacun des groupes H_i possède une suite de Jordan-Hölder, le groupe G possède également une suite de Jordan-Hölder, dont on obtient la suite des quotients par *juxtaposition* (§ 1, n° 3) des suites des quotients des n suites de Jordan-Hölder des H_i ; en particulier,

si H_i est de longueur h_i , la longueur de G est égale à $\sum_{i=1}^n h_i$.

La structure des *sous-groupes stables distingués* d'un groupe semi-simple est élucidée par la proposition suivante :

PROPOSITION 14. — Soit G un groupe semi-simple, produit direct d'une famille $(H_i)_{1 \leq i \leq n}$ de sous-groupes simples. Si K est un sous-groupe stable distingué de G , il existe une sous-famille $(H_i)_{i \in J}$ de la famille $(H_i)_{1 \leq i \leq n}$ telle que G soit produit direct de K et des groupes H_i de cette sous-famille.

En effet, pour toute partie I de l'intervalle $[1, n]$, désignons par H_I le produit direct des sous-groupes H_i tels que $i \in I$. Considérons les parties I telles que $K \cap H_I$ se réduise à e ; soit J un élément maximal de l'ensemble \mathfrak{F} de ces parties (c'est-à-dire une partie ayant la propriété considérée et dont le nombre d'éléments est le plus grand possible); comme $K \cap H_J = \{e\}$, $K \cdot H_J$ est produit direct de K et H_J (prop. 7). Montrons que $K \cdot H_J = G$, ce qui établira la proposition; il suffit de voir que tous les H_i sont contenus dans $K \cdot H_J$. Or, comme les H_i sont simples, l'intersection $H_i \cap (K \cdot H_J)$, qui est un sous-groupe stable distingué de H_i , ne peut être que H_i ou $\{e\}$; s'il existait un indice k tel que $H_k \cap (K \cdot H_J) = \{e\}$, il en résulterait, en posant $I = J \cup \{k\}$, que l'on aurait $K \cap H_I = \{e\}$, et J ne serait pas élément maximal de \mathfrak{F} , contrairement à l'hypothèse.

COROLLAIRE 1. — Soit K un sous-groupe stable distingué d'un groupe semi-simple G , produit direct d'une famille de sous-groupes simples H_i ($1 \leq i \leq n$); il existe une sous-famille $(H_i)_{i \in J}$ de la famille $(H_i)_{1 \leq i \leq n}$ telle que K soit isomorphe au produit direct des groupes de cette sous-famille. K est donc un groupe semi-simple de longueur $\leq n$; sa longueur ne peut être égale à n que si $K = G$.

En effet, avec les notations de la prop. 14, G est produit direct de K et H_J , donc K est isomorphe à G/H_J ; mais, si J' est le complémentaire de J dans l'intervalle $[1, n]$, G/H_J est isomorphe à $H_{J'}$, d'où le corollaire.

COROLLAIRE 2. — Tout groupe quotient d'un groupe semi-simple G est isomorphe à un sous-groupe stable distingué de G (et en particulier est semi-simple).

En effet, avec les notations de la prop. 14, G/K est isomorphe à H_J .

Exercices. — 1) Déterminer toutes les structures de groupe sur un ensemble de n éléments, pour $2 \leq n \leq 6$ (cf. § 2, exerc. 5). Déterminer les sous-groupes et les groupes quotients de ces groupes, ainsi que leurs suites de Jordan-Hölder : montrer en particulier qu'il existe deux groupes d'ordre 4, non isomorphes, mais dont les suites de Jordan-Hölder ont des quotients isomorphes.

¶ 2) a) Une loi associative $(x, y) \rightarrow xy$ sur un ensemble E est une loi de groupe s'il existe $e \in E$ tel que, pour tout $x \in E$, $ex = x$, et si, pour tout $x \in E$, il existe $x' \in E$ tel que $x'x = e$ (montrer que $xx' = e$, en considérant le composé $x'xx'$; en déduire que e est élément neutre).

b) Montrer qu'il en est de même si, pour tout $x \in E$, la translation à gauche γ_x est une application de E sur E et s'il existe un $a \in E$ tel que la translation à droite δ_a soit une application de E sur E (utiliser la prop. 4 du § 2 pour se ramener à a), ou aux exerc. 11 et 13 du § 2).

3) Dans un groupe G , toute partie stable H finie et non vide est un sous-groupe de G (cf. § 2, exerc. 8).

4) Soient A et B deux sous-groupes d'un groupe G .

a) Montrer que le plus petit sous-groupe contenant A et B (c'est-à-dire le sous-groupe engendré par $A \cup B$) est identique à l'ensemble des composés des suites $(x_i)_{1 \leq i \leq 2n+1}$ d'un nombre impair (quelconque) d'éléments, telles que $x_i \in A$ pour i impair, et $x_i \in B$ pour i pair.

b) Pour que AB soit un sous-groupe de G (auquel cas c'est le sous-groupe engendré par $A \cup B$), il faut et il suffit que A et B soient permutables, c'est-à-dire que $AB = BA$.

c) Si A et B sont permutables, et si C est un sous-groupe contenant A , A est permutable avec $B \cap C$, et on a $A(B \cap C) = C \cap (AB)$.

5) Si un sous-groupe d'un groupe G a pour indice 2, il est distingué dans G .

6) Soit (G_α) une famille de sous-groupes distingués d'un groupe

G , telle que $\bigcap_\alpha G_\alpha = \{e\}$; montrer que G est isomorphe à un sous-groupe du groupe produit $\prod_\alpha (G/G_\alpha)$.

7) Si G est produit direct de deux sous-groupes A et B , et si H est un sous-groupe de G tel que $A \subset H$, H est produit direct de A et de $H \cap B$.

8) Soit H un sous-groupe distingué d'un groupe G . Pour que G soit isomorphe au produit $H \times (G/H)$, il faut et il suffit qu'il existe

une représentation f de G sur H telle que $f(x) = x$ pour tout $x \in H$.

9) Soit G un groupe abélien, H un sous-groupe de G tel que G/H soit un groupe monogène infini. Montrer que G est isomorphe au produit $H \times (G/H)$ (considérer le sous-groupe engendré par un élément d'une classe mod. H engendrant G/H).

10) Soit H un sous-groupe distingué d'un groupe G , contenu dans le centre de G . Montrer que si G/H est un groupe monogène, G est abélien.

11) Si tous les éléments d'un groupe G autres que l'élément neutre sont d'ordre 2, G est abélien ; si G est fini, son ordre n est une puissance de 2 (raisonner par récurrence sur n).

12) Soit G un groupe tel que, pour un entier déterminé $n > 1$, on ait $(xy)^n = x^n y^n$ quels que soient $x \in G$, $y \in G$. Si $G^{(n)}$ désigne l'ensemble des x^n , où x parcourt G , et $G_{(n)}$ l'ensemble des $x \in G$ tels que $x^n = e$, montrer que $G^{(n)}$ et $G_{(n)}$ sont des sous-groupes distingués de G ; si G est fini, l'ordre de $G^{(n)}$ est égal à l'indice de $G_{(n)}$.

13) Soit A une partie non vide d'un groupe G ; on appelle *normalisateur* de A l'ensemble N des $x \in G$ tels que $xAx^{-1} = A$; on appelle *centralisateur* de A l'ensemble K des $x \in G$ tels que $xax^{-1} = a$ quel que soit $a \in A$. Montrer que N est un sous-groupe de G , et K un sous-groupe distingué de N . Si A est un sous-groupe de G , son normalisateur N est le plus grand des sous-groupes H de G tels que A soit sous-groupe distingué de H .

14) Si on désigne par $D(G)$ le groupe des commutateurs ou groupe dérivé d'un groupe G , on définit par récurrence le $k^{\text{ème}}$ groupe dérivé $D^k(G)$ de G , comme égal à $D(D^{k-1}(G))$; montrer que $D^k(G)$ est un sous-groupe de G , tel que, pour tout endomorphisme φ de G , $\varphi(D^k(G)) \subset D^k(G)$. Si H est un sous-groupe de G , $D^k(H) \subset D^k(G)$; si H est distingué, $D^k(G/H)$ est isomorphe à $(H.D^k(G))/H$.

On dit qu'un groupe G est *résoluble* (ou *métabélien*) s'il existe une suite de composition (G_i) de G telle que tous les groupes quotients G_i/G_{i+1} soient abéliens. Montrer que, pour que G soit résoluble, il faut et il suffit qu'il existe un entier k tel que $D^k(G) = \{e\}$. En déduire que tout sous-groupe et tout groupe quotient d'un groupe résoluble est résoluble.

¶ 15) Soit \mathfrak{F} un ensemble de sous-groupes stables d'un groupe à opérateurs G ; on dit que \mathfrak{F} satisfait à la condition maximale (resp. condition minimale) si toute partie de \mathfrak{F} , ordonnée par inclusion, possède un élément maximal (resp. minimal).

On suppose que l'ensemble de tous les sous-groupes stables d'un groupe G satisfait à la condition minimale.

a) Prouver qu'il n'existe aucun sous-groupe stable de G isomorphe à G et distinct de G (raisonner par l'absurde en montrant

que l'hypothèse entraînerait l'existence d'une suite infinie strictement décroissante de sous-groupes stables de G).

b) On appelle sous-groupes distingués *minimaux* les éléments minimaux de l'ensemble des sous-groupes stables distingués de G non réduits à e . Soit \mathfrak{M} un ensemble de sous-groupes distingués minimaux de G , S le plus petit sous-groupe stable de G contenant tous les sous-groupes appartenant à \mathfrak{M} ; montrer que S est produit direct d'un nombre fini de sous-groupes distingués minimaux de G (soit (M_n) une suite de sous-groupes distingués minimaux de G appartenant à \mathfrak{M} , et telle que M_{n+1} ne soit pas contenu dans le sous-groupe stable engendré par la réunion de M_1, M_2, \dots, M_n ; soit S_k le sous-groupe stable engendré par la réunion des M_n d'indice $n \geq k$; montrer qu'on a $S_{k+1} = S_k$ à partir d'un certain rang, et par suite que (M_n) est une suite finie ; utiliser enfin la prop. 7).

c) Montrer que tout sous-groupe distingué minimal M de G est produit direct d'un nombre fini de sous-groupes stables, simples et isomorphes entre eux (soit N un sous-groupe distingué minimal de M ; montrer que M est le plus petit sous-groupe stable de G contenant tous les sous-groupes aNa^{-1} , où a parcourt G , et appliquer ensuite b) au groupe M).

16) Si l'ensemble des sous-groupes stables d'un groupe à opérateurs G satisfait aux conditions maximale et minimale (exerc. 15), G possède une suite de Jordan-Hölder (considérer, pour un sous-groupe H de G , un élément maximal de l'ensemble des sous-groupes stables distingués de H , distincts de H).

¶ 17) Soit G un groupe à opérateurs ; on dit qu'une suite de composition (G_i) de G est *distinguée* si tous les G_i sont des sous-groupes stables distingués de G ; une suite distinguée Σ est dite *principale* si elle est strictement décroissante, et s'il n'existe aucune suite distinguée distincte de Σ , plus fine que Σ , et strictement décroissante.

a) Si (G_i) et (H_j) sont deux suites distinguées de G , montrer qu'il existe deux suites distinguées équivalentes, plus fines respectivement que (G_i) et (H_j) (appliquer le th. de Schreier en considérant un domaine d'opérateurs convenable pour G). Donner une seconde démonstration de cette proposition, en « intercalant » les sous-groupes $G'_{ij} = G_i \cap (G_{i+1}H_j)$ et $H'_{ji} = H_j \cap (H_{j+1}G_i)$ dans les suites (G_i) et (H_j) respectivement.

b) Si G possède une suite principale, deux suites principales quelconques de G sont équivalentes ; pour toute suite distinguée Σ strictement décroissante, il existe une suite principale plus fine que Σ . En déduire que, pour que G possède une suite principale, il faut et il suffit que l'ensemble des sous-groupes stables distingués de G satisfasse aux conditions maximale et minimale.

c) Si G possède une suite principale, et si l'ensemble des sous-groupes stables de G satisfait à la condition minimale, tout groupe

quotient G_i/G_{i+1} est produit direct d'un nombre fini de sous-groupes stables simples et isomorphes entre eux (utiliser l'exerc. 15).

¶ 18) Soit (H_i) une famille quelconque de sous-groupes stables d'un groupe à opérateurs G ; on dit encore que G est *produit direct* de cette famille si : 1° pour $i \neq x$, tout élément de H_i est permutable avec tout élément de H_x ; 2° pour tout $x \in G$, il existe, pour chaque i , un élément $x_i \in H_i$ et un seul, tel que $x_i = e$ sauf pour un nombre fini d'indices i_1, i_2, \dots, i_n , et qu'on ait $x = x_{i_1} x_{i_2} \cdots x_{i_n}$. On dit que G est *complètement réductible* s'il est produit direct d'une famille de sous-groupes *simples*.

a) Montrer que, si G est produit direct de la famille de sous-groupes (H_i) , il est isomorphe à un sous-groupe du groupe produit

$$H = \prod_i H_i, \text{ distinct de } H \text{ si la famille } (H_i) \text{ est infinie; en déduire que les } H_i \text{ sont des sous-groupes distingués de } G.$$

b) Étendre aux produits directs infinis et aux groupes complètement réductibles les propositions 7 et 14 (pour généraliser la prop. 14, on fera usage du th. de Zorn).

c) Soit G un groupe à opérateurs, engendré par la réunion d'une famille $(H_i)_{i \in I}$ de sous-groupes stables distingués *simples* de G . Montrer qu'il existe une sous-famille $(H_i)_{i \in J}$ telle que G soit produit direct de cette famille (considérer les parties J de I telles que le sous-groupe engendré par la réunion de la famille $(H_i)_{i \in J}$ soit produit direct de cette famille, et prendre dans l'ensemble de ces parties un élément maximal, dont on démontrera l'existence par le th. de Zorn).

19) Soit L un monoïde libre (§ 1, n° 3) engendré par deux familles $(x_i), (y_i)$ ayant même ensemble d'indices, L' le monoïde obtenu en adjoignant à L un élément neutre e (§ 2, exerc. 1). Montrer que l'ensemble quotient de L' obtenu en identifiant à e tous les composés $x_i y_i$ et $y_i x_i$ (§ 4, exerc. 2 c)) est un groupe, engendré par la famille (x_i) , et qu'on appelle le *groupe libre* engendré par cette famille. Si G est un groupe engendré par une famille (a_i) de ses éléments, montrer que G est isomorphe à un groupe quotient du groupe libre G' engendré par cette famille; ce groupe quotient peut toujours être considéré comme obtenu en *identifiant* chaque élément d'une famille (x_λ) d'éléments de G' à l'élément de même indice d'une seconde famille (y_λ) d'éléments de G' (ayant même ensemble d'indices) (cf. § 4, exerc. 2 c)); on dit que le groupe G est le groupe engendré par les générateurs a_i soumis aux *relations de définition* $x_\lambda = y_\lambda$.

¶ 20) a) Soit G un groupe fini d'ordre mn , tel qu'il existe un

sous-groupe distingué H de G qui soit cyclique d'ordre m , le groupe quotient G/H étant cyclique d'ordre n . Montrer que G est engendré par deux éléments a, b tels que $a^m = e$, $b^n = a^r$, $bab^{-1} = a^s$, où r et s sont deux entiers tels que $r(s-1)$ et s^n-1 soient multiples de m (prendre pour a un élément engendrant H , pour b un élément d'une classe engendrant G/H ; exprimer par des puissances de a les éléments $b^k a^{kb^{-1}}$, et appliquer en particulier aux cas $h = n, k = 1$, et $h = 1, k = r$).

b) On considère inversement le groupe $G(m, n, r, s)$ engendré par deux générateurs a, b , soumis aux relations de définition $a^m = e$, $b^n = a^r$, $bab^{-1} = a^s$, où m et n sont deux entiers ≥ 0 , r et s deux entiers quelconques; montrer que, si $m, r(s-1)$ et s^n-1 ne sont pas tous nuls, $G(m, n, r, s)$ est un groupe fini d'ordre qn , où q est le plus grand commun diviseur de $m, |r(s-1)|$ et $|s^n-1|$; dans ce groupe, le sous-groupe H engendré par a est sous-groupe distingué d'ordre q , et G/H est un groupe cyclique d'ordre n (prouver que tout élément de $G(m, n, r, s)$ peut s'écrire sous la forme $a^x b^y$, où x et y sont deux entiers tels que $0 \leq x \leq q-1, 0 \leq y \leq n-1$, et que $G(m, n, r, s)$ est isomorphe au groupe formé des couples (x, y) d'entiers soumis aux conditions précédentes, avec la loi de composition

$$(x, y) \cdot (x', y') = \begin{cases} (x + x's^y, y + y') & \text{si } y + y' \leq n-1 \\ (x + x's^y + r, y + y' - n) & \text{si } y + y' \geq n \end{cases}$$

la première coordonnée du second membre étant une somme modulo q). Examiner les cas où $m = r(s-1) = s^n-1 = 0$.

Le groupe $G(n, 2, 0, -1)$ est appelé *groupe diédral* d'ordre $2n$ et noté \mathfrak{D}_{2n} ; le groupe $G(4, 2, 2, -1)$ est un groupe d'ordre 8 dit *groupe quaternionique* et noté \mathfrak{Q} . Montrer que, dans \mathfrak{Q} , tout sous-groupe est distingué, et que l'intersection des sous-groupes distincts de $\{e\}$ est un sous-groupe distinct de $\{e\}$. Prouver que \mathfrak{D}_8 n'est pas isomorphe à \mathfrak{Q} .

¶ 21) Soit E un quasi-groupe (§ 5, exerc. 5) non associatif, noté multiplicativement, possédant un idempotent e , et tel que $(xy)(zt) = (xz)(yt)$ quels que soient x, y, z, t . On désigne par $u(x)$ l'élément de E tel que $u(x)e = x$, par $v(x)$ l'élément de E tel que $ev(x) = x$; montrer que la loi de composition $(x, y) \rightarrow u(x)v(y)$ est une loi de groupe abélien sur E , pour laquelle e est élément neutre, que les applications $x \rightarrow xe$ et $y \rightarrow ey$ sont des endomorphismes permutables de cette structure de groupe, et que $xy = u(xe)v(ey)$ (on commencera par établir les identités $e(xy) = (ex)(ey)$, $(xy)e = (xe)(ye)$, $e(xe) = (ex)e$; on remarquera ensuite que les relations $x = y$, $ex = ey$ et $xe = ye$ sont équivalentes). Réciproque.

¶ 22) On considère, sur un ensemble E , une loi interne non

partout définie, notée multiplicativement, et satisfaisant aux conditions suivantes : 1^o si l'un des composés $(xy)z$, $x(yz)$ est défini, il en est de même de l'autre et ils sont égaux (cf. § 1, exerc. 3) ; 2^o si x, x', y sont tels que xy et $x'y$ (resp. yx et yx') soient définis et égaux, on a $x = x'$; 3^o pour tout $x \in E$, il existe trois éléments notés e_x, e'_x et x^{-1} tels que $e_x x = x, e_x x' = x, x^{-1} x = e'_x$; e_x est appelé unité à gauche de x , e'_x unité à droite de x , x^{-1} inverse de x (par abus de langage).

a) Montrer que les composés $xx^{-1}, x^{-1}e_x, e'_x x^{-1}, e_x e_x, e'_x e'_x$ sont définis, et qu'on a $xx^{-1} = e_x, x^{-1}e_x = e'_x x^{-1} = x^{-1}, e_x e_x = e_x, e'_x e'_x = e'_x$.

b) Tout idempotent e de E (§ 1, n° 4) est unité à gauche pour tous les x tels que ex soit défini, unité à droite pour tous les y tels que ye soit défini.

c) Pour que le composé xy soit défini, il faut et il suffit que l'unité à droite de x soit la même que l'unité à gauche de y (pour voir que la condition est suffisante, utiliser la relation $e_y = yy^{-1}$) ; si $xy = z$, on a $x^{-1}z = y, zy^{-1} = x, y^{-1}x^{-1} = z^{-1}, z^{-1}x = y^{-1}, yz^{-1} = x^{-1}$ (les composés écrits aux premiers membres de ces relations étant définis).

d) Pour deux idempotents quelconques e, e' de E , on désigne par $G_{e,e'}$ l'ensemble des $x \in E$ tels que e soit unité à gauche et e' unité à droite de x . Montrer que, si $G_{e,e'}$ n'est pas vide, c'est un groupe pour la loi induite par celle de E .

On dit que E est un *groupoïde* s'il satisfait en outre à la condition suivante : 4^o quels que soient les idempotents $e, e', G_{e,e'}$ n'est pas vide.

e) Dans un groupoïde E , si $a \in G_{e,e'}$, montrer que $x \rightarrow xa$ est une application biunivoque de $G_{e,e'}$ sur $G_{e,e'}$, $y \rightarrow ay$ une application biunivoque de $G_{e',e'}$ sur $G_{e,e'}$, $x \rightarrow a^{-1}xa$ un isomorphisme du groupe $G_{e,e'}$ sur le groupe $G_{e',e'}$.

f) Montrer que la loi définie dans l'exerc. 4b) du § 1 détermine une structure de groupoïde sur l'ensemble Ψ , si tous les ensembles de la famille \mathfrak{F} sont équipotents.

23) a) Étant donné un ensemble quelconque E , on considère, dans l'ensemble $E \times E$, la loi de composition non partout définie, notée multiplicativement, pour laquelle le composé de (x, y) et de (y', z) n'est défini que si $y' = y$, et a dans ce cas la valeur (x, z) . Montrer que $E \times E$, muni de cette loi de composition, est un groupoïde (exerc. 22).

b) Soit $(x, y) \equiv (x', y')$ (R) une relation d'équivalence compatible avec la loi de composition précédente (c'est-à-dire telle que $(x, y) \equiv (x', y')$ et $(y, z) \equiv (y', z')$ entraînent $(x, z) \equiv (x', z')$) ; on suppose en outre que la relation R satisfait à la condition suivante : quels que soient x, y, z , il existe un $t \in E$ et un seul tel que

$(x, y) \equiv (z, t)$, et il existe un $u \in E$ tel que $(x, y) \equiv (u, z)$. Montrer que, dans ces conditions, la structure quotient par R de la structure de groupoïde de $E \times E$ est une structure de groupe (prouver d'abord que la loi quotient est partout définie, puis que, si $\bar{x}, \bar{y}, \bar{z}$ sont trois classes telles que $\bar{xy} = \bar{zz}$, on a $\bar{y} = \bar{z}$; établir enfin que, quels que soient $x \in E, y \in E$, on a $(x, x) \equiv (y, y)$).

c) Soit G le groupe obtenu en munissant le quotient de $E \times E$ par R de la structure précédente. Soit a un élément quelconque de E ; si, pour tout $x \in E$, $f_a(x)$ désigne la classe mod. R de (a, x) , montrer que f_a est une application biunivoque de E sur G , et que la relation $(x, y) \equiv (x', y')$ est équivalente à la relation $f_a(x)(f_a(x'))^{-1} = f_a(y)(f_a(y'))^{-1}$.

Pour que G soit abélien, il faut et il suffit que la relation $(x, y) \equiv (x', y')$ entraîne $(x, x') \equiv (y, y')$.

¶ 24) Soit E un ensemble, f une application de E^m dans E ; on écrira $f(x_1, x_2, \dots, x_m) = x_1 x_2 \dots x_m$; on suppose que f satisfait aux conditions suivantes :

1^o On a identiquement

$$(x_1 x_2 \dots x_m) x_{m+1} \dots x_{2m-1} = x_1 (x_2 x_3 \dots x_{m+1}) x_{m+2} \dots x_{2m-1} ;$$

2^o Quels que soient a_1, a_2, \dots, a_{m-1} , les applications

$$x \rightarrow x a_1 a_2 \dots a_{m-1}$$

$$x \rightarrow a_1 a_2 \dots a_i x a_{i+1} \dots a_{m-1} \quad (1 \leq i \leq m-2)$$

$$x \rightarrow a_1 a_2 \dots a_{m-1} x$$

sont des applications biunivoques de E sur E .

a) Montrer qu'on a identiquement

$$(x_1 x_2 \dots x_m) x_{m+1} \dots x_{2m-1} = x_1 x_2 \dots x_i (x_{i+1} \dots x_{i+m}) x_{i+m+1} \dots x_{2m-1}$$

pour tout indice i tel que $1 \leq i \leq m-1$ (raisonner par récurrence sur i , en considérant l'élément

$$((x_1 x_2 \dots x_m) x_{m+1} \dots x_{2m-1}) a_1 a_2 \dots a_{m-1} \dots$$

b) Quels que soient a_1, a_2, \dots, a_{m-2} , il existe $u \in E$ tel que l'on ait identiquement en x

$$x = x a_1 a_2 \dots a_{m-2} u = u a_1 a_2 \dots a_{m-2} x$$

(raisonner comme dans la prop. 4 du § 2).

c) Dans l'ensemble E^k des suites (u_1, u_2, \dots, u_k) de k éléments de E ($1 \leq k \leq m-1$) on considère la relation d'équivalence R_k qui s'énonce : quels que soient $x_1, x_2, \dots, x_{m-k}, u_1 u_2 \dots u_k x_1 x_2 \dots x_{m-k} = v_1 v_2 \dots v_k x_1 x_2 \dots x_{m-k}$; on désigne par E_k l'ensemble quotient E^k / R_k , par G l'ensemble « somme » (Ens. R, § 4, n° 5) de $E_1 = E, E_2, \dots, E_{m-1}$. Soient $\alpha \in E_i, \beta \in E_j$; si (u_1, u_2, \dots, u_i) est

une suite de la classe α , (ν_1, \dots, ν_j) une suite de la classe β , on considère la suite $(u_1, u_2, \dots, u_i, \nu_1, \dots, \nu_j)$ de E^{i+j} si $i + j < m$, la suite $(u_1, u_2, \dots, u_{i+m}, (u_{i+m+1} \dots u_i \nu_1 \nu_2 \dots \nu_j))$ de $E^{i+j-m+1}$ si $i + j \geq m$; montrer que la classe de cette suite dans E_{i+j} (resp. $E_{i+j-m+1}$) ne dépend que des classes α et β ; on la désigne par $\alpha \cdot \beta$. Montrer qu'on définit ainsi sur G une loi de groupe, que $H = E_{m-1}$ est sous-groupe distingué de G , et que le groupe quotient G/H est cyclique d'ordre $m-1$; prouver enfin que E est identique à une classe (mod. H) engendant G/H , et que $x_1 x_2 \dots x_m$ n'est autre que le composé, dans le groupe G , de la suite (x_1, x_2, \dots, x_m) .

§ 7. — Groupes de transformations.

1. Groupes de transformations.

Comme nous l'avons déjà signalé (§ 6, no 1), l'ensemble des applications biunivoques d'un ensemble E sur lui-même forme un groupe pour la loi de composition $f \circ g$; on désigne ce groupe par la notation \mathfrak{S}_E , et on l'appelle *groupe symétrique* (ou *groupe de toutes les permutations*) de l'ensemble E . Si E et E' sont deux ensembles équivalents, φ une application biunivoque de E sur E' , ψ l'application réciproque de φ , l'application $f \rightarrow \varphi \circ f \circ \psi$ est un *isomorphisme* du groupe symétrique \mathfrak{S}_E sur le groupe symétrique $\mathfrak{S}_{E'}$.

Lorsque E est l'intervalle $[1, n]$ de l'ensemble N des entiers naturels, le groupe symétrique correspondant se note \mathfrak{S}_n ; c'est un groupe fini d'ordre $n!$; le groupe symétrique d'un ensemble quelconque de n éléments est isomorphe à \mathfrak{S}_n .

DÉFINITION 1. — *Tout sous-groupe du groupe symétrique \mathfrak{S}_E est appelé groupe de permutations, ou groupe de transformations, de l'ensemble E .*

On réserve le plus souvent les noms de groupe de permutations et de groupe symétrique au cas où E est fini; tout groupe de permutations de E est alors fini. Si E a n éléments, tout groupe de permutations de E est dit de *degré n* .

Exemples. — 1) *Groupe alterné.* Etant donnée une permutation

$$\pi \in \mathfrak{S}_n, \text{ considérons le produit d'entiers naturels } V_n = \prod_{1 \leq i < j \leq n} (j-i)$$

et formons le produit $\pi(V_n) = \prod_{1 \leq i < j \leq n} (\pi(j) - \pi(i))$; on a

$\pi(V_n) = \epsilon_\pi \cdot V_n$, où $\epsilon_\pi = (-1)^v$, v désignant le nombre des couples (i, j) tels que $1 \leq i < j \leq n$ et $\pi(i) > \pi(j)$ (nombre qu'on appelle *nombre d'inversions* de π). Si f est une application quelconque de N dans N * (ou plus généralement dans un anneau commutatif)*, on a aussi

$$\prod_{1 \leq i < j \leq n} (f(\pi(j)) - f(\pi(i))) = \epsilon_\pi \prod_{1 \leq i < j \leq n} (f(j) - f(i)).$$

Le nombre ϵ_π est appelé la *signature* de la permutation π ; π est dite *paire* (resp. *impaire*) si $\epsilon_\pi = +1$ (resp. $\epsilon_\pi = -1$). La permutation identique ω (élément neutre de \mathfrak{S}_n) est paire. On appelle *transposition* de deux nombres i, j tels que $1 \leq i < j \leq n$ la permutation $\tau \in \mathfrak{S}_n$ telle que $\tau(i) = j$, $\tau(j) = i$, $\tau(h) = h$ pour tout h distinct de i et j ; une transposition est *impaire*.

Si π, ρ sont deux permutations de \mathfrak{S}_n , et $\sigma = \pi\rho$, on a

$$\sigma(V_n) = \epsilon_\rho \cdot \pi(V_n) = \epsilon_\pi \epsilon_\rho V_n$$

d'où la relation

$$(1) \quad \epsilon_{\pi\rho} = \epsilon_\pi \epsilon_\rho$$

qui prouve que l'application $\pi \rightarrow \epsilon_\pi$ est une *représentation* de \mathfrak{S}_n sur le groupe multiplicatif formé des entiers $+1$ et -1 . L'ensemble des permutations paires de \mathfrak{S}_n est l'image réciproque de $+1$ par cette représentation; c'est donc un sous-groupe distingué d'indice 2 (et par suite d'ordre $\frac{n!}{2}$) de \mathfrak{S}_n , qu'on appelle *groupe alterné de degré n* et qu'on désigne par la notation \mathfrak{A}_n .

2) *Groupes des translations d'un groupe.* Si G est un groupe, les *translations à gauche* γ_x (§ 2, no 2) de G sont des permutations de G (§ 2, prop. 3); l'ensemble Γ de ces translations est un *groupe de permutations* de G , *isomorphe* à G . En effet, l'application $x \rightarrow \gamma_x$ de G sur Γ est une *représentation* (§ 2, prop. 1); elle est *biunivoque*, car la relation $\gamma_x = \gamma_y$ entraîne $xe = ye$, donc $x = y$.

On montre de même que l'ensemble Δ des translations à droite de G est un groupe de permutations de G , *isomorphe* au groupe opposé de G , donc *isomorphe* à G .

*3) Dans un espace euclidien, les *déplacements* forment un groupe de transformations; les *translations* forment un sous-groupe de ce groupe; il en est de même des *rotations* autour d'un point (voir chap. IX).*

2. Représentations d'un groupe dans un groupe de transformations.

Étant donné un groupe G , soit φ un isomorphisme de G dans le groupe symétrique \mathfrak{S}_E d'un ensemble E ; on dit que l'image $\varphi(G)$ est une *réalisation du groupe G comme groupe de transformations de E* .

Tout groupe G admet des réalisations comme groupe de transformations, à savoir les groupes des translations de G .

Plus généralement, considérons une *représentation* d'un groupe G dans le groupe symétrique \mathfrak{S}_E d'un ensemble E , et désignons par f_α la permutation de E qui correspond à l'élément $\alpha \in G$ par cette représentation; l'image Γ de G par la représentation $\alpha \rightarrow f_\alpha$ est un groupe de transformations de E , isomorphe au groupe quotient G/K , où K est le sous-groupe distingué de G formé des éléments $\alpha \in G$ tels que f_α soit la permutation identique de E (§ 6, th. 3).

On peut donc dire que Γ est une *réalisation* de G/K comme groupe de transformations.

La représentation $\alpha \rightarrow f_\alpha$ définit sur l'ensemble E une *loi de composition externe* entre opérateurs $\alpha \in G$ et éléments $x \in E$, le composé de α et de x étant $f_\alpha(x)$ (cf. § 3, n° 1): cette loi satisfait aux deux conditions suivantes: a) elle est *associative* par rapport à la loi du groupe G (§ 5, n° 2) puisque $f_\alpha \circ f_\beta = f_{\alpha\beta}$; b) l'élément neutre e de G est *opérateur neutre* pour la loi externe, puisque f_e est la permutation identique de E .

En particulier la donnée d'un *groupe de transformations* quelconque Γ d'un ensemble E définit sur E une loi externe satisfaisant aux conditions précédentes, le composé d'un opérateur $\sigma \in \Gamma$ et d'un élément $x \in E$ étant $\sigma(x)$.

Nous allons voir que les conditions a) et b) caractérisent les lois externes obtenues de la manière précédente. De façon précise:

PROPOSITION 1. — Soit E un ensemble muni d'une loi de composition externe $(x, x) \rightarrow \sigma x$, dont le domaine d'opérateurs G est un groupe, et qui satisfait aux conditions suivantes :

a) La loi externe est associative par rapport à la loi du groupe G (autrement dit, $\alpha(\beta x) = (\alpha\beta)x$, quels que soient α, β, x , le groupe G étant noté multiplicativement);

b) l'élément neutre e de G est opérateur neutre pour la loi externe (autrement dit, $\epsilon x = x$ pour tout $x \in E$).

Dans ces conditions, pour tout $\alpha \in G$, l'application f_α produite par α est une permutation de E , et l'application $\alpha \rightarrow f_\alpha$ est une *représentation* de G dans le groupe symétrique \mathfrak{S}_E .

En effet, la relation $y = \alpha x$ entraîne $\alpha^{-1}y = \alpha^{-1}(\alpha x) = (\alpha^{-1}\alpha)x = \epsilon x = x$, et réciproquement, donc $x \rightarrow \alpha x$ est bien une permutation de E : la seconde partie de la proposition résulte de l'associativité de la loi externe par rapport à la loi du groupe.

On dira pour abréger qu'un ensemble E muni de la structure déterminée par une loi externe satisfaisant aux conditions de la prop. 1 est un ensemble *muni d'un groupe d'opérateurs* G ; on dira aussi que le groupe G *opère* dans l'ensemble E .

3. Extensions d'un groupe de transformations.

Un exemple important de représentations d'un groupe sur un groupe de transformations est fourni par les *extensions* de groupes de transformations. Étant donnés (par exemple) trois ensembles F_1, F_2, F_3 , des permutations f_1, f_2, f_3 de F_1, F_2, F_3 respectivement, et un ensemble M de l'*échelle d'ensembles* (*Ens. R*, § 8) ayant pour base F_1, F_2, F_3 , on sait définir, en procédant de proche en proche dans l'échelle, une permutation de M appelée *extension* de f_1, f_2, f_3 à M , et que nous désignerons par $\varphi_M(f_1, f_2, f_3)$.

Rappelons brièvement comment se fait cette définition; deux cas à sont distinguer :

1^o On a $M = \mathfrak{P}(L)$, où L est un ensemble de l'échelle pour lequel $\varphi_L(f_1, f_2, f_3)$ a déjà été défini; alors $\varphi_M(f_1, f_2, f_3)$ n'est autre que l'extension de $\varphi_L(f_1, f_2, f_3)$ aux ensembles des parties (*Ens. R*, § 2, n° 9);

2^o On a $M = P \times Q$, où P et Q sont des ensembles de l'échelle pour lesquels $\varphi_P(f_1, f_2, f_3)$ et $\varphi_Q(f_1, f_2, f_3)$ ont été définies; alors $\varphi_M(f_1, f_2, f_3)$ est l'extension de ces deux applications aux ensembles produits (*Ens. R*, § 3, n° 14).

Si g_1, g_2, g_3 sont trois autres permutations de F_1, F_2, F_3 respectivement, il résulte aussitôt de la définition précédente qu'on a $\varphi_M(f_1 \circ g_1, f_2 \circ g_2, f_3 \circ g_3) = \varphi_M(f_1, f_2, f_3) \circ \varphi_M(g_1, g_2, g_3)$; autrement dit, φ_M est une *représentation* du groupe produit

$\mathfrak{S}_{F_1} \times \mathfrak{S}_{F_2} \times \mathfrak{S}_{F_3}$ dans le groupe \mathfrak{S}_M . Si $\Gamma_1, \Gamma_2, \Gamma_3$ sont des groupes de transformations de F_1, F_2, F_3 respectivement, la restriction de φ_M au groupe produit $\Gamma_1 \times \Gamma_2 \times \Gamma_3$ est appelée *représentation canonique* de ce groupe dans \mathfrak{S}_M ; l'image de $\Gamma_1 \times \Gamma_2 \times \Gamma_3$ par cette représentation s'appelle l'*extension* de ce groupe produit à l'ensemble M .

Soit maintenant G un groupe quelconque, $h_i (i = 1, 2, 3)$ une représentation de G sur un groupe de transformations Γ_i de F_i ; si on pose, pour tout $\sigma \in G$, $\sigma_M = \varphi_M(h_1(\sigma), h_2(\sigma), h_3(\sigma))$, l'application $\sigma \rightarrow \sigma_M$ est une *représentation* de G dans \mathfrak{S}_M , qu'on appelle l'*extension* à l'ensemble M des représentations h_1, h_2, h_3 .

En particulier, si on prend pour G un groupe de transformations Γ_1 de F_1 , pour h_1 l'application identique de Γ_1 sur lui-même, pour h_2 et h_3 les applications constantes de Γ_1 sur les groupes Γ_2, Γ_3 réduits aux permutations identiques de F_2 et F_3 respectivement, l'extension de ces représentations à M s'appelle encore *représentation canonique* de Γ_1 dans \mathfrak{S}_M ; il est facile de voir (de proche en proche dans l'échelle) que c'est un isomorphisme de Γ_1 dans \mathfrak{S}_M , lorsque M n'appartient pas à l'échelle ayant pour base les seuls ensembles F_2, F_3 .

Il peut se faire qu'une partie P de M soit telle que, pour tout $\sigma \in G$, la *restriction* à P de σ_M soit une permutation de P ; si on désigne cette permutation par σ_P , l'application $\sigma \rightarrow \sigma_P$ est alors une représentation de G dans \mathfrak{S}_P , qu'on appelle encore l'*extension* à P des représentations h_1, h_2, h_3 .

On a un exemple important de ce fait en prenant pour M l'ensemble des parties d'un produit $K \times L$, où K et L sont deux ensembles de l'échelle, pour P l'ensemble des *applications* de K dans L , qu'on peut identifier avec la partie de M formée des *ensembles représentatifs* de ces applications (Ens. R, § 3, no 5); l'élément de M qui correspond, par σ_M , à l'ensemble représentatif d'une application w de K dans L , est l'ensemble représentatif de l'application $\sigma_K(z) \rightarrow \sigma_L(w(z))$.

4. Invariants d'un groupe d'opérateurs. Groupes d'automorphismes.

DÉFINITION 2. — *Etant donné un ensemble E , muni d'un groupe d'opérateurs G , on dit qu'un élément $x \in E$ est un invariant du groupe G (ou que x est invariant par G , ou que G laisse invariant*

x), si x est invariant par tous les opérateurs du groupe G (autrement dit, si, pour tout $\alpha \in G$, on a $\alpha x = x$).

Si on se donne une représentation f d'un groupe G sur un groupe de transformations Γ d'un ensemble E , elle définit G comme groupe d'opérateurs de E (no 2); un invariant de ce groupe d'opérateurs s'appelle aussi *invariant du groupe G , relatif à la représentation f* .

Plus généralement, soient (par exemple) F_1, F_2, F_3 trois ensembles, $\Gamma_i (i = 1, 2, 3)$ un groupe de transformations de F_i , h_i une représentation de G sur Γ_i , M un ensemble de l'échelle ayant pour base F_1, F_2, F_3 (ou une partie convenable d'un ensemble de cet échelle). Si $\sigma \rightarrow \sigma_M$ est l'extension à M des représentations h_1, h_2, h_3 (no 3), on dira, par abus de langage, qu'un invariant de G , relatif à cette représentation, est un invariant de G , *relatif aux représentations h_1, h_2, h_3* .

Un cas particulier important de cette notion est celle d'*application invariante* par le groupe G ; si K et L sont deux ensembles de l'échelle ayant pour base F_1, F_2, F_3 , et w une application de K dans L , on dira que w est *invariante* par G si $\sigma_L(w(z)) = w(\sigma_K(z))$ quels que soient $z \in K$ et $\sigma \in G$. On dit aussi dans ce cas que $w(z)$ est un *covariant* de z (relativement au groupe G et aux représentations h_1, h_2, h_3).

Lorsqu'on considère un groupe de transformations Γ_1 d'un ensemble F_1 , et qu'on parle d'*invariant* de Γ_1 dans un ensemble M de l'échelle ayant pour base F_1 et (par exemple) deux ensembles F_2, F_3 , sans préciser davantage, il doit être entendu qu'il s'agit d'un invariant de Γ_1 relatif à la représentation canonique (no 3) de Γ_1 dans \mathfrak{S}_M .

Exemples. — 1) Si Γ est un groupe de transformations d'un ensemble E , et a un élément quelconque de E , l'ensemble des éléments $\sigma(a)$, où σ parcourt Γ , est une partie de Γ *invariante* par Γ (voir no 5).

2) Soit F un ensemble dans lequel est donnée une loi de composition associative et commutative notée additivement. Considérons l'ensemble P des suites $(x_i)_{1 \leq i \leq n}$ d'éléments de F , c'est-à-dire l'ensemble des applications de l'intervalle $I = [1, n]$ de \mathbb{N} dans F ; si, à chaque élément (x_i) de P , on fait correspondre l'élé-

ment $\sum_{i=1}^n x_i$ de F , on définit une application de P dans F , qui est

un invariant du groupe symétrique $\mathfrak{S}_n = \mathfrak{S}_r$, comme il résulte du théorème de commutativité (§ 1, th. 3) (*).

De même, si on prend plus particulièrement pour F l'ensemble \mathbf{Z} des entiers rationnels * (ou un anneau commutatif) *, le produit

$$\prod_{1 \leq i < j \leq n} (x_j - x_i)$$
, considéré comme application de P dans \mathbf{Z} , est un invariant du groupe alterné \mathfrak{A}_n (mais non du groupe symétrique \mathfrak{S}_n).

*3) Dans l'espace euclidien réel à 3 dimensions $E = \mathbf{R}^3$, la distance $\sqrt{(x' - x)^2 + (y' - y)^2 + (z' - z)^2}$ de deux points $(x, y, z), (x', y', z')$, considérée comme application de $E \times E$ dans \mathbf{R} , est un invariant du groupe des déplacements (voir chap. IX). *

Remarque. — Étant donné un groupe de transformations Γ d'un ensemble E , et un ensemble M de l'échelle ayant pour base E (et éventuellement un certain nombre d'autres ensembles), on se gardera de confondre une partie de M invariante par Γ (élément de $\mathfrak{B}(M)$ invariant par Γ) et un ensemble d'éléments de M invariants par Γ (un tel ensemble constitue évidemment une partie invariante par Γ , mais la réciproque n'est pas vraie en général).

THÉORÈME 1. — Soient E un ensemble muni d'un groupe d'opérateurs G , A une partie non vide de E . L'ensemble des opérateurs $\alpha \in G$ qui laissent invariants tous les éléments de A , est un sous-groupe H de G .

En effet, si $\alpha x = x$ et $\beta x = x$, on a aussi $(\alpha\beta)x = \alpha(\beta x) = \alpha x = x$, et $\alpha^{-1}x = \alpha^{-1}(\alpha x) = (\alpha^{-1}\alpha)x = ex = x$ (e élément neutre de G).

Par abus de langage, on dit que le sous-groupe H ainsi déterminé est le sous-groupe de G laissant invariants les éléments de A .

Remarque. — L'ensemble des invariants de ce sous-groupe contient évidemment A , mais peut contenir des éléments de E n'appartenant pas à A .

Exemple. — *Dans l'espace euclidien, le sous-groupe du groupe des déplacements laissant invariants deux points distincts, est le groupe des rotations autour de la droite joignant ces deux points, et laisse donc invariants tous les points de cette droite.*

(*) L'expression $\sum_{i=1}^n x_i$ est un cas particulier de ce qu'on appelle les « fonctions symétriques » de x_1, x_2, \dots, x_n (cf. chap. IV et VI), qui sont toutes invariantes par le groupe \mathfrak{S}_n ; c'est cette propriété qui est à l'origine du nom de « groupe symétrique ».

Considérons en particulier une structure \mathcal{I} donnée sur un ensemble E (Ens. R, § 8) : c'est un élément d'un ensemble M de l'échelle ayant pour base E et un certain nombre d'ensembles auxiliaires.

Toute permutation f de E dont l'image dans \mathfrak{S}_E (par la représentation canonique de \mathfrak{S}_E dans \mathfrak{S}_M) laisse invariant \mathcal{I} , est, par définition (Ens. R, § 8, n° 5), un automorphisme de la structure \mathcal{I} . Donc :

PROPOSITION 2. — Les automorphismes d'une structure donnée \mathcal{I} sur un ensemble E forment un groupe de transformations de E (qu'on appelle groupe d'automorphismes de la structure \mathcal{I} , ou de l'ensemble E muni de la structure \mathcal{I}).

Soient \mathcal{I}' une structure isomorphe à \mathcal{I} , définie sur un ensemble E' , φ un isomorphisme de \mathcal{I} sur \mathcal{I}' , ψ l'isomorphisme réciproque ; il est immédiat que l'application $f \rightarrow \varphi \circ f \circ \psi$ est un isomorphisme du groupe d'automorphismes de \mathcal{I} sur celui de \mathcal{I}' .

Exemple. — Groupe d'automorphismes d'un groupe. Étant donné un groupe G , les automorphismes de G forment, d'après la prop. 2, un sous-groupe Γ du groupe symétrique \mathfrak{S}_G . Les automorphismes intérieurs α_x de G (§ 6, n° 4) forment un sous-groupe Δ de Γ ; en effet, on vérifie immédiatement l'identité $\alpha_{xy} = \alpha_x \circ \alpha_y$. Cette relation montre en outre que l'application $x \rightarrow \alpha_x$ est une représentation de G sur Δ ; pour que α_x soit l'application identique de G sur lui-même, il faut et il suffit que $xyx^{-1} = y$ quel que soit $y \in G$, c'est-à-dire $xy = yx$ quel que soit $y \in G$; autrement dit, x doit appartenir au centre Z de G ; ceci montre à nouveau, d'après le th. 3 du § 6, que Z est un sous-groupe distingué de G , et on voit de plus que le groupe Δ des automorphismes intérieurs est isomorphe au groupe quotient G/Z .

On notera que le groupe Δ peut être identique à Γ ; il peut aussi se réduire à l'application identique : il faut et il suffit pour cela que $Z = G$, donc que G soit abélien. Les automorphismes de G qui ne sont pas des automorphismes intérieurs sont parfois appelés automorphismes extérieurs de G .

Lorsque G est muni d'une structure de groupe à opérateurs, les automorphismes de cette structure forment un groupe Γ' , qui est évidemment un sous-groupe du groupe Γ des automorphismes de la structure de groupe de G ; on notera qu'en général le groupe Δ des automorphismes intérieurs n'est pas un sous-groupe de Γ' .

5. Groupes transitifs.

Soit Γ un groupe de transformations d'un ensemble E . La relation « il existe $f \in \Gamma$ telle que $y = f(x)$ » est une *relation d'équivalence* dans E ; en effet, elle est *réflexive*, car la permutation identique u appartient à Γ , et on a $x = u(x)$; elle est *symétrique*, car si $f \in \Gamma$ est telle que $y = f(x)$, son application réciproque g appartient à Γ , et $x = g(y)$; enfin, elle est *transitive*, car de $y = f(x)$, $z = g(y)$, on tire $z = g(f(x))$, et si f et g appartiennent à Γ , il en est de même de $g \circ f$.

Les *classes* suivant la relation d'équivalence précédente sont appelées *classes d'intransitivité* du groupe Γ ; si a est un élément de E , la classe d'intransitivité à laquelle il appartient est l'ensemble des $f(a)$, où f parcourt Γ . S'il n'existe qu'une seule classe d'intransitivité (identique à E), on dit que Γ est un groupe *transitif*; dans le cas contraire, Γ est dit *intransitif*. La condition pour que Γ soit transitif peut s'exprimer de la façon suivante : étant donné $a \in E$, pour tout $x \in E$, il existe $f \in \Gamma$ telle que $x = f(a)$.

Exemples. — 1) Le groupe symétrique S_n est évidemment transitif; il en est de même du groupe alterné A_n si $n > 2$, car si i, j, k sont trois entiers distincts de l'intervalle $[1, n]$, la permutation σ de cet intervalle telle que $\sigma(i) = j$, $\sigma(j) = k$, $\sigma(k) = i$ et $\sigma(h) = h$, pour h distinct de i, j, k (« permutation circulaire »), est paire comme on le vérifie aisément.

2) Le groupe des translations à gauche d'un groupe G est transitif, car si e est l'élément neutre de G , on a $\gamma_x(e) = x$; de même, le groupe des translations à droite est transitif.

3) Le groupe Δ des automorphismes intérieurs d'un groupe G (ayant plus d'un élément) est intransitif, car $\alpha_x(e) = e$ quel que soit $x \in E$; les éléments d'une même classe d'intransitivité de Δ sont appelés éléments *conjugués* dans G ; chacun des éléments du centre de G forme à lui seul une classe d'intransitivité de Δ .

4) Si Γ est un groupe de transformations intransitif d'un ensemble E , et A une classe d'intransitivité de Γ , les *restrictions* à A des permutations du groupe Γ constituent un groupe *transitif* de transformations de A .

6. Espaces homogènes.

Soit E un ensemble muni d'un groupe d'opérateurs G (n° 2); on dit que le groupe G opère *transitivement* dans E si (avec les no-

tations du n° 2) l'image de G dans S_E par la représentation $\alpha \rightarrow \alpha_x$ est un groupe *transitif* de permutations de E .

DÉFINITION 3. — On appelle espace homogène un ensemble E muni d'un groupe d'opérateurs G qui opère transitivement dans E .

Tout groupe transitif Γ de permutations d'un ensemble E définit donc sur E une structure d'espace homogène, la loi de composition externe faisant correspondre à $\sigma \in \Gamma$ et à $x \in E$ l'élément $\sigma(x)$.

Exemple. — *Tout espace euclidien est un espace homogène dont le groupe des déplacements est le groupe d'opérateurs (voir chap. IX).*

Remarque. — On peut encore dire qu'un espace homogène est un ensemble E , muni d'un groupe d'opérateurs G , et dont la loi externe satisfait à la condition suivante : quels que soient $x \in E$ et $y \in E$, il existe $\alpha \in G$ tel que $y = \alpha x$. On peut observer que cette condition, jointe à l'associativité de la loi externe par rapport à la loi du groupe G , entraîne que l'élément neutre e de G est opérateur neutre : en effet, il existe $\lambda \in G$ tel que $x = \lambda x$, donc on a $\epsilon x = \epsilon(\lambda x) = (\epsilon\lambda)x = \lambda x = x$.

Étant donné un groupe quelconque G , la *loi externe à gauche* (§ 3, n° 2) déduite de la loi du groupe, détermine sur G une structure d'espace homogène, dont G lui-même est le groupe d'opérateurs (le groupe de permutations Γ , image de G dans S_G , n'étant autre que le groupe des translations à gauche de G). Considérons alors un espace homogène E , ayant G comme groupe d'opérateurs, et soit a un élément de E , quelconque, mais choisi une fois pour toutes ; l'application $\alpha \rightarrow \alpha a$ est une *représentation* de G (muni de la structure d'espace homogène précédente) dans l'espace homogène E , et c'est une représentation sur E puisque G opère transitivement dans E . Donc (§ 4, th. 1), E est isomorphe au quotient de G (considéré comme espace homogène) par la relation d'équivalence $\alpha a = \beta a$. Or, cette relation, étant compatible à gauche avec la loi du groupe G , est de la forme $\beta \in \alpha H_a$, où H_a est le sous-groupe de G formé des $\alpha \in G$ laissant invariant a ; et le quotient de G par cette relation est l'ensemble des classes à gauche suivant H_a , muni de la loi de composition externe qui, à tout opérateur $\alpha \in G$ et à toute classe à gauche $\xi \cdot H_a$, fait correspondre la classe à gauche $\alpha \xi \cdot H_a$.

Inversement, soit H un sous-groupe quelconque de G , et désignons par G/H l'ensemble quotient de G par la relation d'équivalence (compatible à gauche avec la loi du groupe) $\beta \in \alpha H$; la loi quotient, par cette relation, de la loi externe à gauche déduite de la loi de groupe de G , définit sur G/H une structure d'espace homogène ayant G pour groupe d'opérateurs; il suffit de montrer que G opère transitivement dans G/H : or, si $u = \alpha \cdot H$ et $v = \beta \cdot H$ sont deux éléments quelconques de G/H , on a $v = (\beta \alpha^{-1})u$. L'ensemble G/H , muni de cette structure, est appelé l'espace homogène défini par le sous-groupe H du groupe G .

Si H est un sous-groupe quelconque, l'ensemble G/H ne sera muni en général d'aucune loi interne; si H est distingué, on a vu que la loi interne quotient de celle de G par H , est une loi de groupe sur G/H ; on aura soin, dans ce cas, de ne pas confondre le groupe quotient G/H défini par cette loi, et l'espace homogène G/H .

En résumant les résultats obtenus, nous arrivons au théorème suivant :

THÉORÈME 2. — Soient E un espace homogène, G le groupe des opérateurs de E . Si a est un élément quelconque de E , et si H_a désigne le sous-groupe de G formé des opérateurs α laissant invariant a , l'espace homogène E est isomorphe à l'espace homogène G/H_a défini par le sous-groupe H_a de G .

Si on considère un autre élément $b \in E$, E est aussi isomorphe à l'espace homogène G/H_b ; d'ailleurs, si $\beta \in G$ est tel que $b = \beta a$, les relations $\alpha b = b$ et $\beta^{-1} \alpha \beta a = a$ sont équivalentes, donc $H_b = \beta H_a \beta^{-1}$. L'intersection des groupes H_x , lorsque x parcourt E , n'est autre que le groupe K des opérateurs neutres de E ; on peut donc dire que K est le plus grand sous-groupe distingué de G contenu dans tous les H_x .

On en déduit la caractérisation de toutes les réalisations (n° 2) d'un groupe G comme groupe transitif de transformations (ou, comme nous dirons encore, les réalisations transitives de G):

PROPOSITION 3. — Toute réalisation transitive d'un groupe G est (à une isomorphie près) un groupe formé des permutations produites par les opérateurs d'un espace homogène G/H , où H est un

sous-groupe de G ne contenant aucun sous-groupe distingué de G autre que $\{e\}$.

Si on prend en particulier $H = \{e\}$, on obtient comme réalisation transitive de G le groupe des translations à gauche de G .

7. Groupes primitifs.

Cherchons les structures quotients d'une structure d'espace homogène; on peut, d'après le th. 2, se borner au cas d'un espace homogène G/H , défini par un sous-groupe H d'un groupe G . Si on munit G de sa structure d'espace homogène définie par la loi externe à gauche déduite de la loi de groupe, la structure de G/H est le quotient de la structure d'espace homogène de G par la relation $y \in xH$; si on désigne par R cette relation, il résulte du premier th. d'isomorphie (§ 4, th. 2) que toute relation d'équivalence sur G/H , compatible avec la structure de cet espace homogène, est de la forme S/R , où S est une relation compatible à gauche avec la loi de groupe de G , et entraînée par R ; donc (§ 6, th. 1), S est de la forme $y \in xK$, où K est un sous-groupe de G contenant H ; et le premier th. d'isomorphie montre encore que la structure quotient de G/H par la relation S/R est isomorphe à celle de l'espace homogène G/K . En résumé :

PROPOSITION 4. — Toute structure quotient d'un espace homogène G/H défini par un sous-groupe H d'un groupe G , est isomorphe à celle d'un espace homogène G/K , où K est un sous-groupe de G contenant H ; et réciproquement, tout sous-groupe K contenant H définit une structure quotient de G/H .

Considérons en particulier la structure d'espace homogène définie sur un ensemble E par un groupe transitif Γ de transformations de E ; d'après ce qui précède, si Δ désigne le sous-groupe de Γ laissant invariant un élément $a \in E$, l'espace homogène E est isomorphe à Γ/Δ , et les structures quotients de la structure de E correspondent biunivoquement aux sous-groupes Θ de Γ tels que $\Delta \subset \Theta \subset \Gamma$. Il y a toujours au moins deux tels sous-groupes, savoir Δ et Γ ; le premier correspond à E lui-même, le second à un espace homogène réduit à un seul élément; s'il n'y a pas d'autre sous-groupe Θ tel que $\Delta \subset \Theta \subset \Gamma$, on dit que Γ est un groupe

de transformations *primitif*; dans le cas contraire, Γ est dit *imprimitif*.

Dire que Γ est primitif, c'est donc dire que le sous-groupe Δ est un élément *maximal* de l'ensemble des sous-groupes de Γ distincts de Γ .

PROPOSITION 5. — Pour qu'un groupe transitif Γ de permutations d'un ensemble E soit imprimitif, il faut et il suffit qu'il existe une partie A de E , contenant plus d'un élément, distincte de E , et telle que, pour toute permutation $\sigma \in \Gamma$, on ait $\sigma(A) \subset A$ ou $A \cap \sigma(A) = \emptyset$.

Montrons d'abord que la condition est nécessaire. En effet, avec les notations précédentes, s'il existe un sous-groupe Θ distinct de Δ et Γ et tel que $\Delta \subset \Theta \subset \Gamma$, il définit dans E une relation d'équivalence R compatible avec la structure d'espace homogène de E , et les classes d'équivalence suivant R ont plus d'un élément et sont distinctes de E ; si A est une quelconque de ces classes, $\sigma(A)$ est encore une classe suivant R pour toute permutation $\sigma \in \Gamma$; la conclusion résulte de ce que ces classes forment une partition de E .

Pour voir que la condition est suffisante, remarquons d'abord qu'elle entraîne que, pour toute permutation $\sigma \in \Gamma$ telle que $\sigma(A) \subset A$, on a $\sigma(A) = A$; en effet on tire $A \subset \sigma^{-1}(A)$, donc $A \cap \sigma^{-1}(A) \neq \emptyset$, et par suite $\sigma^{-1}(A) \subset A$, d'où $A = \sigma^{-1}(A) = \sigma(A)$. On en conclut aussitôt (th. 1) que l'ensemble Θ des permutations $\sigma \in \Gamma$ telles que $\sigma(A) \subset A$ (ou, ce qui revient au même d'après l'hypothèse, $A \cap \sigma(A) \neq \emptyset$) est un sous-groupe de Γ . Ce sous-groupe est distinct de Γ , puisque $A \neq E$ par hypothèse, et que Γ est transitif; il est distinct de Δ , car A contient au moins un élément $b \neq a$, et si τ est une permutation de Γ telle que $\tau(a) = b$, on a $\tau \notin \Delta$, et $\tau(A) \cap A \neq \emptyset$, donc $\tau \in \Theta$; par suite, Γ est imprimitif.

Les classes d'équivalence suivant la relation R qui correspond au sous-groupe Θ sont appelées *classes d'imprimitivité* de Γ correspondant à ce sous-groupe: ce sont les éléments de l'espace homogène quotient de E par la relation R (isomorphe à Γ/Θ).

Exercices. — 1) Dans un groupe fini G , montrer que le nombre des conjugués (n° 4) d'un élément $a \in G$ est égal à l'indice du normalisateur (§ 6, exerc. 13) de a , et est par suite un diviseur de l'ordre de G .

¶ 2) Si G est un groupe fini d'ordre n , le nombre des automor-

phismes de G est $\leq n^{\frac{\log n}{\log 2}}$ (montrer qu'il existe un système de générateurs $\{a_1, a_2, \dots, a_m\}$ de G tel que a_i n'appartienne pas au sous-groupe engendré par a_1, a_2, \dots, a_{i-1} pour $2 \leq i \leq m$; en déduire que $2^m \leq n$, et que le nombre des automorphismes de G est $\leq n^m$).

3) Soit Γ le groupe des automorphismes d'un groupe G , Δ le groupe des automorphismes intérieurs de G ; montrer que Δ est sous-groupe distingué de Γ . Pour qu'un automorphisme σ de G soit permutable avec tous les automorphismes intérieurs de G , il faut et il suffit que, pour tout $x \in G$, $x^{-1}\sigma(x)$ appartienne au centre de G ; en déduire que, si le centre de G est réduit à l'élément neutre, il est de même du centralisateur (§ 6, exerc. 13) de Δ dans Γ .

¶ 4) a) Soit G un groupe simple non abélien, Γ le groupe des automorphismes de G , Δ le groupe des automorphismes intérieurs de G (isomorphe à G). Si s est un automorphisme du groupe Γ , montrer que $s(\Delta) = \Delta$ (en utilisant l'exerc. 3 ci-dessus, et la prop. 7 du § 6, remarquer que l'intersection $\Delta \cap s(\Delta)$ ne peut se réduire à l'élément neutre de Γ .)

b) Montrer que le seul automorphisme de Γ laissant invariant chacun des éléments de Δ est l'automorphisme identique (écrire que cet automorphisme laisse invariant α et $\alpha\sigma\alpha^{-1}$, quels que soient $\alpha \in \Delta$ et $\sigma \in \Gamma$, et utiliser l'exerc. 3).

c) Soient s un automorphisme de Γ , φ l'isomorphisme $x \rightarrow \alpha_x$ de G sur Δ , ψ l'isomorphisme réciproque, σ l'automorphisme $\psi \circ s \circ \varphi$ de G ; montrer que l'automorphisme $\xi \rightarrow \sigma^{-1}s(\xi)\sigma$ de Γ est l'automorphisme identique (utiliser b) en remarquant que, pour tout $x \in G$, on a $s(\alpha_x) = \alpha_{\sigma(x)}$. En déduire que tout automorphisme de Γ est un automorphisme intérieur.

¶ 5) a) Soit G un groupe, Σ le groupe de ses automorphismes, Γ le groupe des translations à gauche de G (isomorphe à G). Montrer que, dans le groupe symétrique \mathfrak{S}_G , l'intersection $\Sigma \cap \Gamma$ se réduit à l'élément neutre et que $\Sigma\Gamma = \Gamma\Sigma$. En déduire que $\Omega = \Gamma\Sigma$ est un sous-groupe de \mathfrak{S}_G , qu'on appelle l'*holomorphie* du groupe G (cf. § 6, exerc. 3).

b) Montrer que Γ est sous-groupe distingué de Ω , et que tout automorphisme de Γ est de la forme $\gamma \rightarrow \sigma\gamma\sigma^{-1}$, où $\sigma \in \Sigma$.

c) Le groupe Δ des translations à droite de G est sous-groupe distingué de Ω , et l'intersection $\Gamma \cap \Delta$ est le centre de chacun des deux groupes Γ , Δ .

d) Montrer que Ω est le normalisateur (§ 6, exerc. 13) de Γ dans \mathfrak{S}_G (soit τ un élément du normalisateur de Γ dans \mathfrak{S}_G ; si on pose $\tau\gamma_x\tau^{-1} = \gamma_{\sigma(x)}$, prouver que $\sigma(x) = \tau(xu)$, où $u = \tau^{-1}(e)$, puis montrer que σ est un automorphisme de G , et utiliser c)).

e) Montrer que Δ est le centralisateur (§ 6, exerc. 13) de Γ dans \mathfrak{S}_n .

6) a) Soit (E_i) une partition d'un ensemble E , Γ l'ensemble des permutations σ de E telles que $\sigma(E_i) \subset E_i$ pour tout indice i . Montrer que Γ est un sous-groupe de \mathfrak{S}_E ; si on désigne par Γ_i le sous-groupe de Γ formé des permutations σ telles que $\sigma(E_i) = E_i$, $\sigma(x) = x$ pour tout $x \in E_i$, montrer que Γ_i est isomorphe à \mathfrak{S}_{E_i}

et que Γ est isomorphe au produit $\prod_i \Gamma_i$.

b) Soit σ une permutation quelconque de E , (E_i) la partition de E formée des classes d'intransitivité du sous-groupe monogène de \mathfrak{S}_E engendré par σ . Le composant σ_i de σ dans le groupe Γ_i correspondant à E_i engendre dans ce groupe un groupe monogène, transitif dans E_i ; on dit que cette permutation est une *permutation circulaire* ou un *cycle*, et que les σ_i sont les *cycles composants* de la permutation σ . Lorsque le nombre des cycles composants de σ , non réduits à la permutation identique, est fini, σ est égal à leur produit (dans un ordre quelconque, les cycles composants de σ étant deux à deux permutable). Lorsqu'un E_i a un nombre fini d'éléments, on peut ranger ces éléments en une suite finie $(a_i)_{1 \leq i \leq n}$, telle que $a_{i+1} = \sigma(a_i)$ pour $1 \leq i \leq n-1$, et $a_1 = \sigma(a_n)$; le cycle correspondant de σ se note alors $(a_1 \ a_2 \ \dots \ a_n)$, et on dit qu'il est de longueur n . Si τ est une permutation quelconque de \mathfrak{S}_E , on a

$$(1) \quad \tau \cdot (a_1 \ a_2 \ \dots \ a_n) \cdot \tau^{-1} = (\tau(a_1) \ \tau(a_2) \ \dots \ \tau(a_n)).$$

¶ 7) a) Montrer que toute permutation de \mathfrak{S}_n est un produit de transpositions (raisonner par récurrence sur le nombre d'éléments non invariants par la permutation considérée).

b) En déduire que \mathfrak{S}_n est engendré par les $n-1$ transpositions $(1 \ 2)$, $(1 \ 3)$, ..., $(1 \ n)$, et aussi par les $n-1$ transpositions $(1 \ 2)$, $(2 \ 3)$, ..., $(n-1 \ n)$ (utiliser la formule (1) de l'exerc. 6).

c) En déduire que \mathfrak{S}_n est engendré par les deux permutations $(1 \ 2)$ et $(1 \ 2 \ 3 \ \dots \ n)$ (même méthode).

¶ 8) a) Montrer que toute permutation σ de \mathfrak{A}_n est un produit de cycles de longueur 3 (qui ne sont pas en général les cycles composants de σ) (le démontrer pour un produit de deux transpositions et utiliser l'exerc. 7 a)).

b) En déduire que \mathfrak{A}_n est engendré par les $n-2$ permutations $(1 \ 2 \ 3)$, $(1 \ 2 \ 4)$, ..., $(1 \ 2 \ n)$ (utiliser la formule (1) de l'exerc. 6).

c) En déduire que, si n est impair, \mathfrak{A}_n est engendré par les deux permutations $(1 \ 2 \ 3)$ et $(1 \ 2 \ \dots \ n)$, et si n est pair, par les deux permutations $(1 \ 2 \ 3)$ et $(2 \ 3 \ \dots \ n)$.

d) Montrer que, si un sous-groupe distingué de \mathfrak{A}_n contient un

cycle de longueur 3, il est identique à \mathfrak{A}_n (prouver, à l'aide de la formule (1) de l'exerc. 6, que le sous-groupe contient tous les cycles $(1 \ 2 \ k)$ pour $3 \leq k \leq n$).

9) On dit qu'un groupe de permutations Γ d'un ensemble E est *r fois transitif* si, quelles que soient les deux suites (a_1, a_2, \dots, a_r) , (b_1, b_2, \dots, b_r) de r éléments distincts de E , il existe une permutation $\gamma \in \Gamma$ telle que $\gamma(a_i) = b_i$ pour $1 \leq i \leq r$, cette propriété n'ayant plus lieu pour un couple au moins de suites de $r+1$ éléments distincts de E .

a) Montrer qu'un groupe r fois transitif est primitif si $r > 1$ (appliquer la prop. 4).

b) L'ordre d'un groupe de permutations Γ , r fois transitif et de degré n , est de la forme $n(n-1)\dots(n-r+1)d$, où d est un diviseur de $(n-r)!$ (considérer le sous-groupe des permutations de Γ laissant invariants r éléments, et calculer son indice).

¶ 10) Soit Γ un groupe de permutations r fois transitif d'un ensemble E de n éléments; pour une permutation $\sigma \in \Gamma$, distincte de la permutation identique, soit $n-s$ le nombre d'éléments de E invariants par σ . Si $s > r$, montrer qu'il existe une permutation $\tau \in \Gamma$ telle que $\sigma^{-1}\tau\sigma^{-1}$ soit distincte de la permutation identique, et que le nombre d'éléments de E qu'elle laisse invariants soit $\geq n-2(s-r+1)$ (utiliser la décomposition de σ en ses cycles composants (exerc. 6) et la formule (1) de l'exerc. 6). Si $s = r$, montrer de même qu'il existe $\tau \in \Gamma$ telle que $\sigma^{-1}\tau\sigma^{-1}$ soit un cycle de longueur 3. En déduire que, si $r \geq 3$, et si Γ ne contient pas le groupe alterné \mathfrak{A}_n , on a $s \geq 2r-2$ pour toute permutation de Γ (utiliser l'exerc. 8). Conclure finalement que, si Γ n'est pas identique à \mathfrak{A}_n ou à \mathfrak{S}_n , on a $r \leq \frac{n}{3} + 1$.

¶ 11) a) Montrer que le groupe alterné \mathfrak{A}_n est $n-2$ fois transitif.

b) Montrer que \mathfrak{A}_n est un groupe simple pour $n \neq 4$ (en utilisant a), la méthode de l'exerc. 10, et l'exerc. 8d), montrer que \mathfrak{A}_n est simple pour $n > 6$; examiner de manière analogue les cas où $n \leq 6$.

12) Soit Γ un groupe transitif de permutations d'un ensemble E ; si Δ est sous-groupe distingué de Γ , montrer que toute classe d'intransitivité de Δ est une classe d'imprimitivité de Γ (utiliser la prop. 5). En déduire que, si Γ est primitif, Δ est transitif.

13) Soit Γ un groupe intransitif de permutations d'un ensemble E . Si A est une classe d'intransitivité de Γ , $B = \mathbb{C}A$ son complémentaire, on désigne par Γ_A et Γ_B les groupes formés des restrictions des permutations de Γ à A et B respectivement, par Δ_A et Δ_B les sous-groupes de Γ qui laissent invariants respectivement tout élément de A et tout élément de B . Montrer que Δ_A et

Δ_B sont des sous-groupes distingués de Γ , et que Γ_A est isomorphe à Γ/Δ_A et Γ_B à Γ/Δ_B ; si Δ_{AB} (resp. Δ_{BA}) est le groupe formé des restrictions des permutations de Δ_A (resp. Δ_B) à B (resp. A), montrer que les groupes quotients Γ_A/Δ_{BA} , Γ_B/Δ_{AB} et $\Gamma/(\Delta_A\Delta_B)$ sont isomorphes (appliquer le th. 6 du § 6 à la représentation $\sigma \rightarrow \sigma_A$ qui, à toute permutation $\sigma \in \Gamma$, fait correspondre sa restriction à A).

¶ 14) a) Soit Γ un groupe de permutations d'un ensemble E de m éléments ; montrer que, si Δ_a est le sous-groupe de Γ laissant invariant un élément $a \in E$, l'indice $(\Gamma : \Delta_a)$ est égal au nombre d'éléments de la classe d'intransitivité de Γ à laquelle appartient a .

b) Soit v_k le nombre de permutations de Γ laissant invariants k éléments de E ; si n est l'ordre de Γ , t le nombre de ses classes d'intransitivité, démontrer la formule

$$(2) \quad nt = \sum_{k=0}^m k \cdot v_k.$$

(si $p(\sigma)$ est le nombre d'éléments invariants par une permutation $\sigma \in \Gamma$, évaluer de deux manières différentes le nombre $\sum_{\sigma \in \Gamma} p(\sigma)$, et utiliser a)).

c) Montrer que, si le nombre $p(\sigma) = k$ est le même pour toutes les permutations de Γ autres que la permutation identique, et si l'ordre de Δ_a est > 1 pour tout a , on a $k \leq t < 2k$ (remarquer que $m \leq kn$). Dans le cas particulier où $k = 2$, trouver les ordres possibles des sous-groupes Δ_a correspondant aux classes d'intransitivité de Γ ; montrer que, si $t = 3$, l'ordre du sous-groupe Δ_a ne peut être > 2 pour les éléments de deux des trois classes d'intransitivité que si n a l'une des valeurs 12, 24 ou 60.

15) Soit E un ensemble muni d'une loi de composition externe $(\alpha, x) \rightarrow \alpha x$, dont le domaine d'opérateurs est un groupe G , et qui est associative (§ 5, n° 2) par rapport à la loi de groupe de G . Si e est l'élément neutre de G , montrer que l'ensemble $A = eE$ est stable pour la loi externe considérée, et que, pour la loi induite sur A , A est un ensemble muni du groupe d'opérateurs G , au sens du n° 2. Si Γ est le groupe des permutations de A produites par les opérateurs de G , chacune des classes d'intransitivité de Γ est une partie stable de A , et la structure induite sur une quelconque de ces classes est une structure d'espace homogène.

¶ 16) Soit G un groupe, H un sous-groupe de G . On suppose donnée une application biunivoque r de l'ensemble G/H des classes à gauche (mod. H) dans G , qui, à tout $X \in G/H$ fasse correspondre un élément $r(X) \in X \subset G$; on a donc $X = r(X).H$. On définit sur G/H une loi de composition interne τ en posant $X \tau Y = r(X)r(Y).H$; montrer que l'on a $X \tau H = X$ quel que

soit X , et que, pour la loi τ , toute translation à gauche est une application biunivoque de G/H sur lui-même. Si G' est le sous-groupe de G engendré par l'ensemble des éléments $r(X)$, et $H' = H \cap G'$, la loi interne définie d'une manière analogue sur G'/H' par l'application r , détermine sur cet ensemble une structure isomorphe à celle déterminée sur G/H par la loi τ .

b) Pour que la loi τ soit associative, il faut et il suffit que H' soit un sous-groupe distingué de G' , auquel cas la structure déterminée par τ est isomorphe à la structure du groupe quotient G'/H' (pour voir que la condition est suffisante, montrer d'abord, à l'aide de l'exerc. 2a) du § 6, que si τ est associative, elle détermine sur G/H une structure de groupe ; désignant par K le plus grand sous-groupe distingué de G' contenu dans H' , montrer ensuite en écrivant la condition d'associativité pour τ , que $(r(X \tau Y))^{-1}r(X)r(Y) \in K$ quels que soient X, Y ; en déduire que l'application $X \rightarrow r(X).K$ est un isomorphisme du groupe G/H (pour la loi τ) sur le groupe quotient G'/K ; conclure que $H' = K$, en remarquant que H' est une réunion de classes mod. K).

c) Inversement, on suppose donnée sur un ensemble E , une loi interne τ partout définie, telle que toute translation à gauche soit une application biunivoque de E sur lui-même, et qu'il existe $e \in E$ tel que $x \tau e = x$ pour tout $x \in E$. Soit Γ le groupe de permutations de E engendré par les translations à gauche γ_x , Δ le sous-groupe des permutations de Γ laissant invariant e ; montrer qu'à toute classe à gauche X modulo Δ , il correspond un élément et un seul $x \in E$ tel que $\gamma_x \in X$; si on pose $r(X) = \gamma_x$, l'application $x \rightarrow \gamma_x$ est un isomorphisme de l'ensemble E , muni de la loi τ , sur l'ensemble Γ/Δ , muni de la loi $(X, Y) \rightarrow r(X)r(Y).\Delta$.

§ 8. — Anneaux et anneaux à opérateurs.

1. Anneaux.

DÉFINITION 1. — Sur un ensemble A , on appelle structure d'anneau une structure algébrique déterminée par deux lois de composition internes partout définies, dont la première est une loi de groupe abélien sur A , et dont la seconde est associative et doublement distributive par rapport à la première. Un ensemble muni d'une structure d'anneau prend le nom d'anneau.

Le plus souvent, on note additivement la loi de groupe abélien d'un anneau A , multiplicativement sa seconde loi de composition

interne. Les hypothèses sur l'addition dans A s'expriment alors par les identités

$$(1) \quad x + (y + z) = (x + y) + z \quad (\text{associativité})$$

$$(2) \quad x + y = y + x \quad (\text{commutativité})$$

par l'existence d'un élément neutre noté 0, tel qu'on ait identiquement

$$(3) \quad x + 0 = x$$

enfin par l'existence, pour tout x , d'un élément *opposé* à x , noté $-x$, tel que

$$(4) \quad x + (-x) = 0.$$

Les hypothèses sur la multiplication s'expriment de même par les identités

$$(5) \quad x(yz) = (xy)z \quad (\text{associativité})$$

$$(6) \quad \begin{cases} x(y+z) = xy + xz \\ (y+z)x = yx + zx \end{cases} \quad (\text{double distributivité}).$$

Si la multiplication dans un anneau A possède un élément neutre, cet élément est appelé *élément unité* de A, et se note souvent 1 (si aucune confusion n'est à craindre). De même, lorsqu'on parle d'éléments *réguliers*, d'éléments *inversibles*, d'éléments *permutables*, d'éléments *centraux* ou du *centre* d'un anneau A, toutes ces notions sont relatives à la multiplication dans A.

Lorsqu'on remplace la multiplication, dans un anneau A, par la loi *opposée*, cette loi et l'addition déterminent encore sur A une structure d'anneau, qui est dite opposée à la première ; deux anneaux, dont les structures sont opposées, sont dits *opposés*.

On dit qu'un anneau est *commutatif* si sa multiplication est commutative ; il est identique à son opposé.

Sur un anneau A, l'addition, et les deux lois externes déduites par *dédoubllement* (§ 3, n° 2) de la multiplication, déterminent une structure de *groupe abélien à opérateurs*, A lui-même étant le domaine d'opérateurs pour chacune des deux lois externes ; pour tout $a \in A$, on appelle *homothétie à gauche* (resp. *homothétie à droite*) de l'anneau A, correspondant à a , l'endomorphisme $x \rightarrow ax$ (resp. $x \rightarrow xa$) du groupe additif de A.

Exemples d'anneaux. I. *Anneau des entiers rationnels.* — Nous avons défini, sur l'ensemble \mathbb{Z} des entiers rationnels, l'addition

(§ 2, n° 5) et la multiplication (§ 2, n° 8) ; l'addition est une loi de groupe abélien, et la multiplication est doublement distributive par rapport à l'addition ; donc \mathbb{Z} , muni de ces deux lois, est un anneau qu'on appelle *l'anneau des entiers rationnels*. Il est évidemment commutatif, et admet +1 comme élément unité.

II. * Les *polynomes* d'une variable réelle, à coefficients réels (ou à coefficients entiers) forment un anneau commutatif, ayant pour élément unité la constante 1 (cf. chap. IV). Plus généralement, les fonctions réelles d'une variable réelle forment un anneau commutatif, ayant la constante 1 comme élément unité.*

III. Sur un groupe abélien quelconque G (noté additivement) on peut définir une structure d'anneau commutatif en prenant pour multiplication la loi $(x, y) \rightarrow 0$ qui est associative, commutative, et distributive par rapport à l'addition. On peut encore dire que cette multiplication est définie par la condition $G \cdot G = \{0\}$; les anneaux satisfaisant à cette condition sont dits *de carré nul* ; un tel anneau n'admet évidemment pas d'élément unité, s'il n'est pas réduit à l'élément 0.

IV. *Anneau des endomorphismes d'un groupe abélien.* — Soit G un groupe abélien, noté additivement. L'ensemble G^G des applications de G dans lui-même est muni de deux lois de composition associatives : d'une part, la loi $(f, g) \rightarrow f + g$ (rappelons que $h = f + g$ est l'application de G dans G telle que $h(x) = f(x) + g(x)$ pour tout $x \in G$), qui définit sur G^G une structure de *groupe abélien* (§ 6, n° 5) ; d'autre part, la loi $(f, g) \rightarrow f \circ g$, que nous noterons ici $f \cdot g$. L'ensemble E des *endomorphismes* du groupe G est un sous-groupe du groupe abélien G^G : en effet, si f et g sont deux endomorphismes, et $h = f - g$, on a $h(x+y) = f(x+y) - g(x+y) = f(x) + f(y) - (g(x) + g(y)) = (f(x) - g(x)) + (f(y) - g(y)) = h(x) + h(y)$, donc h est un endomorphisme. En outre E est évidemment stable pour la loi $(f, g) \rightarrow f \cdot g$; enfin, cette dernière loi induit sur E une loi *doublement distributive* par rapport à la loi $(f, g) \rightarrow f + g$: en effet, si $\varphi = (g+h) \cdot f$, on a $\varphi(x) = g(f(x)) + h(f(x))$, donc $\varphi = g \cdot f + h \cdot f$; d'autre part, si $\psi = f \cdot (g+h)$, on a $\psi(x) = f(g(x) + h(x)) = f(g(x)) + f(h(x))$ (puisque f est un endomorphisme) donc $\psi = f \cdot g + f \cdot h$.

La structure induite sur E par les deux lois considérées est donc une structure d'anneau ; E, muni de cette structure, est appelé *l'anneau des endomorphismes* du groupe G. L'anneau des endo-

morphismes d'un groupe abélien G admet toujours un élément unité, savoir l'application identique de G sur lui-même ; mais il n'est pas commutatif en général (voir exerc. 2).

Les anneaux définis de cette manière jouent un rôle considérable en Algèbre (cf. chap. II et VII).

On notera que l'anneau des endomorphismes du groupe abélien \mathbb{Z} est isomorphe à l'anneau \mathbb{Z} des entiers rationnels (§ 2, no 8).

2. Anneaux à opérateurs.

DÉFINITION 2. — *On appelle anneau à opérateurs un ensemble A muni d'une structure d'anneau, et d'une ou plusieurs lois de composition externes, distributives par rapport à l'addition dans A , et telles que, si on note $(\alpha, x) \rightarrow \alpha x$ une quelconque de ces lois, on ait identiquement*

$$(7) \quad \alpha(xy) = (\alpha x)y = x(\alpha y).$$

Les lois de composition externes d'un anneau à opérateurs A , et les deux lois externes déduites par dédoublement de la multiplication dans A , déterminent (avec l'addition comme loi interne) une structure de *groupe abélien à opérateurs* sur A ; la condition (7) exprime que les lois externes de l'anneau A sont *permutables* (§ 5, no 3) avec chacune des deux lois externes déduites par dédoublement de la multiplication.

Les endomorphismes $x \rightarrow \alpha x$ de la structure de *groupe additif* (sans opérateurs) de A , produits par les opérateurs de l'anneau A , sont souvent appelés *homothéties externes* de l'anneau à opérateurs A ; ils sont donc permutable (dans l'anneau des endomorphismes du groupe additif A) avec les homothéties à droite et à gauche de A ; on peut encore dire que ce sont des endomorphismes de la structure de *groupe à opérateurs* de A , déterminée par l'addition et les deux lois externes déduites par dédoublement de la multiplication.

Exemple. — Si A est un anneau, K une partie du *centre* de A , la loi $(a, x) \rightarrow ax$ entre opérateurs $a \in K$ et éléments $x \in A$ détermine (avec la structure d'anneau de A) une structure d'anneau à opérateurs sur A ; les propriétés de cette structure dépendent essentiellement de la partie K qu'on considère et il faudra soigneusement distinguer les diverses structures d'anneau à opérateurs qu'on peut être amené à définir de cette manière (cf. chap. II et VII).

Lorsque, dans un anneau à opérateurs A , on remplace la multiplication par la loi *opposée*, il résulte de (7) que cette loi, l'ad-

N

dition et les lois externes de A définissent encore une structure d'anneau à opérateurs, dite opposée à la première ; l'anneau à opérateurs obtenu en munissant A de cette structure est dit *opposé* à A .

Conformément aux notations générales (§ 2, no 7), dans un anneau quelconque A , on notera d'ordinaire $n \cdot x$ ou nx , pour $n \in \mathbb{Z}$ et $x \in A$, la somme d'une suite de n termes égaux à x si $n > 0$, l'élément 0 si $n = 0$, et l'élément $-((--n) \cdot x)$ si $n < 0$. On définit ainsi entre entiers rationnels et éléments de A une loi externe (qu'on aura soin de ne pas confondre avec la multiplication dans A) ; cette loi est distributive par rapport à l'addition et satisfait aux identités (7) en vertu de la double distributivité de la multiplication dans A par rapport à l'addition ; elle détermine donc, avec l'addition et la multiplication dans A , une structure d'*anneau à opérateurs* sur A . Mais il n'y aura pas lieu de distinguer cette structure de la structure d'anneau donnée sur A , car les notions essentielles relatives aux structures algébriques, définies au § 4 (parties stables, relations d'équivalence compatibles avec une structure, homomorphismes) sont *identiques* pour ces deux structures.

Plus généralement, si A est un anneau à opérateurs, on ne distinguera pas sa structure de celle qu'on obtient en adjoignant la loi externe $(n, x) \rightarrow n \cdot x$ aux lois externes déjà impliquées par la structure de A .

Cette remarque permet donc de considérer les anneaux sans opérateurs comme cas particuliers des anneaux à opérateurs ; aussi, dans toute la suite de ce paragraphe, n'étudierons-nous que ces derniers. Lorsqu'aucune confusion ne sera possible, nous employerons le terme d' « anneau » au sens d' « anneau à opérateurs », par abus de langage ; lorsqu'un résultat ne sera valable que pour les anneaux *sans opérateurs* (ou, ce qui revient au même, les anneaux à opérateurs dont $(n, x) \rightarrow n \cdot x$ est la seule loi externe) on le spécifiera explicitement.

3. Diviseurs de zéro. Anneaux d'intégrité.

Soit A un anneau. Généralisant la terminologie utilisée pour les entiers naturels (*Ens.*, chap. III), on dira qu'un élément $a \in A$ est *multiple à gauche* (resp. *multiple à droite*) d'un élément $b \in A$

s'il existe $c \in A$ tel que $a = cb$ (resp. $a = bc$) ; on dit aussi alors que b est *diviseur à droite* (resp. *diviseur à gauche*) de a .

Si A est commutatif, on parlera simplement de « *multiple* » et de « *diviseur* », puisque l'ordre des facteurs est indifférent.

2

On observera que, si A n'a pas d'élément unité, un élément $a \in A$ n'est pas nécessairement diviseur (à droite ou à gauche) de lui-même ; c'est ce que montre l'exemple d'un anneau de carré nul (exemple III). De même, pour $n \in \mathbf{Z}$, $n.x$ ne sera pas en général multiple de x si A n'a pas d'élément unité. Au contraire, si A possède un élément unité e , on peut écrire $n.x = n.ex = (n.e)x = x(n.e)$.

Pour tout élément x d'un anneau A , on a $x^2 = x(x+0) = x^2 + x0$ d'où $x0 = 0$; de même $0x = 0$: tout multiple (à gauche ou à droite) de 0 est égal à 0. Par suite, quels que soient x, y , on a $(-x)y = x(-y) = -xy$, car $(-x)y + xy = (-x + x)y = 0y = 0$; on en conclut que $(-x)(-y) = xy$. Par récurrence sur l'entier $n > 0$, on voit que $(-x)^n = x^n$ si n est pair, et $(-x)^n = -x^n$ si n est impair.

La relation $x0 = 0$ montre aussi que si un anneau A n'est pas réduit à 0 et possède un élément unité e , on a $e \neq 0$.

Conformément à la terminologie introduite ci-dessus, tout élément $x \in A$ devrait être considéré comme un diviseur (à droite et à gauche) de 0 ; mais, par abus de langage, on réserve le nom de *diviseur à gauche de 0* (resp. *diviseur à droite de 0*) à tout élément a différent de 0 tel qu'il existe b différent de 0 satisfaisant à la relation $ab = 0$ (resp. $ba = 0$). On peut encore dire que les diviseurs à gauche et les diviseurs à droite de 0, ainsi que 0 lui-même, sont les éléments *non réguliers* (§ 2, n° 2) de A (lorsque A n'est pas réduit au seul élément 0) ; en effet, si un élément $a \neq 0$ n'est pas régulier, il existe deux éléments distincts x, y tels que $ax = ay$ ou $xa = ya$, c'est-à-dire $a(x-y) = 0$ ou $(x-y)a = 0$, avec $x-y \neq 0$; la réciproque est évidente.

Dans un anneau sans diviseur de 0, la relation $ab = 0$ est équivalente à « $a = 0$ ou $b = 0$ » ; on en déduit, par récurrence sur l'entier $n > 0$, que la relation $a^n = 0$ est équivalente à $a = 0$.

DÉFINITION 3. — *On appelle anneau d'intégrité un anneau non réduit à 0, commutatif et sans diviseur de zéro.*

Exemples. — 1) L'anneau \mathbf{Z} des entiers rationnels est un anneau d'intégrité ; par contre, l'anneau des endomorphismes d'un groupe abélien quelconque aura en général des diviseurs de 0 (voir exerc. 2).

2) Dans un anneau de carré nul (exemple III), tout élément $\neq 0$ est diviseur de 0.

4. Sous-anneaux.

DÉFINITION 4. — *On appelle sous-anneau d'un anneau (à opérateurs) A une partie non vide B de A , telle que la structure induite sur B par celle de A soit une structure d'anneau à opérateurs.*

PROPOSITION 1. — *Pour qu'une partie non vide B d'un anneau A soit un sous-anneau de A , il faut et il suffit que B soit un sous-groupe du groupe additif de A , et soit stable pour la multiplication et les lois externes de A .*

La démonstration est immédiate à partir des définitions.

Les conditions pour qu'une partie non vide B de A soit un sous-anneau s'écrivent encore (§ 6, prop. 1) : $B + B \subset B$, $-B \subset B$, $BB \subset B$ et $\alpha B \subset B$ pour tout opérateur α de A . Les trois premières de ces conditions sont nécessaires et suffisantes pour que la structure d'anneau (sans opérateurs) de A induise sur B une structure d'anneau, autrement dit, pour que B soit sous-anneau de A considéré comme anneau sans opérateurs (c'est-à-dire muni de sa structure d'anneau, mais non de ses lois externes).

Exemples. — 1) Tout sous-groupe du groupe additif \mathbf{Z} , étant de la forme $n.\mathbf{Z}$, avec $n \in \mathbf{N}$, est un sous-anneau de \mathbf{Z} ; il y a donc identité entre les sous-anneaux de l'anneau \mathbf{Z} et les sous-groupes de son groupe additif. Aucun de ces sous-anneaux, autres que \mathbf{Z} lui-même et $\{0\}$, n'a d'élément unité.

* 2) Sur le corps des nombres complexes \mathbf{C} , considérons la structure d'anneau à opérateurs défini par la loi externe $(\alpha, z) \rightarrow \alpha z$ entre opérateurs réels α et nombres complexes z (cf. n° 2). Pour cette structure, le seul sous-anneau de \mathbf{C} distinct de $\{0\}$ et \mathbf{C} est l'ensemble des nombres réels \mathbf{R} . En effet, si un sous-anneau A de \mathbf{C} contient un nombre non réel z , il contient aussi z^2 , donc tous les nombres complexes $\alpha z + \beta z^2$, où α et β prennent toutes les valeurs réelles ; mais comme le rapport z^2/z n'est pas réel, l'ensemble ainsi obtenu est identique à \mathbf{C} . L'ensemble \mathbf{Z} des entiers rationnels n'est donc pas un sous-anneau de l'anneau à opérateurs \mathbf{C} , bien qu'il soit un sous-anneau de \mathbf{C} considéré comme anneau sans opérateurs. *

2

Remarque. — Ce dernier exemple prouve que la notion de sous-anneau d'un anneau à opérateurs A, dépend essentiellement des lois externes données dans la structure de A, et non seulement de sa structure d'anneau. Un sous-anneau de A reste évidemment sous-anneau lorsqu'on restreint les lois externes de A à des parties des domaines d'opérateurs donnés, ou qu'on ne considère que certaines de ces lois externes, et non les autres ; mais la réciproque est inexacte. Toutefois, la présence ou l'absence de la loi externe $(n, x) \rightarrow n \cdot x$ ($n \in \mathbf{Z}$), dans la structure d'anneau à opérateurs donnée, ne modifie en rien la notion de sous-anneau relative à cette structure : cela est dû au fait que tout sous-groupe du groupe additif de A est stable pour cette loi.

Lorsqu'il y aura lieu de considérer, sur un ensemble A, plusieurs structures d'anneaux à opérateurs ayant même structure d'anneau sous-jacente, on distinguera les sous-anneaux relatifs à ces diverses structures en précisant pour quelles lois externes ils sont stables.

Toute intersection de sous-anneaux de A est encore un sous-anneau ; on peut donc définir le sous-anneau engendré par une partie quelconque X de A comme le plus petit sous-anneau contenant X.

PROPOSITION 2. — *Dans un anneau A, l'ensemble des éléments permutable avec tous les éléments d'une partie quelconque M de A, est un sous-anneau de A.*

En effet, cet ensemble est stable pour la multiplication (§ 1, prop. 1) ; il est stable pour chacune des lois externes de A, car si x est permutable avec $z \in M$, on a, pour tout opérateur α de A, $(\alpha x)z = \alpha(xz) = \alpha(zx) = z(\alpha x)$ d'après (7). Enfin, si x et y sont permutable avec $z \in M$, il en est de même de $x - y$, car

$$(x - y)z = xz - yz = zx - zy = z(x - y).$$

COROLLAIRE 1. — *Le centre d'un anneau A est un sous-anneau de A.*

COROLLAIRE 2. — *L'ensemble des endomorphismes d'un groupe abélien à opérateurs G est un sous-anneau de l'anneau des endomorphismes E du groupe G.*

En effet, ces endomorphismes sont identiques aux endomorphismes de la structure de groupe de G qui sont permutable avec les homothéties de G. Le sous-anneau de E qu'ils forment est appelé l'anneau des endomorphismes du groupe à opérateurs G.

5. Relations d'équivalence dans un anneau. Idéaux. Anneaux quotients.

Cherchons les relations d'équivalence compatibles avec la structure d'un anneau A. D'après le th. 4 du § 6, une relation R, compatible avec l'addition et avec les lois externes de A, est de la forme $x - y \in H$, où H est un sous-groupe du groupe additif de A, stable pour les lois externes de A. Pour exprimer que R est compatible avec la multiplication, on exprime séparément qu'elle est compatible à gauche et compatible à droite (§ 4, prop. 1). Or, la compatibilité à gauche signifie que $x \equiv y$ (mod. R) entraîne $zx \equiv zy$ (mod. R), c'est-à-dire que $x - y \in H$ entraîne $zx - zy = z(x - y) \in H$ quel que soit $z \in A$. On est donc conduit à poser la définition suivante :

DÉFINITION 5. — *On appelle idéal à gauche (resp. idéal à droite) d'un anneau A, tout sous-groupe H du groupe additif de A, stable pour les lois externes de A, et tel que $zH \subset H$ (resp. $Hz \subset H$) pour tout $z \in A$. Une partie de A qui est à la fois idéal à gauche et idéal à droite de A est appelée idéal bilatère de A.*

Les conditions pour qu'une partie non vide H d'un anneau A soit un idéal à gauche (resp. à droite) de A s'écrivent donc $H + H \subset H$, $-H \subset H$, $A \cdot H \subset H$ (resp. $H \cdot A \subset H$), et $\alpha H \subset H$ pour tout opérateur α de A. Tout idéal est évidemment un sous-anneau de A, la réciproque étant inexacte. Les idéaux d'un anneau sont d'ordinaire désignés par des minuscules gothiques.

Tout idéal à gauche dans un anneau A est idéal à droite dans l'opposé de A, et réciproquement. Lorsque A est commutatif, les trois espèces d'idéaux se confondent, et on parle alors simplement d'idéaux de A.

Remarques. — 1) Un idéal à gauche dans un anneau A n'est autre qu'un sous-groupe du groupe additif de A, stable pour les lois externes de l'anneau A, et pour la loi externe à gauche déduite de la multiplication de A.

2) Comme celle de sous-anneau, la notion d'idéal, dans un anneau à opérateurs A, est essentiellement relative aux lois externes données sur A ; les remarques faites au n° 4 pour les sous-anneaux s'appliquent également aux idéaux. En particulier, lorsqu'il y aura lieu de considérer sur un ensemble A, plusieurs

structures d'anneau à opérateurs ayant même structure d'anneau sous-jacente, on distinguera les idéaux relatifs à ces diverses structures en précisant pour quelles lois externes ils sont *stables*.

THÉORÈME 1. — *Toute relation d'équivalence compatible avec la structure d'un anneau A, est de la forme $x - y \in \alpha$, où α est un idéal bilatère de A ; et le quotient de A par cette relation est un anneau.*

La première partie résulte de ce qui précède. D'autre part, le quotient de l'addition dans A par la relation d'équivalence considérée R est une loi de groupe abélien sur A/R , et les quotients des lois externes de A sont distributives par rapport à la loi de groupe (§ 6, n° 11) ; enfin, le quotient par R de la multiplication dans A est une loi associative sur A/R (§ 4, n° 3), doublement distributive par rapport à la loi quotient de l'addition (§ 5, n° 1), et on vérifie aisément qu'elle satisfait aux identités (7).

La relation d'équivalence $x - y \in \alpha$, définie par un idéal bilatère α dans un anneau A, se note le plus souvent $x \equiv y \pmod{\alpha}$, ou $x \equiv y \pmod{\alpha}$, et s'appelle *congruence modulo α* . Les relations $x \equiv y \pmod{\alpha}$, $x' \equiv y' \pmod{\alpha}$ entraînent donc $x + x' \equiv y + y' \pmod{\alpha}$, $-x \equiv -y \pmod{\alpha}$, $xx' \equiv yy' \pmod{\alpha}$ et $\alpha x \equiv \alpha y \pmod{\alpha}$ pour tout opérateur α (*règles du calcul des congruences*).

Z

On notera par contre que la relation $xy \equiv xz \pmod{\alpha}$ n'entraîne pas nécessairement $y \equiv z \pmod{\alpha}$, car la classe $(\text{mod. } \alpha)$ de x n'est pas nécessairement élément régulier pour le quotient de la multiplication, même si x est régulier pour la multiplication dans A (voir exemple 4 ci-dessous).

DÉFINITION 6. — *Le quotient d'un anneau A par la congruence modulo un idéal bilatère α s'appelle l'anneau quotient de A par α , et se note A/α .*

Exemples d'idéaux et d'anneaux quotients. — 1) Un anneau A est toujours idéal bilatère dans A ; de même l'ensemble réduit au seul élément 0 est un idéal bilatère dans A, qu'on appelle l'*idéal nul*, et qu'on note (0). L'anneau quotient $A/(0)$ est isomorphe à A ; l'anneau quotient A/A est réduit à 0.

2) Pour tout élément a d'un anneau A, l'ensemble $A.a$ (resp. $a.A$) est un idéal à gauche (resp. à droite) de A ; on notera que, si A n'a pas d'élément unité, cet idéal ne contient pas nécessairement a .

3) Si M est une partie quelconque de A, l'ensemble des éléments $x \in A$ tels que $xy = 0$ (resp. $yx = 0$) pour tout $y \in M$, est un idéal à gauche (resp. à droite) qu'on appelle l'*annulateur à gauche* (resp. *annulateur à droite*) de M. Si A n'a pas de diviseurs de 0, et si M contient un élément $\neq 0$, les annulateurs de M se réduisent à l'idéal nul.

4) Les idéaux dans l'anneau Z des entiers rationnels sont des sous-groupes additifs de Z, donc de la forme $n.Z$, où $n \in \mathbb{N}$; mais réciproquement, il est évident que tout ensemble de cette forme est un idéal de Z ; en d'autres termes, il y a identité entre les idéaux de l'anneau Z et les sous-groupes du groupe additif Z ; l'idéal $n.Z$ se note encore (n) . Pour $n > 0$, l'anneau quotient $Z/(n)$ est un anneau commutatif fini de n éléments, dont les lois internes sont l'addition et la multiplication modulo n (§ 4, n° 3) ; on remarquera qu'il possède en général des diviseurs de 0 : par exemple, on a $2 \not\equiv 0 \pmod{4}$, mais $2.2 \equiv 0 \pmod{4}$ donc la classe $(\text{mod. } 4)$ de 2 est diviseur de 0 dans l'anneau $Z/(4)$.

6. Propriétés des idéaux.

Dans ce n° et le suivant, nous ne parlerons que des idéaux à gauche ; nous laissons au lecteur le soin d'énoncer les propositions correspondantes pour les idéaux à droite et les idéaux bilatères.

Soit A un anneau, α un idéal à gauche de A, B un sous-anneau de A ; l'intersection $B \cap \alpha$ est un idéal à gauche dans l'anneau B. En particulier, si $\alpha \subset B$, α est un idéal à gauche dans B ; mais inversement, un idéal à gauche dans B n'est pas nécessairement idéal à gauche dans A.

Les idéaux à gauche de A étant identiques aux sous-groupes stables relatifs à une structure de groupe à opérateurs sur A, toutes les propriétés des sous-groupes stables d'un groupe à opérateurs (§ 6, n° 10) leur sont applicables. C'est ainsi que l'intersection d'une famille (α_i) d'idéaux à gauche est un idéal à gauche ; parmi les idéaux à gauche qui contiennent une partie donnée M de A, il en existe un plus petit, qu'on appelle l'*idéal à gauche engendré* par M ; on dit aussi que M est un *système de générateurs* de cet idéal.

En particulier, dans un anneau A ayant un élément unité e, l'*idéal à gauche engendré* par l'ensemble réduit à un seul élément a est l'ensemble $A.a$ des éléments de la forme xa , où x parcourt A ; cet ensemble est en effet un idéal à gauche, contient $a = ea$, et est contenu dans tout idéal à gauche contenant a . Lorsqu'en

outre A est commutatif, l'idéal $A \cdot a = a \cdot A$ engendré par un seul élément a se note (a) et s'appelle *idéal principal*.

Nous avons vu ci-dessus que, dans l'anneau \mathbf{Z} , tout idéal est principal.

PROPOSITION 3. — *Dans un anneau A, l'idéal à gauche engendré par la réunion d'une famille $(\alpha_i)_{i \in I}$ d'idéaux à gauche de A, est l'ensemble des sommes $\sum_{i \in H} x_i$, où $x_i \in \alpha_i$, et H est une partie finie quelconque de l'ensemble d'indices I.*

On vérifie aisément que l'ensemble des sommes $\sum_{i \in H} x_i$ est le sous-groupe du groupe additif de A engendré par la réunion des α_i ; il suffit de remarquer que si $x = \sum_{i \in H} x_i$, $y = \sum_{i \in K} y_i$ sont deux de ses éléments, on peut aussi écrire $x = \sum_{i \in H \cup K} x_i$, $y = \sum_{i \in H \cup K} y_i$ en posant $x_i = 0$ si $i \notin H$, $y_i = 0$ si $i \notin K$; on a donc $x + y = \sum_{i \in H \cup K} (x_i + y_i)$ et $x_i + y_i \in \alpha_i$. D'autre part, pour tout $z \in A$, on a $z(\sum_{i \in H} x_i) = \sum_{i \in H} zx_i$, et $zx_i \in \alpha_i$; enfin, pour tout opérateur α de A, on a de même $\alpha(\sum_{i \in H} x_i) = \sum_{i \in H} \alpha x_i$, et $\alpha x_i \in \alpha_i$.

COROLLAIRE. — *Le plus petit idéal à gauche contenant un nombre fini d'idéaux à gauche α_i ($1 \leq i \leq n$) est leur somme $\sum_{i=1}^n \alpha_i$.*

Par extension, on appelle encore *somme* d'une famille infinie $(\alpha_i)_{i \in I}$ d'idéaux à gauche de A, et on note $\sum_{i \in I} \alpha_i$, l'idéal engendré par la réunion des α_i (cf. chap. II, § 1).

Si on considère l'idéal à gauche engendré par une partie non vide quelconque M de A, il est clair que cet idéal contient, pour tout $x \in M$, l'idéal à gauche α_x engendré par le seul élément x ; il est donc identique à la somme $\sum_{x \in M} \alpha_x$. En particulier :

PROPOSITION 4. — *Dans un anneau A ayant un élément unité, l'idéal à gauche engendré par une partie non vide M de A est identique à l'ensemble des sommes de la forme $\sum_i x_i \alpha_i$, où (α_i) est une famille finie quelconque d'éléments de M, et les x_i des éléments quelconques de A.*

Exemple. — Dans l'anneau \mathbf{Z} , l'idéal engendré par un ensemble de deux éléments m, n est la somme $(m) + (n)$ des idéaux principaux engendrés par chacun d'eux; comme tout idéal dans \mathbf{Z} , cet idéal est un idéal principal (d) ($d \in \mathbf{N}$). Or, pour qu'un idéal principal (a) contienne m , il faut et il suffit que a soit un diviseur de m . On voit donc que tous les diviseurs communs de m et n sont diviseurs d'un même élément $d \in \mathbf{N}$, qui est lui-même diviseur commun de m et n , et par suite le plus grand des diviseurs communs ≥ 0 de m et n ; aussi appelle-t-on d le plus grand commun diviseur (en abrégé p. g. c. d.) de m et n ; et on voit qu'il existe deux entiers (positifs ou négatifs) p, q , tels que $d = pm + qn$.

Remarquons en passant que le plus grand idéal contenu dans les idéaux (m) et (n) , c'est-à-dire leur intersection $(m) \cap (n)$, est aussi un idéal principal (r) ($r \in \mathbf{N}$); un raisonnement analogue prouve que tout multiple commun de m et n est un multiple de r , et que r est le plus petit des multiples communs ≥ 0 de m et n ; on l'appelle le plus petit commun multiple (p. p. c. m.) de m et n .

On généralise aisément ces considérations à un nombre fini quelconque d'entiers rationnels (cf. chap. V).

7. Idéaux maximaux.

DÉFINITION 7. — *L'ensemble des idéaux à gauche d'un anneau A étant ordonné par inclusion, tout élément maximal de l'ensemble des idéaux à gauche différents de A est appelé idéal à gauche maximal de A.*

Exemple. — Un idéal maximal dans l'anneau \mathbf{Z} est un idéal principal (p), où $p > 1$ est un nombre entier caractérisé par la propriété de ne posséder aucun diviseur q tel que $1 < q < p$; un tel nombre est appelé *nombre premier*; par exemple, les nombres 2, 3, 5, 7 sont premiers.

Tout entier $n > 1$ possède un diviseur premier, car le plus petit des diviseurs $\neq 1$ de n est évidemment premier.

On peut encore dire que, dans \mathbf{Z} , tout idéal $(n) \neq \mathbf{Z}$ est contenu dans un idéal maximal; sous cette forme, la proposition est un cas particulier du théorème général suivant :

THÉORÈME 2 (Krull). — *Dans un anneau A possédant un élément unité, tout idéal à gauche différent de A est contenu dans un idéal à gauche maximal.*

D'après le th. de Zorn (Ens. R, § 6, n° 10), il suffit de prouver que l'ensemble \mathfrak{F} des idéaux à gauche $\neq A$, ordonné par inclusion, est *inductif*, c'est-à-dire que, si \mathfrak{G} est une partie totalement ordonnée de \mathfrak{F} , la réunion \mathfrak{M} des idéaux appartenant à \mathfrak{G} est un idéal à gauche $\neq A$. Or, aucun des idéaux de \mathfrak{G} ne contient l'élément unité e de A, donc $e \notin \mathfrak{M}$; d'autre part, tout $x \in \mathfrak{M}$ appartient à un idéal $\mathfrak{a} \in \mathfrak{G}$, donc $zx \in \mathfrak{a} \subset \mathfrak{M}$ et $\alpha x \in \mathfrak{a} \subset \mathfrak{M}$ pour tout $z \in A$ et tout opérateur α de A; enfin, si x et y sont deux éléments quelconques de \mathfrak{M} , il existe deux idéaux $\mathfrak{a}, \mathfrak{b}$, appartenant à \mathfrak{G} et tels que $x \in \mathfrak{a}$, $y \in \mathfrak{b}$; comme l'un des deux idéaux $\mathfrak{a}, \mathfrak{b}$ contient l'autre, $x - y$ appartient à l'un d'eux, et par suite à \mathfrak{M} .

Remarque. — Le th. 2 n'est plus toujours vrai lorsqu'on ne suppose pas que A possède un élément unité (voir exerc. 14 b)).

8. Homomorphismes d'anneaux.

Les définitions générales du § 4, n° 4, permettent de définir une *représentation* d'un anneau A dans un ensemble A' muni d'une structure *homologue* à celle de A (§ 4, n° 1): cela signifie ici que la structure de A' est déterminée d'une part par deux lois internes, correspondant respectivement à l'addition et la multiplication dans A, d'autre part par des lois externes correspondant biunivoquement à celles de A, les lois correspondantes ayant même domaine d'opérateurs. Dans ces conditions (les lois correspondantes étant notées par le même signe) :

DÉFINITION 8. — *On dit qu'une application f d'un anneau A dans un ensemble A' muni d'une structure homologue est une représentation (ou un homomorphisme) de A dans A' si, quels que soient les éléments $x \in A$, $y \in A$ et l'opérateur α de A, les composés $f(x) + f(y)$, $f(x)f(y)$ et $\alpha f(x)$ sont définis, et on a $f(x+y) = f(x) + f(y)$, $f(xy) = f(x)f(y)$, $f(\alpha x) = \alpha f(x)$.*

L'application canonique de A sur un anneau quotient de A est un homomorphisme, dit *homomorphisme canonique*.

En utilisant le th. 1 ci-dessus, le théorème d'homomorphie (§ 4, th. 1) donne, pour les anneaux, le théorème suivant :

THÉORÈME 3. — *Soit f une représentation d'un anneau A dans un ensemble A' muni d'une structure homologue. L'image f(A) est un anneau (pour la structure induite par celle de A'), dans lequel f(0) est élément neutre pour l'addition (noté également 0). L'image réciproque $\mathfrak{a} = f(0)$ de cet élément neutre est un idéal bilatère de A; l'anneau f(A) est isomorphe à l'anneau quotient A/ \mathfrak{a} , et la représentation f est composée d'un isomorphisme de A/ \mathfrak{a} dans A' et de l'homomorphisme canonique de A sur A/ \mathfrak{a} .*

Exemple. — Soit A un anneau sans opérateurs, non réduit à 0 et possédant un élément unité e; l'application $n \rightarrow n \cdot e$ est une représentation de l'anneau \mathbf{Z} dans A; le sous-anneau de A formé des éléments $n \cdot e$ est donc isomorphe à un anneau quotient $\mathbf{Z}/(q)$, où q est un entier ≥ 0 , qu'on appelle la *caractéristique* de l'anneau A (cf. chap. II, § 1); si $q > 0$, on peut définir ce nombre comme le plus petit des entiers $m > 0$ tels que, pour tout $x \in A$, $m \cdot x = 0$. En particulier, l'anneau $\mathbf{Z}/(n)$ a pour caractéristique n.

PROPOSITION 5. — *Dans un anneau A, si a est un élément inversible, l'application $x \rightarrow axa^{-1}$ est un automorphisme de A.*

On a en effet $a(x + y)a^{-1} = axa^{-1} + aya^{-1}$, $a(xy)a^{-1} = (axa^{-1})(aya^{-1})$, et, pour tout opérateur α de A, $a(\alpha x)a^{-1} = \alpha(axa^{-1})$ en vertu de (7); d'autre part, la relation $y = axa^{-1}$ équivaut à $x = a^{-1}ya$, donc $x \rightarrow axa^{-1}$ est une application biunivoque de A sur lui-même. On l'appelle encore *automorphisme intérieur* de A.

9. Sous-anneaux et idéaux dans un anneau quotient.

THÉORÈME 4. — *Soit f l'homomorphisme canonique d'un anneau A sur le quotient A' = A/ \mathfrak{a} de A par un idéal bilatère \mathfrak{a} .*

a) *L'image réciproque $B = \overline{f}(B')$ d'un sous-anneau B' de A' est un sous-anneau de A, contenant \mathfrak{a} ; on a $B' = f(B)$, et B' est un anneau isomorphe à l'anneau quotient B/ \mathfrak{a} .*

b) *La relation $B = \overline{f}(B')$ établit une correspondance biunivoque entre les sous-anneaux de A' et les sous-anneaux de A contenant \mathfrak{a} .*

c) *Si B est un sous-anneau quelconque de A, B + \mathfrak{a} est un sous-*

anneau de A, et $f(B)$ est un sous-anneau de A' isomorphe à $B/(B \cap \alpha)$ et à $(B + \alpha)/\alpha$.

On vérifie immédiatement que, si B' est un sous-anneau de A' , $B = \bar{f}(B')$ est un sous-anneau de A, et contient α ; comme f applique A sur A' , il applique B sur B' , donc B' est isomorphe à B/α d'après le th. 3; d'où a).

Inversement, si B est un sous-anneau de A contenant α , B est saturé pour la congruence mod. α , donc si $B' = f(B)$, on a $B = \bar{f}(B')$, ce qui prouve b).

Établissons enfin c). Si B est un sous-anneau quelconque de A, la restriction de f à B est une représentation de B dans A' , et l'image réciproque de 0 par cette représentation est $B \cap \alpha$; d'après le th. 3, $f(B)$ est donc isomorphe à $B/(B \cap \alpha)$. L'ensemble $B + \alpha$ s'obtient en saturant B pour la relation $x \equiv y \pmod{\alpha}$; d'après le second th. d'isomorphie (§ 4, th. 3), il est stable pour la multiplication et les lois externes de A, et comme c'est un sous-groupe du groupe additif de A, c'est un sous-anneau de A; le second th. d'isomorphie prouve en outre que $(B + \alpha)/\alpha$ est isomorphe à $B/(B \cap \alpha)$.

THÉORÈME 5. — Soit f l'homomorphisme canonique d'un anneau A sur le quotient $A' = A/\alpha$ de A par un idéal bilatère α .

a) L'image réciproque $\mathfrak{b} = \bar{f}(\mathfrak{b}')$ d'un idéal à gauche (resp. à droite) \mathfrak{b}' de A' est un idéal à gauche (resp. à droite) de A, contenant α , et on a $\mathfrak{b}' = f(\mathfrak{b})$.

b) La relation $\mathfrak{b} = \bar{f}(\mathfrak{b}')$ établit une correspondance biunivoque entre les idéaux à gauche (resp. à droite) de A' et les idéaux à gauche (resp. à droite) de A contenant α . Si \mathfrak{b}' et \mathfrak{c}' sont deux idéaux à gauche (resp. à droite) de A' , on a

$$(8) \quad \bar{f}(\mathfrak{b}' + \mathfrak{c}') = \bar{f}(\mathfrak{b}') + \bar{f}(\mathfrak{c}'), \quad \bar{f}(\mathfrak{b}' \cap \mathfrak{c}') = \bar{f}(\mathfrak{b}') \cap \bar{f}(\mathfrak{c}').$$

c) Si \mathfrak{b}' est un idéal bilatère de A' , $\mathfrak{b} = \bar{f}(\mathfrak{b}')$ est un idéal bilatère de A, contenant α , et A/\mathfrak{b} est isomorphe à A'/\mathfrak{b}' .

On vérifie immédiatement que si \mathfrak{b}' est idéal à gauche (resp. à droite, bilatère) de A' , $\mathfrak{b} = \bar{f}(\mathfrak{b}')$ est idéal à gauche (resp. à droite, bilatère) de A et contient α ; comme f applique A sur A' , il applique \mathfrak{b} sur \mathfrak{b}' , d'où a). Inversement, si \mathfrak{b} est idéal à gauche de A,

$f(\mathfrak{b})$ est idéal à gauche de A' ; car si $x \in \mathfrak{b}$, et $z' \in A'$, il existe $z \in A$ tel que $z' = f(z)$, donc $z'f(x) = f(z)f(x) = f(zx) \in f(\mathfrak{b})$; démonstration analogue pour les idéaux à droite. En particulier, si $\mathfrak{b} \supset \alpha$, \mathfrak{b} est saturé pour la congruence mod. α , donc si $\mathfrak{b}' = f(\mathfrak{b})$, $\mathfrak{b} = \bar{f}(\mathfrak{b}')$, ce qui établit la première partie de b); les relations (8) sont valables pour des parties quelconques \mathfrak{b}' et \mathfrak{c}' de A' (§ 6, nº 13).

On peut aussi remarquer que, dans l'ensemble des idéaux de A' , ordonné par inclusion, la somme de deux idéaux est leur *borne supérieure*, et leur intersection leur *borne inférieure*; de même dans l'ensemble des idéaux de A contenant α ; les formules (8) résultent alors de ce que l'application biunivoque $\mathfrak{b}' \rightarrow \bar{f}(\mathfrak{b}')$ du premier de ces ensembles sur le second est *croissante*.

Enfin, lorsque \mathfrak{b}' est idéal bilatère de A' et $\mathfrak{b} = \bar{f}(\mathfrak{b}')$, l'isomorphie de A/\mathfrak{b} et A'/\mathfrak{b}' résulte du premier th. d'isomorphie (§ 4, th. 2).

Pour tout sous-anneau $B \supset \alpha$ de A, on *identifiera* en général les anneaux $f(B)$ et B/α ; en particulier, pour un idéal $\mathfrak{b} \supset \alpha$, on notera \mathfrak{b}/α l'idéal $f(\mathfrak{b})$ de A' ; lorsque \mathfrak{b} est un idéal bilatère, la partie c) du th. 5 s'exprime donc en disant que l'anneau quotient $(A/\alpha)/(\mathfrak{b}/\alpha)$ est isomorphe à A/\mathfrak{b} .

10. Produits d'anneaux.

Il est immédiat, d'après les remarques du § 4, nº 5 et du § 5, nº 1, que le produit des structures d'une famille (A_i) d'anneaux à opérateurs homologues est encore une structure d'anneau à opérateurs; on pose donc la définition suivante :

DÉFINITION 9. — On appelle anneau produit d'une famille $(A_i)_{i \in I}$ d'anneaux à opérateurs homologues, l'ensemble $A = \prod_{i \in I} A_i$, muni de la structure d'anneau à opérateurs déterminée par les lois $((x_i), (y_i)) \rightarrow (x_i + y_i)$, $((x_i), (y_i)) \rightarrow (x_i y_i)$, $(z, (x_i)) \rightarrow (z x_i)$ (z opérateur quelconque des A_i).

Un cas particulier important de produits d'anneaux est l'anneau formé par les applications d'un ensemble E dans un anneau A, qui est identique à l'anneau produit A^E (cf. § 4, nº 8).

Si B_i est un sous-anneau (resp. idéal à gauche, idéal à droite) de A_i , $B = \prod_{i \in I} B_i$ est un sous-anneau (resp. idéal à gauche, idéal à droite) de $A = \prod_{i \in I} A_i$. En particulier, soit J une partie non vide de I , et $K = \bigcap J$; si on prend $B_i = A_i$ pour $i \in J$, $B_i = \{0\}$ pour $i \in K$, le sous-anneau $A'_J = \prod_{i \in J} B_i$ est un idéal bilatère de A , dont la structure d'anneau (à opérateurs) est isomorphe à celle de l'anneau produit $A_J = \prod_{i \in J} A_i$, avec lequel on l'identifiera souvent. La projection pr_J de A sur A_J est un homomorphisme; l'image réciproque de 0 par cet homomorphisme n'est autre que A'_K , donc A_J est isomorphe à A/A'_K , et A est isomorphe au produit $A'_J \times (A/A'_K)$. On a en outre $A'_J \cdot A'_K = \{0\}$ d'après la définition de la multiplication dans A : on dit que les sous-anneaux A'_J et A'_K s'annulent mutuellement. Il en résulte que tout idéal dans A'_J est aussi un idéal dans A .

On voit aussi que tout produit d'anneaux non réduits à 0 contient des diviseurs de 0.

Lorsque J est un ensemble $\{i\}$ à un seul élément, on désigne encore par A'_i le sous-anneau A'_J , isomorphe à A_i . Si α est un idéal à gauche (resp. à droite) dans A , sa projection sur A_i est un idéal à gauche (resp. à droite) dans A_i (th. 5); en outre :

PROPOSITION 6. — *Si l'anneau produit A possède un élément unité (c'est-à-dire si chacun des A_i possède un élément unité), l'idéal $\alpha \cap A'_i$ est isomorphe à la projection de α sur A_i ; en outre, si l'ensemble d'indices I est fini, α est identique au produit de ses projections sur les A_i .*

En effet, soit $x = (x_i)$ un élément de α , e_i l'élément unité de A_i , e'_i l'élément unité de A'_i ; α contient $e'_i x$, qui n'est autre que l'élément dont toutes les coordonnées sont nulles, à l'exception de celle d'indice i , égale à x_i ; d'où aussitôt la proposition.

Cette proposition est inexacte si on ne suppose plus que A ait un élément unité (voir exerc. 14 c)).

11. Composé direct de sous-anneaux.

Soit $A = \prod_{1 \leq i \leq n} A_i$ un produit d'une famille finie d'anneaux A_i ; avec les notations précédentes, le groupe additif de A est *somme directe* (§ 6, n° 6) des groupes additifs des A'_i (par abus de langage, on exprime ce fait en disant que l'anneau A est *somme directe des sous-anneaux A'_i*); mais il y a plus, car si $x = \sum_{i=1}^n x_i$, $y = \sum_{i=1}^n y_i$ sont les décompositions (uniques) de deux éléments quelconques x, y de A ($x_i \in A'_i$, $y_i \in A'_i$), on a $xy = \sum_{i=1}^n x_i y_i$.

DÉFINITION 10. — *On dit qu'un anneau A est composé direct d'une famille finie $(B_i)_{1 \leq i \leq n}$ de sous-anneaux de A s'il est somme directe des B_i , et si on a identiquement*

$$\left(\sum_{i=1}^n x_i \right) \left(\sum_{i=1}^n y_i \right) = \sum_{i=1}^n x_i y_i \quad (x_i \in B_i, y_i \in B_i).$$

Si A est composé direct des sous-anneaux B_i , il est donc isomorphe à leur produit.



On aura soin de ne pas confondre, pour les anneaux, les notions de *somme directe* et de *composé direct* de sous-anneaux : un anneau peut fort bien être somme directe de sous-anneaux (et même d'idéaux à droite ou d'idéaux à gauche) sans être leur composé direct ; on en verra des exemples au chap. II.

PROPOSITION 7. — *Si un anneau A est somme directe d'une famille finie $(B_i)_{1 \leq i \leq n}$ de sous-anneaux, les propositions suivantes sont équivalentes :*

- a) A est composé direct des B_i ;
- b) les sous-anneaux B_i sont des idéaux bilatères dans A ;
- c) les sous-anneaux B_i s'annulent mutuellement.

En effet, a) entraîne b) puisque A est isomorphe à $\prod_{1 \leq i \leq n} B_i$; b) entraîne c), car si les B_i sont des idéaux bilatères, on a

$$B_i \cdot B_j \subset B_i \cap B_j = \{0\} \text{ pour } i \neq j;$$

enfin c) entraîne a) d'après la distributivité de la multiplication et la déf. 10.

Exemple. — Considérons, dans l'anneau quotient $\mathbf{Z}/(6)$, le sous-anneau A formé des classes (mod. 6) de 0 et 3, et le sous-anneau B formé des classes (mod. 6) de 0, 2 et 4 ; A est isomorphe à $\mathbf{Z}/(2)$ et B à $\mathbf{Z}/(3)$; $\mathbf{Z}/(6)$ est somme directe de A et B, car on a $1 = 3 - 2$, et on ne peut avoir $u \equiv v \pmod{6}$, $u \equiv 0 \pmod{2}$, et $v \equiv 0 \pmod{3}$ que si $u \equiv v \equiv 0 \pmod{6}$; enfin, il est immédiat que A et B s'annulent mutuellement ; donc $\mathbf{Z}/(6)$ est composé direct de A et B, et par suite isomorphe au produit $(\mathbf{Z}/(2)) \times (\mathbf{Z}/(3))$ (cf. chap. V).

En raison de l'isomorphie d'un composé direct et d'un produit, si A est composé direct des sous-anneaux B_i , le centre C de A est composé direct des centres C_i des B_i , et on a $C_i = C \cap B_i$ (§ 4, n° 5).

PROPOSITION 8. — Soit A un anneau composé direct de sous-anneaux B_i ($1 \leq i \leq n$) ; si α_i est un idéal bilatère dans B_i , et $\alpha = \sum_{i=1}^n \alpha_i$, l'anneau quotient A/α est isomorphe au produit des anneaux B_i/α_i . C'est une conséquence immédiate de la prop. 4 du § 4.

Exercices. — 1) Déterminer toutes les structures d'anneau sur un ensemble de n éléments, pour $2 \leq n \leq 5$, ainsi que les idéaux de ces anneaux.

2) Montrer que l'anneau des endomorphismes du groupe abélien produit de deux groupes cycliques d'ordre 2, est non commutatif et admet des diviseurs de 0.

3) Soit A un anneau (sans opérateurs) ; sur l'ensemble $\mathbf{Z} \times A$ on définit l'addition et la multiplication de la manière suivante :

$$(m, x) + (n, y) = (m+n, x+y)$$

$$(m, x)(n, y) = (mn, m \cdot y + n \cdot x + xy).$$

Montrer que ces deux lois définissent sur $\mathbf{Z} \times A$ une structure d'anneau ayant un élément unité, et que A est isomorphe à un idéal bilatère de cet anneau.

4) Soit A un anneau ayant un élément unité e. Si, pour un élément $a \in A$, il existe un $a' \in A$ et un seul tel que $aa' = e$, a est inversible et a' est l'inverse de a (montrer d'abord que a n'est pas diviseur à gauche de 0, puis considérer le produit $aa'a$).

¶ 5) Soit A un anneau sans diviseur de 0 et ayant un élément unité e. On suppose donnée sur A une loi interne τ partout définie, telle que la loi externe à droite déduite de τ soit distributive par

rapport à l'addition, la loi externe à gauche déduite de τ distributive par rapport à la multiplication.

a) Montrer que, si A n'est pas de caractéristique 2, on a $x \tau y = 0$ quels que soient x et y dans A (utiliser l'exerc. 4 du § 5) (*).

b) Si A est de caractéristique 2, et si on n'a pas $x \tau y = 0$ pour tout couple (x, y) d'éléments de A, l'ensemble G des $u \in A$ tels que $u \tau e = 0$ est un sous-groupe d'indice 2 du groupe additif de A, et la loi τ est déterminée si on connaît les composés $a \tau x$, pour un élément fixe (arbitraire) $a \in G$. Inversement, la donnée d'un sous-groupe G d'indice 2 du groupe additif de A, et d'une application f de A dans lui-même telle que $f(xy) = f(x)f(y)$, détermine une loi τ ayant les propriétés voulues.

6) Soit A un anneau à opérateurs, B une partie quelconque de A. Soit B' la partie de A, stable pour les lois externes de A, engendrée par B.

a) Si $B'' = B'^{\infty}$ est la partie stable pour la multiplication engendrée par B' , le sous-anneau engendré par B est identique au sous-groupe du groupe additif de A engendré par B'' .

b) L'idéal à gauche engendré par B est identique au sous-groupe du groupe additif engendré par $B' + A.B'$; l'idéal bilatère engendré par B est identique au sous-groupe du groupe additif engendré par $B' + A.B'.A$.

¶ 7) Soit A un anneau (sans opérateurs), sans diviseur de 0, tel que tout sous-groupe additif de A soit un idéal à gauche dans A. Montrer que A est isomorphe à un sous-anneau de \mathbf{Z} , ou à un anneau quotient de la forme $\mathbf{Z}/(p)$, où p est premier (en exprimant que le groupe additif engendré par un élément $a \neq 0$ est un idéal à gauche, montrer qu'on définit un isomorphisme de A dans \mathbf{Z} ou dans un anneau quotient de \mathbf{Z}).

8) Dans un anneau, l'idéal à droite engendré par un idéal à gauche est un idéal bilatère.

9) Dans un anneau, l'annulateur à droite d'un idéal à droite est un idéal bilatère.

10) Dans un anneau A, l'idéal bilatère engendré par les éléments $xy - yx$, où x et y parcourent A, est le plus petit des idéaux bilatères α tels que A/α soit commutatif.

11) Soit (α_a) une famille d'idéaux bilatères d'un anneau A, telle que $\bigcap_a \alpha_a = (0)$. Montrer que A est isomorphe à un sous-anneau de l'anneau produit $\prod_a (A/\alpha_a)$.

(*). On verra au chap. IV un exemple d'anneau d'intégrité, de caractéristique quelconque, sur lequel une loi τ est telle que la loi externe à droite déduite de τ soit à la fois distributive par rapport à l'addition et à la multiplication, et que $x \tau y$ ne soit nul que pour $x = 0$ ou $y = 0$.

¶ 12) Dans un anneau A, on dit qu'un idéal bilatère α est irréductible s'il n'existe pas de couple d'idéaux bilatères β, γ , distincts de α et tels que $\alpha = \beta \cap \gamma$.

a) Montrer que l'intersection de tous les idéaux irréductibles de A se réduit à 0 (remarquer que l'ensemble des idéaux bilatères ne contenant pas un élément $a \neq 0$ est inductif, et appliquer le th. de Zorn).

b) En déduire que tout idéal bilatère α de A est l'intersection de tous les idéaux irréductibles qui le contiennent (utiliser le th. 5).

¶ 13) Dans un anneau commutatif A, on dit qu'un idéal $\mathfrak{p} \neq A$ est premier si l'anneau quotient A/\mathfrak{p} est un anneau d'intégrité (autrement dit, si les relations $x \notin \mathfrak{p}, y \notin \mathfrak{p}$ entraînent $xy \notin \mathfrak{p}$).

a) Si A possède un élément unité, tout idéal maximal α de A est premier (remarquer que, dans l'anneau quotient A/α , l'idéal engendré par un élément quelconque $\neq 0$ est identique à A/α , et en déduire que tout élément de A/α est inversible).

b) Tout idéal premier est irréductible (exerc. 12).

c) Si l'ensemble \mathfrak{F} des idéaux premiers contenant un idéal donné $\neq A$ n'est pas vide (ce qui est toujours le cas si A possède un élément unité), il est inductif pour la relation \supset ; si A possède un élément unité, \mathfrak{F} est inductif pour la relation \subset .

d) Soit α un idéal quelconque $\neq A$, \mathfrak{b} l'ensemble des $x \in A$ tels qu'il existe une puissance $x^n \in \alpha$ (pour un n dépendant de x). Montrer que \mathfrak{b} est un idéal, et que, si $\mathfrak{b} \neq A$, l'intersection des idéaux premiers contenant α est identique à \mathfrak{b} (remarquer que, si $a \notin \mathfrak{b}$, l'ensemble des idéaux contenant α , mais ne contenant aucune puissance a^n , est inductif pour la relation \subset , et prouver que, si \mathfrak{p} est un élément maximal de cet ensemble, \mathfrak{p} est premier).

14) Pour la structure d'anneau de carré nul (n° 1, exemple III) définie sur un groupe abélien donné G, il y a identité entre les idéaux de G et les sous-groupes du groupe additif G.

a) On prend pour G le groupe additif $\mathbb{Z}/(p)$ des nombres entiers modulo un nombre premier p . Montrer que, dans l'anneau de carré nul G, l'idéal (0) est maximal, mais non premier.

b) On prend pour G le sous-groupe du groupe additif \mathbb{Q}/\mathbb{Z} des nombres rationnels modulo 1, formé des classes (mod. 1) des nombres rationnels de la forme k/p^n , où k et n sont des entiers arbitraires ≥ 0 , et p un nombre premier fixe. Montrer que tout sous-groupe de G est de la forme G_n , où G_n est l'ensemble des classes (mod. 1) des nombres de la forme k/p^n où $n \geq 0$ est fixé, et k arbitraire. En déduire que, dans l'anneau de carré nul G, il n'existe pas d'idéal maximal ni d'idéal premier.

c) En prenant pour G le groupe additif \mathbb{Z} des entiers rationnels, donner un exemple d'idéal, dans le produit $G \times G$ de l'anneau de carré nul G par lui-même, qui ne soit pas identique au produit de ses projections sur les anneaux facteurs.

15) Soit A un anneau possédant un élément unité. Si A est somme directe d'un nombre fini d'idéaux à gauche \mathfrak{l}_i ($1 \leq i \leq n$)

et si $e = \sum_{i=1}^n e_i$ ($e_i \in \mathfrak{l}_i$), on a $e_i^2 = e_i$, $e_i e_j = 0$ pour $i \neq j$, et $\mathfrak{l}_i = Ae_i$ (écrire que $x = xe$ pour tout $x \in A$). Réciproquement, si n idempotents e_i sont tels que $e_i e_j = 0$ pour $i \neq j$ et $e = \sum_{i=1}^n e_i$,

A est somme directe des n idéaux à gauche Ae_i . Pour que les idéaux Ae_i soient tous bilatères, il faut et il suffit que les e_i appartiennent au centre de A (utiliser la prop. 7).

¶ 16) Soit A un anneau, e un idempotent de A.

a) Montrer que A est somme directe de l'idéal à gauche $\alpha = Ae$, et de l'annulateur à gauche \mathfrak{b} de e (remarquer que, pour tout $x \in A$, $x - xe \in \mathfrak{b}$).

b) Tout idéal à droite \mathfrak{d} de A est somme directe de $\mathfrak{d} \cap \alpha$ (idéal à droite dans le sous-anneau α) et $\mathfrak{d} \cap \mathfrak{b}$ (idéal à droite dans le sous-anneau \mathfrak{b}).

c) Si $Ae = eA$, e est élément unité du sous-anneau α , \mathfrak{b} est un idéal bilatère de A, et A est composé direct de α et \mathfrak{b} ; tout idéal à gauche (resp. à droite) \mathfrak{c} de A est somme directe des idéaux à gauche (resp. à droite) $\mathfrak{c} \cap \alpha$ et $\mathfrak{c} \cap \mathfrak{b}$ de A.

¶ 17) Soit A un anneau ayant un élément unité e . Si le centre C de A est composé direct de sous-anneaux C_i ($1 \leq i \leq n$), et si α_i est l'idéal bilatère de A engendré par C_i , A est composé direct des α_i (pour montrer que A est somme des α_i , écrire que

$$x = xe = \sum_{i=1}^n xe_i, \text{ où } e_i \text{ est élément unité de } C_i, \text{ pour tout } x \in A;$$

pour voir que cette somme est directe, montrer que, pour tout $z \in \alpha_i$, on a $ze_i = z$, $ze_j = 0$ pour $j \neq i$.

¶ 18) Un anneau sans opérateur A est appelé anneau booléien si chacun de ses éléments est idempotent (autrement dit, si $x^2 = x$ pour tout $x \in A$).

a) Dans l'ensemble $\mathfrak{P}(E)$ des parties d'un ensemble E, montrer qu'on définit une structure d'anneau booléien en posant $AB = A \cap B$ et $A + B = (A \cap \complement B) \cup (B \cap \complement A)$. Cet anneau est isomorphe à l'anneau K^E des applications de E dans l'anneau $K = \mathbb{Z}/(2)$ des entiers modulo 2 (considérer, pour chaque partie $X \subset E$, sa « fonction caractéristique » φ_X , telle que $\varphi_X(x) = 1$ si $x \in X$, $\varphi_X(x) = 0$ si $x \notin X$).

b) Tout anneau booléien A est commutatif et de caractéristique 2 (écrire que $x + x$ est idempotent, puis que $x + y$ est idempotent).

c) Si un anneau booléien A ne contient pas de diviseur de 0, il

est réduit à 0 ou est isomorphe à $\mathbb{Z}/(2)$ (si x et y sont deux éléments quelconques de A , montrer que $xy(x+y) = 0$). En déduire que, dans un anneau booléien, tout idéal premier (exerc. 13) est maximal.

d) Dans un anneau booléien A , tout idéal $\alpha \neq A$ est l'intersection des idéaux premiers contenant α (appliquer l'exerc. 13 d)). En déduire que tout idéal irréductible (exerc. 12) est maximal (autrement dit, que les notions d'idéal irréductible, d'idéal premier et d'idéal maximal coïncident dans un anneau booléien).

e) Montrer que tout anneau booléien est isomorphe à un sous-anneau d'un anneau produit K^n , où $K = \mathbb{Z}/(2)$ (utiliser d) et l'exerc. 11).

f) Si \mathfrak{p}_i ($1 \leq i \leq n$) sont n idéaux maximaux distincts dans un anneau booléien A , et $\alpha = \bigcap_{1 \leq i \leq n} \mathfrak{p}_i$, montrer que l'anneau quotient A/α est isomorphe à l'anneau produit K^n (raisonner par récurrence sur n , en déterminant les idéaux maximaux dans K^n à l'aide de la prop. 6). En déduire que tout anneau booléien fini est de la forme K^n .

g) Dans un anneau booléien A , la relation $xy = x$ est une relation d'ordre (§ 1, exerc. 15) ; si on la note $x \leq y$, montrer que pour cette relation, A est un ensemble réticulé (Ens. R, § 6, no 8), possède un plus petit élément α , et que pour tout couple (x, y) d'éléments tels que $x \leq y$, il existe un élément $d(x, y)$ tel que $\inf(x, d(x, y)) = \alpha$, $\sup(x, d(x, y)) = y$. Réciproquement, si un ensemble ordonné A possède ces trois propriétés, montrer que les lois de composition $xy = \inf(x, y)$ et $x + y = d(\sup(x, y), \inf(x, y))$ définissent sur A une structure d'anneau booléien.

19) On appelle *annéloïde* un ensemble E muni de deux lois de composition internes : a) une multiplication xy partout définie et associative ; b) une loi notée additionnellement, *non partout définie*, et satisfaisant aux conditions suivantes : 1^o elle est *commutative* (autrement dit, si $x + y$ est défini, il en est de même de $y + x$, et on a $x + y = y + x$; on dit alors que x et y sont *addibles*) ;

2^o x et y étant addibles, pour que $x + y$ et z soient addibles il faut et il suffit que x et z d'une part, y et z d'autre part, soient addibles ; alors x et $y + z$ sont addibles et on a $(x + y) + z = x + (y + z)$;

3^o il existe un élément neutre 0 ;

4^o si x et z d'une part, y et z d'autre part, sont addibles et si $x + z = y + z$, on a $x = y$;

5^o la multiplication est doublement distributive par rapport à l'addition.

Tout anneau est un annéloïde ; pour qu'un annéloïde admettant

un élément unité e soit un anneau, il faut et il suffit qu'il existe un élément x addible avec e et tel que $x + e = 0$.

Examiner comment s'étendent aux annéloïdes les définitions et résultats du § 8 et les exercices ci-dessus (on appellera idéal à gauche d'un annéloïde E une partie α de E stable pour l'addition, et telle que $E \cdot \alpha \subset \alpha$).

20) Soit G un groupe à opérateurs, f et g deux endomorphismes de G . Pour que l'application $x \rightarrow f(x)g(x)$ soit un endomorphisme de G , il faut et il suffit que tout élément du sous-groupe $f(G)$ soit permutable avec tout élément du sous-groupe $g(G)$; si on note alors $f + g$ cet endomorphisme, et fg l'endomorphisme composé $x \rightarrow f(g(x))$, montrer que l'ensemble E des endomorphismes de G , muni de ces deux lois de composition, est un *annéloïde* ayant un élément unité (exerc. 19) ; pour que E soit un anneau, il faut et il suffit que G soit abélien.

Pour qu'un élément $f \in E$ soit addible avec tous les éléments de E , il faut et il suffit que $f(G)$ soit contenu dans le centre de G ; l'ensemble N de ces endomorphismes est un *anneau* qu'on appelle le *noyau* de l'annéloïde E .

Un endomorphisme f de G est dit *distingué* s'il est permutable avec tous les automorphismes intérieurs de G ; pour tout sous-groupe stable distingué H de G , $f(H)$ est alors un sous-groupe stable distingué de G . Montrer que l'ensemble D des endomorphismes distingués de G forme un sous-annéloïde de E , et que le noyau N est un idéal bilatère dans D (*).

§ 9. — Corps.

1. Corps et corps à opérateurs.

DÉFINITION 1. — On dit qu'un anneau K est un *corps* si l'ensemble des éléments $\neq 0$ de K est un groupe pour la loi induite par la multiplication de K .

Lorsqu'un anneau à opérateurs K possède cette propriété, on dit que K est un *corps à opérateurs*. De même que pour les anneaux, quand il ne sera pas nécessaire de préciser pour éviter toute confusion, nous parlerons de « corps » en sous-entendant qu'il s'agit d'un « corps à opérateurs ».

L'ensemble des éléments $\neq 0$ d'un corps K se notera d'ordinaire

(*) Voir H. FITTING, Die Theorie der Automorphismenringe Abelscher Gruppen, und hr Analogon bei nicht kommutativen Gruppen, *Math. Ann.*, t. CVII (1933), p. 514.

K^* ; muni de la structure de groupe qu'y détermine la multiplication de K , on l'appelle le *groupe multiplicatif* du corps K . Comme K^* est un groupe par définition, il n'est pas vide; son élément neutre e est l'*élément unité* du corps K ; comme il est $\neq 0$, un corps a au moins deux éléments.

L'anneau opposé d'un corps est évidemment encore un corps. On dit qu'un corps est *commutatif* si sa multiplication est commutative; un tel corps est identique à son opposé. Un corps non commutatif est parfois appelé *corps gauche*.

Exemples de corps commutatifs (*). — *1) Les corps les plus importants en Mathématique sont le *corps des nombres rationnels*, qui sera défini au n° 5, le *corps des nombres réels* et le *corps des nombres complexes*, que nous définirons en Topologie générale (*Top. gén.*, chap. IV et V). *

2) Sur un ensemble E de deux éléments, on peut définir une structure de corps et (à une permutation près) une seule. En effet, un des éléments de E est l'élément neutre 0 du groupe additif, l'autre est l'élément neutre e du groupe multiplicatif. Le groupe additif est complètement défini par la donnée de $e + e$, qui ne peut être que 0 ; le groupe multiplicatif se réduit à e ; enfin, on doit avoir $e \cdot 0 = 0 \cdot e = 0$. On vérifie aussitôt qu'on détermine bien ainsi sur E une structure de corps commutatif.

2. Sous-corps.

Soit B une partie non réduite à 0 d'un anneau A ; pour que B , muni de la structure induite par celle de A , soit un *corps*, il faut d'abord que B soit un *sous-anneau* de A ; en outre, ce sous-anneau doit posséder un élément unité e (qui n'est pas nécessairement élément unité de A), et tout élément $x \neq 0$ de B doit être *inversible* dans B . Inversement, si ces conditions sont remplies, B est un corps; en effet, l'ensemble B^* des éléments $\neq 0$ de B est alors stable pour la multiplication (§ 2, cor. 2 de la prop. 5), et la prop. 1 du § 6 montre que c'est un groupe.

Si A est un *corps*, les conditions pour qu'une partie B de A soit un corps se simplifient de la façon suivante: il faut et il suffit que B soit un sous-anneau de A , non réduit à 0 et *contenant les inverses* (dans A) de tous ses éléments $\neq 0$ (l'ensemble B^* , sous-groupe de A^* , doit en effet contenir l'élément unité de A).

(*) Aux chap. II et VII, nous donnerons des exemples de corps non commutatifs.

Plus généralement, si un sous-anneau B d'un corps A n'est pas réduit à 0 et possède un élément unité u , u est égal à l'élément unité e de A , car de $u^2 = u$ et $u \neq 0$, on tire $u = u \cdot u^{-1} = e$.

Si un sous-anneau B d'un corps K est un corps, on dit que c'est un *sous-corps* de K ; K est souvent appelé un *sur-corps* ou une *extension* du sous-corps B .

Étant donné un corps K , toute intersection de sous-corps de K est encore un sous-corps de K ; on peut donc définir le sous-corps *engendré* par une partie quelconque X de K comme le plus petit sous-corps de K contenant X .

PROPOSITION 1. — *Dans un corps K , l'ensemble des éléments permutable avec tous les éléments d'une partie quelconque M de K , est un sous-corps de K .*

En effet (§ 8, prop. 2) cet ensemble est un sous-anneau de K ; d'autre part, si $x \neq 0$ est permutable avec $z \in M$, il en est de même de x^{-1} (§ 2, prop. 6), d'où la proposition.

COROLLAIRE. — *Le centre d'un corps K est un sous-corps (commutatif) de K .*

3. Homomorphismes des corps.

PROPOSITION 2. — *Dans un corps K , les seuls idéaux à gauche (resp. à droite) sont (0) et K .*

En effet, si $x \neq 0$ appartient à un idéal à gauche α , $x^{-1}x = e \in \alpha$ donc $\alpha = K$.

THÉORÈME 1. — *Si f est un homomorphisme d'un corps K dans un ensemble E muni d'une structure homologue, ou bien $f(K)$ est un anneau réduit à 0 , ou bien $f(K)$ est un corps, et f un isomorphisme de K sur $f(K)$.*

En effet, l'image réciproque $f^{-1}(0)$ de l'élément 0 de l'anneau $f(K)$ est un idéal bilatère dans K , donc identique à K ou à (0) , et le théorème résulte du th. 3 du § 8.

La proposition 2 admet la réciproque suivante :

PROPOSITION 3. — *Si, dans un anneau A non réduit à 0 et admet-*

tant un élément unité, il n'existe aucun idéal à gauche distinct de (0) et de A, A est un corps.

En effet, soit x un élément quelconque $\neq 0$ de A ; comme A possède un élément unité e , l'idéal à gauche engendré par x est l'ensemble Ax ; comme il contient $x \neq 0$, il est identique à A, donc il existe $x' \in A$ tel que $x'x = e$. On a $x' \neq 0$, donc le même raisonnement prouve qu'il existe $x'' \in A$ tel que $x''x' = e$; par suite $xx' = ex' = x''x'xx' = x''ex' = x''x' = e$, autrement dit, x' est inverse de x , ce qui prouve la proposition.

Remarque. — 1) La prop. 3 n'est plus exacte si on ne suppose pas que A admette un élément unité (voir exerc. 3).

2) Dans un anneau (à opérateurs) non commutatif A, il peut fort bien n'exister aucun idéal bilatère distinct de (0) et A, sans que A soit un corps (de tels anneaux seront étudiés au chap. VII).

Le théorème suivant est un corollaire de la prop. 3 :

THÉORÈME 2. — Soit A un anneau ayant un élément unité, a un idéal bilatère de A. Pour que l'anneau quotient A/a soit un corps, il faut et il suffit que a soit un idéal à gauche maximal de A.

En effet, A/a possède un élément unité, et la condition de l'énoncé exprime que les seuls idéaux à gauche de A/a sont (0) et A/a , d'après le th. 5 du § 8.

On voit en particulier que, pour que l'anneau $\mathbb{Z}/(p)$ soit un corps, il faut et il suffit que p soit premier ; par exemple, $\mathbb{Z}/(2)$ est un corps à deux éléments, isomorphe au corps à deux éléments défini au no 1.

4. Corps des fractions d'un anneau d'intégrité.

Comme tout élément $\neq 0$ d'un corps K est inversible, donc régulier pour la multiplication, un sous-anneau quelconque de K est un anneau sans diviseur de 0 ; en particulier, tout sous-anneau d'un corps commutatif est un anneau d'intégrité. Nous allons montrer qu'inversement, tout anneau d'intégrité peut être « plongé » dans un corps commutatif.

Plus généralement :

PROPOSITION 4. — Soit A un anneau à opérateurs commutatifs, \bar{A} le symétrisé de A pour la seule multiplication (§ 2, th. 1).

a) On peut définir sur \bar{A} une structure d'anneau à opérateurs et une seule prolongeant celle de A.

b) Soit f une représentation de A dans un anneau à opérateurs A' , telle que l'image par f de tout élément régulier dans A soit inversible dans A' ; on peut prolonger f d'une manière et d'une seule en une représentation \bar{f} de \bar{A} dans A' .

a) Considérons comme d'ordinaire A comme plongé dans \bar{A} ; tout élément régulier de A est alors inversible dans \bar{A} , et tout élément de \bar{A} est de la forme $\frac{x}{y}$, où $x \in A$, $y \in A$, et y est régulier.

Cherchons à définir la somme de deux éléments $z = \frac{x}{y}$, $z' = \frac{x'}{y'}$ de \bar{A} , de façon que l'addition ainsi définie induise sur A la loi additive donnée, et que la multiplication dans \bar{A} soit distributive par rapport à cette addition ; comme on a $z = \frac{xy'}{yy'}$, $z' = \frac{x'y}{yy'}$, ces conditions entraînent nécessairement que $z + z' = \frac{xy' + x'y}{yy'}$.

Inversement, montrons d'abord que l'élément de A ainsi défini ne dépend que de z et z' et non de leur représentation sous forme de fractions ; en effet, si $z = \frac{x_1}{y_1}$, on a $x_1y = xy_1$, donc $(x_1y' + x'y_1)y = (xy' + x'y)y_1$, d'où $\frac{x_1y' + x'y_1}{y_1y'} = \frac{xy' + x'y}{yy'}$.

On vérifie aussitôt que l'addition ainsi définie dans \bar{A} est associative et commutative, que tout élément $z = \frac{x}{y}$ admet un opposé $z' = \frac{(-x)}{y}$, et enfin que la multiplication est distributive par rapport à cette addition, donc que ces deux lois définissent sur \bar{A} une structure d'anneau commutatif prolongeant celle de A.

Reste à prolonger à \bar{A} les lois externes de l'anneau A, de façon que les identités (7) du § 8 restent vérifiées ; ici encore, cela n'est possible que d'une seule manière, car si α est un opérateur de A, et $z = \frac{x}{y}$, on doit avoir $\alpha z = \frac{(\alpha x)}{y}$ en vertu de la condition précédente. L'élément αz ainsi défini ne dépend que de α et z , et non de la représentation de z sous forme de fraction, car si $\frac{x_1}{y_1} = \frac{x}{y}$, on a $\alpha(x_1y) = \alpha(xy_1)$, donc $(\alpha x_1)y = (\alpha x)y_1$; la loi externe définie de cette manière est bien distributive par rapport à l'addition dans \bar{A} et satisfait aux identités (7) du § 8.

b) Si on considère sur \bar{A} la structure définie par la seule multiplication, on sait (§ 2, th. 2) que f se prolonge d'une seule manière en une représentation \bar{f} de \bar{A} (muni de la seule multiplication) dans A' (muni de la seule multiplication), en posant $\bar{f}\left(\frac{x}{y}\right) = f(x)(f(y))^{-1}$. Il reste à vérifier que $\bar{f}(z + z') = \bar{f}(z) + \bar{f}(z')$ et $\bar{f}(\alpha z) = \alpha \bar{f}(z)$, quels que soient $z \in \bar{A}$, $z' \in \bar{A}$ et l'opérateur α , ce qui est immédiat.

DÉFINITION 2. — On appelle *anneau des fractions* (ou *anneau des quotients*) d'un anneau commutatif A , l'anneau commutatif obtenu en munissant le symétrisé \bar{A} de A (pour la seule multiplication) de la structure définie dans la prop. 4.

PROPOSITION 5. — L'anneau des fractions \bar{A} d'un anneau d'intégrité A est un corps commutatif, appelé *corps des fractions* (ou *corps des quotients*) de A .

En effet, tout élément $\neq 0$ de A étant régulier, tout élément $\neq 0$ de \bar{A} est inversible (§ 2, corollaire du th. 1).

PROPOSITION 6. — Si un anneau d'intégrité A est contenu dans un corps K (non nécessairement commutatif), l'ensemble des éléments xy^{-1} de K , où x parcourt A , et y l'ensemble des éléments $\neq 0$ de A , est un sous-corps commutatif de K , isomorphe au corps des fractions de A .

C'est une conséquence immédiate de la seconde partie de la prop. 4, appliquée à l'application identique de A sur lui-même ; la représentation de \bar{A} dans K , obtenue par prolongement, est nécessairement un isomorphisme d'après le th. 1.

5. Le corps des nombres rationnels.

DÉFINITION 3. — On appelle *corps des nombres rationnels*, et on désigne par \mathbf{Q} , le corps des fractions de l'anneau \mathbf{Z} des entiers rationnels ; les éléments de \mathbf{Q} sont appelés *nombres rationnels*.

On a défini sur \mathbf{Z} une relation d'ordre $x \leqslant y$ (§ 2, n° 5), qui satisfait aux deux conditions suivantes :

- a) $x \leqslant y$ entraîne $x + z \leqslant y + z$ quel que soit z ;
- b) la structure d'ordre définie par $x \leqslant y$ est une structure d'ensemble totalement ordonné.

Nous allons voir qu'on peut définir sur \mathbf{Q} une relation d'ordre et une seule, qui satisfasse encore à ces deux conditions et induise sur \mathbf{Z} la relation précédente (cf. chap. VI).

En effet, remarquons d'abord que la relation $x > 0$ entraîne, d'après a), que $p \cdot x > 0$ pour tout entier $p > 0$, par récurrence sur p ; il en résulte que si n est un entier > 0 , on a $\frac{1}{n} > 0$; sinon, d'après b), on aurait $\frac{1}{n} < 0$, donc $-\frac{1}{n} > 0$, et $n \cdot \left(-\frac{1}{n}\right) = -1 > 0$, ce qui est absurde. On en conclut que, si p et q sont deux entiers > 0 , le nombre rationnel $\frac{p}{q} = p \cdot \frac{1}{q}$ est > 0 ; comme tout nombre rationnel peut s'écrire sous la forme $\frac{p}{q}$, avec $p \in \mathbf{Z}$, $q \in \mathbf{N}^*$, on voit que l'ensemble \mathbf{Q}_+ des nombres rationnels $\geqslant 0$ est identique à l'ensemble des nombres de la forme $\frac{p}{q}$, avec $p \in \mathbf{N}$, $q \in \mathbf{N}^*$. D'après a) la relation $x \leqslant y$ doit être équivalente à $y - x \geqslant 0$; s'il existe une relation d'ordre sur \mathbf{Q} satisfaisant aux conditions imposées, elle est nécessairement équivalente à la relation $y - x \in \mathbf{Q}_+$. Inversement on vérifie immédiatement que cette relation est bien une relation d'ordre sur \mathbf{Q} satisfaisant aux conditions a) et b), et induisant sur \mathbf{Z} la relation définie antérieurement.

Quand nous parlerons de \mathbf{Q} comme d'un ensemble ordonné, il sera toujours entendu, sauf mention expresse du contraire, qu'il s'agit de la relation d'ordre que nous venons de définir.

Les nombres rationnels $\geqslant 0$ (resp. $\leqslant 0$, > 0 , < 0) sont dits *positifs* (resp. *négatifs*, *strictement positifs*, *strictement négatifs*) (*).

D'après la définition de la relation $x \geqslant 0$ dans \mathbf{Q} , les relations $x \geqslant 0$, $y \geqslant 0$ entraînent $xy \geqslant 0$; de même, $x \geqslant 0$ et $y \leqslant 0$ entraînent $xy \leqslant 0$, $x \leqslant 0$ et $y \leqslant 0$ entraînent $xy \geqslant 0$ (*règles des signes*). Il en résulte en particulier que l'ensemble des nombres rationnels > 0 , qu'on note \mathbf{Q}_+^* , est un sous-groupe du groupe multiplicatif \mathbf{Q}^* des nombres rationnels $\neq 0$; tout nombre rationnel $x \neq 0$ se mettant d'une manière et d'une seule sous l'une des formes $(+1)y$, $(-1)y$, où $y > 0$, on voit que le groupe multiplicatif \mathbf{Q}_+^* est le *produit direct* du sous-groupe \mathbf{Q}_+^* et du sous-groupe $\{-1, +1\}$; le composant y de x dans \mathbf{Q}_+^* s'appelle la *valeur absolue* de x , et se note $|x|$.

(*) Ici encore, nous nous écartons de la terminologie courante, où positif signifie > 0 (voir § 2, note du n° 5).

(cf. chap. V) ; le composant de x dans $\{-1, +1\}$ (égal à $+1$ si $x > 0$, à -1 si $x < 0$) s'appelle *signe* de x et se note $\text{sgn } x$.

On prolonge d'ordinaire ces deux fonctions à \mathbb{Q} tout entier en posant $|0| = 0$, et $\text{sgn } 0 = 0$.

Exercices. — 1) Quelles sont les structures de corps parmi les structures d'anneau déterminées dans l'exerc. 1 du § 8 ?

2) Un anneau *fini* sans diviseur de 0 est un corps (§ 2, exerc. 6).

¶ 3) Soit A un anneau à opérateurs dans lequel les seuls idéaux à gauche sont (0) et A . Montrer que : ou bien A est un anneau de *carré nul* (§ 8, no 1) et le groupe additif à opérateurs de A est simple, ou bien A est un *corps*.

En écartant la première de ces alternatives, on montrera successivement que : a) il existe $a \in A$ tel que $A \cdot a \neq (0)$; b) il existe $e \in A$ tel que $ea = a$ et $e^2 = e$; c) e est élément unité de A (considérer l'ensemble des éléments $x - xe$, puis l'ensemble des éléments $x - ex$, où x parcourt A).

4) Dans le corps \mathbb{Q} des nombres rationnels, il n'existe aucun sous-corps distinct de \mathbb{Q} .

¶ 5) Soit K un corps commutatif de caractéristique $\neq 2$; soit G un sous-groupe du groupe additif de K , tel que, si H désigne l'ensemble formé de 0 et des inverses des éléments $\neq 0$ de G , H soit aussi un sous-groupe du groupe additif de K . Montrer qu'il existe un élément $a \in K$ et un sous-corps K' de K tels que $G = a \cdot K'$ (établir d'abord que, si x et y sont deux éléments de G tels que $y \neq 0$, on a $\frac{x^2}{y} \in G$; en déduire que, si x, y, z sont trois éléments de G tels que $z \neq 0$, $\frac{xy}{z} \in G$).

6) Soit K un corps commutatif de caractéristique $\neq 2$; soit f une application de K dans K , telle que $f(x + y) = f(x) + f(y)$ quels que soient x et y , et que, pour tout $x \neq 0$, on ait $f(x)f\left(\frac{1}{x}\right) = 1$. Montrer que f est un isomorphisme de K sur un sous-corps de K (prouver que $f(x^2) = (f(x))^2$).

¶ 7) Soient A un anneau commutatif ayant un élément unité, \bar{A} l'anneau des fractions de A . Si S est une partie de A , stable pour la multiplication, et dont tous les éléments sont réguliers, on désigne par A_S le sous-anneau de \bar{A} formé des éléments $\frac{x}{s}$, où x parcourt A et s parcourt S .

a) Si α est un idéal de A , l'idéal de A_S engendré par α est identique à l'ensemble $\alpha \cdot A_S$ des éléments $\frac{x}{s}$, où x parcourt α et s parcourt S . Si α et β sont deux idéaux de A , on a $(\alpha + \beta) \cdot A_S = \alpha \cdot A_S + \beta \cdot A_S$, et $(\alpha \cap \beta) \cdot A_S = (\alpha \cdot A_S) \cap (\beta \cdot A_S)$.

b) Si \mathfrak{c} est un idéal de A_S , on a $(\mathfrak{c} \cap A) \cdot A_S = \mathfrak{c}$.

c) Si α est un idéal de A , on a $\alpha \subset (\alpha \cdot A_S) \cap A$; l'idéal $(\alpha \cdot A_S) \cap A$ est l'ensemble des éléments $x \in A$ tels qu'il existe un $s \in S$ pour lequel $xs \in \alpha$.

d) Soient α un idéal de A , φ l'application canonique de A sur l'anneau quotient A/α ; pour que les éléments de $\varphi(S)$ soient réguliers dans A/α , il faut et il suffit que $(\alpha \cdot A_S) \cap A = \alpha$; l'anneau quotient $A_S/(\alpha \cdot A_S)$ est alors isomorphe à $(A/\alpha)_{\varphi(S)}$.

e) Pour que le complémentaire S d'un idéal \mathfrak{p} de A soit stable pour la multiplication, il faut et il suffit que \mathfrak{p} soit premier (§ 8, exerc. 13); l'anneau quotient $A_S/(\mathfrak{p} \cdot A_S)$ est alors un corps, isomorphe au corps des fractions de l'anneau d'intégrité A/\mathfrak{p} .

¶ 8) Soit A un anneau non commutatif, sans diviseur de 0. On dit que A admet un *corps des quotients à gauche* s'il est isomorphe à un sous-anneau A' d'un corps K , tel que tout élément de K soit de la forme $x^{-1}y$, où $x \in A'$, $y \in A'$.

a) Soit A^* l'ensemble des éléments $\neq 0$ de A . Pour que A admette un corps des quotients à gauche, il faut que la condition suivante soit remplie : (G) quels que soient $x \in A$, $x' \in A^*$, il existe $u \in A^*$ et $v \in A$ tels que $ux = vx'$.

b) On suppose inversement que la condition (G) soit remplie. Montrer que, dans l'ensemble $A \times A^*$, la relation R entre (x, x') et (y, y') qui s'énonce « pour tout couple (u, v) d'éléments $\neq 0$ tels que $ux' = vy'$, on a $ux = vy$ » est une relation d'équivalence.

Soient (x, x') , (y, y') deux éléments de $A \times A^*$, ξ et η leurs classes respectives (mod. R). Pour tout couple $(u, u') \in A \times A^*$ tel que $u'x = uy'$, montrer que la classe (mod. R) de $(uy, u'x')$ ne dépend pas de la classe ξ et η ; si on la désigne par $\xi\eta$, on définit dans l'ensemble $K = (A \times A^*)/R$ une loi de composition. Si K^* est l'ensemble des éléments de K distincts de la classe 0 des éléments $(0, x')$ de $A \times A^*$, K^* , muni de la loi induite par la loi précédente, est un groupe.

Pour tout élément $x \in A$, les éléments $(x'x, x')$, où x' parcourt A^* , forment une classe (mod. R). Si on fait correspondre cette classe à x , on définit un isomorphisme de A (pour la seule multiplication) dans K . Identifiant A à son image par cet isomorphisme, la classe (mod. R) d'un couple $(x, x') \in A \times A^*$ est identifiée à l'élément $x'^{-1}x$.

Cela étant, si $\xi = x'^{-1}x$ est un élément de K , et si 1 désigne l'élément unité de K^* , on désigne par $\xi + 1$ l'élément $x'^{-1}(x + x')$, qui ne dépend pas de la représentation de ξ sous la forme $x'^{-1}x$. On pose ensuite $\xi + 0 = \xi$, et, pour $\eta \neq 0$, $\xi + \eta = \eta(\eta^{-1}\xi + 1)$. Montrer que l'addition et la multiplication ainsi définies sur K déterminent sur cet ensemble une structure de corps, qui prolonge

la structure d'anneau de A ; autrement dit, la condition (G) est suffisante pour que A admette un corps des quotients à gauche.

9) Soit A un anneau sans diviseur de 0. Pour que A admette un corps des quotients à gauche (exerc. 8), il faut et il suffit que dans A , l'intersection de deux idéaux à gauche distincts ne se réduise jamais à 0.



NOTE HISTORIQUE

(N.-B. — Les chiffres romains renvoient à la bibliographie placée à la fin de cette note).

Il est peu de notions, en Mathématique, qui soient plus primitives que celle de loi de composition : elle semble inséparable des premiers rudiments du calcul sur les entiers naturels et les grandeurs mesurables. Les documents les plus anciens qui nous restent sur la Mathématique des Égyptiens et des Babyloniens nous montrent déjà en possession d'un système complet de règles de calcul sur les entiers naturels > 0 , les nombres rationnels > 0 , les longueurs et les aires; encore que les textes qui nous sont parvenus ne traitent que de problèmes dans lesquels les données ont des valeurs numériques explicitées (*), ils ne laissent aucun doute sur la généralité attribuée aux règles employées, et dénotent une habileté technique tout à fait remarquable dans le maniement des équations du premier et du second degré ((I), p. 179 et suiv.). On n'y trouve d'ailleurs aucune trace d'un souci de justification des règles utilisées, ni même de définition précise des opérations qui interviennent : celles-ci comme celles-là restent du domaine de l'empirisme.

Pareil souci, par contre, se manifeste déjà très nettement chez les Grecs de l'époque classique ; on n'y rencontre pas encore, il est vrai, de traitement axiomatique de la théorie des entiers naturels (une telle axiomatisation n'apparaîtra qu'à la fin du xixe siècle ; voir la Note historique du Livre I, chap. III) ; mais, dans les *Éléments* d'Euclide, nombreux sont les passages donnant des démonstrations formelles de règles de calcul tout aussi intuitivement « évidentes » que celles du calcul des entiers (par exemple, la commutativité du produit de deux nombres rationnels). Les plus remarquables des démonstrations de cette nature sont celles qui se rapportent à la théorie des grandeurs, la création la plus originale de la

(*) Il ne faut pas oublier que ce n'est qu'avec Viète (xvi^e siècle) que s'introduit l'usage de désigner par des lettres tous les éléments (donnés ou inconnus) qui interviennent dans un problème d'Algèbre. Jusque là, les seules équations qui soient résolues dans les traités d'Algèbre sont à coefficients numériques ; lorsque l'auteur énonce une règle générale pour traiter les équations analogues, il le fait (du mieux qu'il peut) en langage ordinaire ; en l'absence d'un énoncé explicite de ce genre, la conduite des calculs dans les cas numériques traités rend plus ou moins vraisemblable la possession d'une telle règle.

Mathématique grecque (équivalente, comme on sait, à notre théorie des nombres réels > 0 ; voir la Note historique du Livre III, chap. iv) : Euclide y considère, entre autres, le produit de deux rapports de grandeurs, montre qu'il est indépendant de la forme sous laquelle se présentent ces rapports (premier exemple de « quotient » d'une loi de composition par une relation d'équivalence, au sens du § 4), et qu'il est commutatif ((II), Livre V, prop. 22-23) (*).

Il ne faut pas dissimuler, cependant, que ce progrès vers la rigueur s'accompagne, chez Euclide, d'une stagnation, et même sur certains points d'un recul, en ce qui concerne la technique du calcul algébrique. La prépondérance écrasante de la Géométrie (en vue de laquelle est manifestement conçue la théorie des grandeurs) paralyse tout développement autonome de la notation algébrique : les éléments entrant dans les calculs doivent, à chaque moment, être « représentés » géométriquement ; en outre, les deux lois de composition qui interviennent ne sont pas définies sur le même ensemble (l'addition des rapports n'est pas définie de façon générale, et le produit de deux longueurs n'est pas une longueur, mais une aire) ; il en résulte un manque de souplesse qui rend à peu près impraticable le maniement des relations algébriques de degré supérieur au second.

Ce n'est qu'au déclin de la Mathématique grecque classique qu'on voit Diophante revenir à la tradition des « logisticiens » ou calculateurs professionnels, qui avaient continué à appliquer telles quelles les règles héritées des Égyptiens et des Babyloniens : ne s'embarrassant plus de représentations géométriques pour les « nombres » qu'il considère, il est naturellement amené à développer les règles du calcul algébrique abstrait ; par exemple, il donne des règles qui (en langage moderne) équivalent à la formule $x^{m+n} = x^m x^n$ pour les petites valeurs (positives ou négatives) de m et n ((III), t. I, p. 8-13) ; un peu plus loin (p. 12-13) se trouve énoncée la « règle des signes », premier germe du calcul sur les nombres négatifs (**); enfin Diophante utilise, pour la première fois, un symbole littéral pour représenter une inconnue dans une équation. Par contre, il ne semble guère préoccupé de rattacher à des idées générales les méthodes qu'il applique à la résolution de ses problèmes ; quant à la conception axiomatique des lois de composition, telle qu'elle commençait à se faire jour chez Euclide, elle paraît étrangère à la pensée de Diophante comme

(*) Euclide ne donne pas à cet endroit, il est vrai, de définition formelle du produit de deux rapports, et celle qui se trouve un peu plus loin dans les *Éléments* (Livre VI, déf. 5) est considérée comme interpolée : il n'en a pas moins, bien entendu, une conception parfaitement claire de cette opération et de ses propriétés.

(**) Diophante ne connaît pas les nombres négatifs ; cette règle ne peut donc s'interpréter que comme se rapportant au calcul des polynomes, et permettant de « développer » des produits tels que $(a - b)(c - d)$.

à celle de ses continuateurs immédiats ; on ne la retrouvera en Algèbre qu'au début du XIX^e siècle.

Il fallait d'abord, durant les siècles intermédiaires, que d'une part se développât un système de notation algébrique adéquat à l'expression de lois abstraites, et que, d'autre part, la notion de « nombre » reçût un élargissement tel qu'il permit, par l'observation de cas particuliers assez diversifiés, de s'élever à des conceptions générales. A cet égard, la théorie axiomatique des rapports de grandeurs, créée par les Grecs, était insuffisante, car elle ne faisait que préciser la notion intuitive de nombre réel > 0 et les opérations sur ces nombres, déjà connues des Babyloniens sous forme plus confuse ; il va s'agir au contraire maintenant de « nombres » dont les Grecs n'avaient pas eu l'idée, et dont, au début, aucune « représentation » sensible ne s'imposait : d'une part, le zéro et les nombres négatifs, qui apparaissent dès le haut Moyen Âge dans la Mathématique hindoue ; de l'autre, les nombres imaginaires, création des algébristes italiens du XVI^e siècle.

Si on met à part le zéro, introduit d'abord comme symbole de numération avant d'être considéré comme un nombre (voir la Note historique du Livre I, chap. III), le caractère commun de ces extensions est d'être (au début tout au moins) purement « formelles ». Il faut entendre par là que les nouveaux « nombres » apparaissent tout d'abord comme résultats d'opérations appliquées dans des conditions où elles n'ont, en s'en tenant à leur définition stricte, aucun sens (par exemple, la différence $a - b$ de deux entiers naturels lorsque $a < b$) : d'où les noms de nombres « faux », « fictifs », « absurdes », « impossibles », « imaginaires », etc., qui leur sont attribués. Pour les Grecs de l'époque classique, épris avant tout de pensée claire, de pareilles extensions étaient inconcevables ; elles ne pouvaient provenir que de calculateurs plus disposés que ne l'étaient les Grecs à accorder une confiance quelque peu mystique à la puissance de leurs méthodes (« la généralité de l'Analyse », comme dira le XVIII^e siècle), et à se laisser entraîner par le mécanisme de leurs calculs sans en vérifier à chaque pas le bien-fondé ; confiance d'ailleurs justifiée le plus souvent *a posteriori*, par les résultats exacts auxquels conduisait l'extension, à ces nouveaux êtres mathématiques, de règles de calcul valables uniquement, en toute rigueur, pour les nombres antérieurement connus. C'est ce qui explique comment on s'enhardit peu à peu à considérer pour elles-mêmes (indépendamment de toute application à des calculs concrets), ces généralisations de la notion de nombre, qui, au début, n'intervenaient qu'à titre d'intermédiaires dans une suite d'opérations dont le point de départ et l'aboutissement étaient de véritables « nombres » ; une fois ce pas franchi, on commence à rechercher des interprétations, plus ou moins tangibles, des entités nouvelles qui acquièrent ainsi droit de cité dans la Mathématique (*).

(*) Cette recherche n'a d'ailleurs constitué qu'un stade transitoire dans l'évolution des notions dont il s'agit ; dès le milieu du XIX^e siècle, on est revenu,

A cet égard, les Hindous sont déjà conscients de l'interprétation que doivent recevoir les nombres négatifs dans certains cas (une dette dans un problème commercial, par exemple). Aux siècles suivants, à mesure que se diffusent en Occident (par l'intermédiaire des Arabes) les méthodes et les résultats des mathématiques grecque et hindoue, on se familiarise davantage avec le maniement de ces nombres, et on commence à en avoir d'autres « représentations » de caractère géométrique ou cinématique. C'est d'ailleurs là, avec une amélioration progressive de la notation algébrique, le seul progrès notable en Algèbre pendant la fin du Moyen âge.

Au début du xvi^e siècle, l'Algèbre connaît un nouvel essor, grâce à la découverte, par les mathématiciens de l'école italienne, de la résolution « par radicaux » de l'équation du 3^e, puis de celle du 4^e degré (dont nous parlerons avec plus de détail dans la Note historique du chap. vi) ; c'est à cette occasion que, malgré leurs répugnances, ils se trouvent pour ainsi dire contraints d'introduire dans leurs calculs les imaginaires ; peu à peu, d'ailleurs, la confiance naît dans le calcul de ces nombres « impossibles », comme dans celui des nombres négatifs, et bien qu'ici aucune « représentation » n'en ait été imaginée pendant plus de deux siècles.

D'autre part, la notation algébrique reçoit ses perfectionnements décisifs de Viète et de Descartes ; à partir de ce dernier, l'écriture algébrique est déjà, à peu de choses près, celle que nous utilisons aujourd'hui.

Du milieu du xvii^e à la fin du xviii^e siècle, il semble que les vastes horizons ouverts par la création du Calcul infinitésimal fassent quelque peu négliger l'Algèbre en général, et singulièrement la réflexion mathématique sur les lois de composition, ou sur la nature des nombres réels et complexes (*). C'est ainsi que la composition des forces et la composition des vitesses, bien connues en Mécanique dès la fin du xvii^e siècle, n'exercèrent aucune répercussion sur l'Algèbre, bien qu'elles renfermassent déjà en germe le calcul vectoriel. Il faut attendre en effet le mouvement d'idées qui, aux environs de 1800, conduit à la représentation géométrique des nombres complexes (voir la Note historique du Livre III, chap. v), pour voir utiliser, en Mathématiques pures, l'addition des vecteurs (**).

de façon pleinement consciente cette fois, à une conception formelle des diverses extensions de la notion de nombre, conception qui a fini par s'intégrer dans le point de vue « formaliste » et axiomatique, qui domine l'ensemble des mathématiques modernes.

(*) Il faut mettre à part les tentatives de Leibniz, d'une part pour mettre sous forme algébrique les raisonnements de logique formelle, d'autre part pour fonder un « calcul géométrique » opérant directement sur les éléments géométriques, sans l'intermédiaire des coordonnées ((IV), t. V, p. 141). Mais ces tentatives restèrent à l'état d'ébauches, et n'eurent aucun écho chez les contemporains ; elles ne devaient être reprises qu'au cours du xix^e siècle (voir ci-dessous).

(**) Cette opération est d'ailleurs introduite sans aucune référence à la Mécanique ; le lien entre les deux théories n'est explicitement reconnu que par les fondateurs du Calcul vectoriel, dans le second tiers du xix^e siècle.

C'est vers cette même époque que, pour la première fois en Algèbre, la notion de loi de composition s'étend, dans deux directions différentes, à des éléments qui ne présentent plus avec les « nombres » (au sens le plus large donné jusque-là à ce mot) que des analogies lointaines. La première de ces extensions est due à C. F. Gauss, à l'occasion de ses recherches arithmétiques sur les formes quadratiques $ax^2 + bxy + cy^2$ à coefficients entiers. Lagrange avait défini, dans l'ensemble des formes de même discriminant, une relation d'équivalence (*), et avait, d'autre part, démontré une identité qui fournissait, dans cet ensemble, une loi de composition commutative (non partout définie) ; partant de ces résultats, Gauss montre que cette loi est compatible (au sens du § 4) avec la relation d'équivalence précédente ((V), t. I, p. 272) : « *On voit par là* », dit-il alors, « *ce qu'on doit entendre par une classe composée de deux ou de plusieurs classes.* » Il procède ensuite à l'étude de la loi « quotient » qu'il vient ainsi de définir, établit en substance que c'est (en langage moderne) une loi de groupe abélien, et ce par des raisonnements dont la généralité dépasse de loin, le plus souvent, le cas spécial que Gauss envisage (par exemple, le raisonnement par lequel il prouve l'unicité de l'élément symétrique est identique à celui que nous avons donné pour une loi de composition quelconque dans la prop. 3 du § 2 (*ibid.*, p. 273)). Mais il ne s'arrête pas là : revenant un peu plus loin sur la question, il reconnaît l'analogie entre la composition des classes et la multiplication des entiers modulo un nombre premier (***) (*ibid.*, p. 371), mais constate aussi que le groupe des classes de formes quadratiques de discriminant donné n'est pas toujours un groupe cyclique ; les indications qu'il donne à ce sujet prouvent clairement qu'il avait reconnu, au moins sur ce cas particulier, la structure générale des groupes abéliens finis, que nous étudierons au chapitre v ((V), t. I, p. 374 et t. II, p. 266).

L'autre série de recherches dont nous voulons parler aboutit, elle aussi, à la notion de groupe, pour l'introduire de façon définitive en Mathématique : c'est la « théorie des substitutions », développement des idées de

(*) Deux formes sont équivalentes lorsque l'une d'elles se déduit de l'autre par un « changement de variables » $x' = \alpha x + \beta y, y' = \gamma x + \delta y$, où $\alpha, \beta, \gamma, \delta$ sont des entiers tels que $\alpha\delta - \beta\gamma = 1$.

(***) Il est tout à fait remarquable que Gauss note *additivement* la composition des classes de formes quadratiques, malgré l'analogie qu'il signale lui-même, et malgré le fait que l'identité de Lagrange, qui définit la composée de deux formes, suggère beaucoup plus naturellement la notation multiplicative (à laquelle sont d'ailleurs revenus tous les successeurs de Gauss). Il faut voir dans cette indifférence en matière de notation un témoignage de plus de la généralité à laquelle Gauss était certainement parvenu dans ses conceptions relatives aux lois de composition. Il ne bornait d'ailleurs pas ses vues aux lois commutatives, comme le montre un fragment non publié de son vivant, mais datant des années 1819-1820, où il donne, plus de vingt ans avant Hamilton, les formules de multiplication des quaternions ((V), t. VIII, p. 357).

Lagrange, Vandermonde et Gauss sur la résolution des équations algébriques. Nous n'avons pas à faire ici l'historique détaillé de cette question (voir la Note historique du chap. VI) ; il nous faut en retenir la définition par Ruffini, puis Cauchy ((VI), (2), t. I, p. 64), du « produit » de deux permutations d'un ensemble fini (*), et des premières notions concernant les groupes finis de permutations : transitivité, primitivité, élément neutre, éléments permutables, etc. Mais ces premières recherches restent, dans l'ensemble, assez superficielles, et c'est Evariste Galois qui doit être considéré comme le véritable initiateur de la théorie : ayant, dans ses mémorables travaux (VIII), ramené l'étude des équations algébriques à celle des groupes de permutations qu'il leur associe, il approfondit considérablement cette dernière, tant en ce qui concerne les propriétés générales des groupes (c'est Galois qui définit le premier la notion de sous-groupe distingué et en reconnaît l'importance), que la détermination de groupes possédant des propriétés particulières (où les résultats qu'il obtient comptent encore aujourd'hui parmi les plus subtils de la théorie). C'est aussi à Galois que revient la première idée de la « représentation linéaire des groupes » (***) (voir chap. VII), et ce fait prouve clairement qu'il était en possession de la notion d'*isomorphie* de deux structures de groupe, indépendamment de leurs « réalisations ».

Toutefois, s'il paraît incontestable que les méthodes géniales de Gauss et de Galois les avaient amenés à une conception très large de la notion de loi de composition, ils n'eurent pas l'occasion de développer particulièrement leurs idées sur ce point, et leurs travaux n'eurent pas d'action immédiate sur l'évolution de l'Algèbre abstraite (****). C'est dans une troisième direction que se font les progrès les plus nets vers l'abstraction : à la suite de réflexions sur la nature des imaginaires (dont la représentation géométrique avait suscité, au début du XIX^e siècle, d'assez nombreux travaux), les algébristes de l'école anglaise dégagent les premiers, de 1830 à 1850, la notion abstraite de loi de composition, et élargissent immédiatement le champ de l'Algèbre en appliquant cette notion à une foule d'êtres mathématiques nouveaux : algèbre de la Logique avec Boole (voir Notes historiques du Livre I, chap. I et II), vecteurs et quaternions avec Hamilton (IX), systèmes hypercomplexes généraux, matrices et lois

(*) La notion de fonction composée était naturellement connue bien antérieurement, tout au moins pour les fonctions de variables réelles ou complexes ; mais l'aspect algébrique de cette loi de composition, et le lien avec le produit de deux permutations, ne sont mis en lumière que par les travaux d'Abel ((VII), t. I, p. 478) et de Galois.

((**)) C'est à cette occasion que Galois, par une extension hardie du « formalisme » qui avait conduit aux nombres complexes, considère des « racines imaginaires » d'une congruence modulo un nombre premier, et découvre ainsi les *corps finis*, que nous étudierons au chapitre VI.

((****)) Ceux de Galois restèrent d'ailleurs ignorés jusqu'en 1846, et ceux de Gauss n'exercèrent une influence directe qu'en Théorie des Nombres.

non associatives avec Cayley ((X), t. I, p. 127 et 301, et t. II, p. 185 et 475). Une évolution parallèle se poursuit indépendamment sur le Continent, notamment en ce qui concerne le Calcul vectoriel (Möbius, Bellavitis), l'Algèbre linéaire et les systèmes hypercomplexes (Grassmann), dont nous parlerons avec plus de détail aux chap. II et III (*).

De tout ce bouillonnement d'idées originales et fécondes qui vient reviser l'Algèbre dans la première moitié du XIX^e siècle, celle-ci sort renouvelée jusque dans ses tendances. Auparavant, méthodes et résultats gravitaient autour du problème central de la résolution des équations algébriques (ou des équations diophantiennes en Théorie des Nombres) : « *l'Algèbre* », dit Serret dans l'Introduction de son Cours d'Algèbre supérieure (XII) « est, à proprement parler, l'Analyse des équations ». Après 1850, si les traités d'Algèbre laissent encore pendant longtemps la prééminence à la théorie des équations, les recherches nouvelles ne sont plus dominées par le souci d'applications immédiates à la résolution des équations numériques, et s'orientent de plus en plus vers ce que nous considérons aujourd'hui comme le problème essentiel de l'Algèbre, l'étude des structures algébriques pour elles-mêmes.

Ces travaux se répartissent assez nettement en trois courants, qui prolongent respectivement les trois mouvements d'idées que nous avons analysés ci-dessus, et se poursuivent parallèlement sans influences réciproques sensibles jusque dans les dernières années du XIX^e siècle (**).

C'est d'abord l'édification, par l'école allemande du XIX^e siècle (Dirichlet, Kummer, Kronecker, Dedekind, Hilbert) de la théorie des nombres algébriques, issue de l'œuvre de Gauss, à qui est due la première étude de ce genre, celle des nombres $a + bi$ (a et b rationnels). Nous n'avons pas à suivre ici l'évolution de cette théorie : il nous faut seulement relever, pour notre objet, les notions algébriques abstraites qui s'y font jour. Dès les premiers successeurs de Gauss, l'idée de *corps* (de nombres algébriques) est à la base de tous les travaux sur la question (comme aussi des recherches d'Abel et de Galois sur les équations algébriques) ; son champ d'application s'agrandit lorsque Dedekind et Weber (XIII) calquent la théorie des fonctions algébriques d'une variable sur celle des nombres algébriques. C'est à Dedekind aussi (XIV) qu'est due l'introduction de la notion d'*idéal*, qui fournit un nouvel exemple de loi de composition entre

((*)) Les principales théories développées au cours de cette période se trouvent remarquablement exposées dans l'ouvrage contemporain de H. Hankel (XI), où la notion abstraite de loi de composition est conçue et présentée avec une parfaite netteté.

((**)) Nous laissons ici volontairement de côté tout ce qui concerne, pendant cette période, l'évolution de la géométrie algébrique, et de la théorie des invariants, qui lui est étroitement liée ; ces deux théories se développent suivant leurs méthodes propres, orientées vers l'Analyse plutôt que vers l'Algèbre, et ce n'est qu'à une époque récente qu'elles ont trouvé leur place dans le vaste édifice de l'Algèbre moderne.

ensembles d'éléments ; à lui et à Kronecker remonte le rôle de plus en plus grand joué par les groupes abéliens et les modules dans la théorie des corps algébriques ; nous y reviendrons aux chapitres II, V et VI.

Nous renvoyons aussi aux chapitres ultérieurs (chap. II, III et VII) l'historique du développement de l'Algèbre linéaire et des systèmes hyper-complexes, qui se poursuit sans introduire de notion algébrique nouvelle pendant la fin du XIX^e et le début du XX^e siècle, en Angleterre (Sylvester, W. Clifford) et en Amérique (B. et C. S. Peirce, Dickson, Wedderburn) suivant la voie tracée par Hamilton et Cayley, en Allemagne (Weierstrass, Dedekind, Frobenius, Molien) et en France (Laguerre, E. Cartan) d'une manière indépendante des Anglo-Saxons, et en suivant des méthodes assez différentes.

Quant à la théorie des groupes, c'est surtout sous l'aspect de la théorie des groupes finis de permutations qu'elle se développe d'abord, à la suite de la publication des œuvres de Galois et de leur diffusion par les ouvrages de Serret (XII), et surtout le grand « Traité des Substitutions » de C. Jordan (XV). Ce dernier y résume, en les perfectionnant beaucoup, les travaux de ses prédecesseurs sur les propriétés particulières aux groupes de permutations (transitivité, primitivité, etc.), obtenant des résultats dont la plupart n'ont guère été dépassés depuis ; il étudie également, de façon approfondie, des groupes particuliers fort importants, les groupes linéaires et leurs sous-groupes (voir chap. VII et VIII) ; en outre, c'est lui qui introduit la notion fondamentale de représentation d'un groupe sur un autre, ainsi que (un peu plus tard) celle de groupe quotient, et qui démontre une partie du théorème connu sous le nom de « théorème de Jordan-Hölder » (*). C'est enfin à Jordan que remonte la première étude des groupes *infinis* (XVI), que S. Lie d'une part, F. Klein et H. Poincaré de l'autre, devaient considérablement développer, dans deux directions différentes, quelques années plus tard.

Entre temps, la définition des groupes « abstraits » avait été donnée par Cayley en 1854 ((X), t. II, p. 123 et 131), en même temps que celle des espaces homogènes, et sous une forme qui n'était d'ailleurs correcte que pour les groupes finis. Toutefois, même les recherches sur les groupes abstraits finis sont encore pendant longtemps conçues comme études de groupes de permutations, et ce n'est que vers 1880 que commence à se développer consciemment la théorie autonome des groupes finis. Nous ne poursuivons pas plus loin l'historique de cette théorie, qui n'est abordée que très superficiellement dans ce Traité ; nous renvoyons le lecteur désireux d'approfondir les questions qui s'y rattachent, et les nombreux et difficiles problèmes qu'elle soulève, aux monographies modernes de Burnside (XVII), Speiser (XVIII) et Zassenhaus (XIX).

(*) Jordan n'avait établi que l'invariance (à l'ordre près) des *ordres* des groupes quotients d'une « suite de Jordan-Hölder » pour un groupe fini ; c'est O. Hölder qui montre que les groupes quotients eux-mêmes étaient (à l'ordre près) indépendants de la suite considérée.

Ce n'est pas davantage le lieu de parler de l'extraordinaire fortune que connaît, depuis la fin du XIX^e siècle, l'idée de groupe (et celle d'*invariant*, qui lui est intimement liée) en Analyse, en Géométrie, en Mécanique et en Physique théorique. C'est par un envahissement analogue de cette notion, et des notions algébriques qui lui sont apparentées (groupes à opérateurs, anneaux, idéaux, modules) dans les parties de l'Algèbre qui paraissaient jusqu'alors assez éloignées de leur domaine propre, que se marque la dernière période de l'évolution que nous retracions ici, et qui aboutit à la synthèse des trois tendances que nous avons suivies ci-dessus. Cette unification est surtout l'œuvre de l'école allemande moderne : commencé avec Dedekind et Hilbert dans les dernières années du XIX^e siècle, le travail d'axiomatisation de l'Algèbre a été vigoureusement poursuivi par E. Steinitz, puis, à partir de 1920, sous l'impulsion d'E. Artin, E. Noether et des algébristes de leur école (Hasse, Krull, O. Schreier, van der Waerden). Le traité de van der Waerden (XX), publié en 1930, a réuni pour la première fois ces travaux en un exposé d'ensemble, ouvrant la voie et servant de guide aux multiples recherches d'Algèbre abstraite de ces dernières années.

INDEX DES NOTATIONS

BIBLIOGRAPHIE

- (I) O. NEUGEBAUER, *Vorlesungen über Geschichte der antiken Mathematik*, Bd. I : Vorgriechische Mathematik, Berlin (Springer), 1934.
- (II) *Euclidis Elementa*, 5 vol., éd. J. L. Heiberg, Lipsiae (Teubner), 1883-88.
- (II bis) T. L. HEATH, *The thirteen books of Euclid's Elements...*, 3 vol., Cambridge, 1908.
- (III) *Diophanti Alexandrini Opera Omnia...*, 2 vol., éd. P. Tannery, Lipsiae (Teubner), 1893-95.
- (III bis) *Diophante d'Alexandrie*, trad. P. Ver Eecke, Bruges (Desclée-de Brouwer), 1926.
- (IV) G. W. LEIBNIZ, *Mathematische Schriften*, éd. C. I. Gerhardt, t. V, Halle (Schmidt), 1858.
- (V) C. F. GAUSS, *Werke*, vol. I (Göttingen, 1870), II (*ibid.*, 1863) et VIII (*ibid.*, 1900).
- (VI) A. L. CAUCHY, *Oeuvres complètes* (2), t. I, Paris (Gauthier-Villars), 1905.
- (VII) N. H. ABEL, *Oeuvres*, 2 vol., éd. Sylow et Lie, Christiania, 1881.
- (VIII) E. GALOIS, *Oeuvres mathématiques*, Paris (Gauthier-Villars), 1897.
- (IX) W. R. HAMILTON, *Lectures on Quaternions*, Dublin, 1853.
- (X) A. CAYLEY, *Collected mathematical papers*, t. I et II, Cambridge (University Press), 1889.
- (XI) H. HANKEL, *Vorlesungen über die complexen Zahlen und ihre Functionen*, 1^{er} Teil : Theorie der complexen Zahlensysteme, Leipzig (Voss), 1867.
- (XII) J. A. SERRET, *Cours d'Algèbre supérieure*, 3^e éd., Paris (Gauthier-Villars), 1866.
- (XIII) R. DEDEKIND und H. WEBER, Theorie der algebraischen Funktionen einer Veränderlichen, *J. de Crelle*, t. XCII (1882), p. 181.
- (XIV) R. DEDEKIND, *Gesammelte mathematische Werke*, 3 vol., Braunschweig (Vieweg), 1932.
- (XV) C. JORDAN, *Traité des substitutions et des équations algébriques*, Paris (Gauthier-Villars), 1870.
- (XVI) C. JORDAN, Mémoire sur les groupes de mouvements, *Ann. di Mat.* (2), t. II (1868), p. 167.
- (XVII) W. BURNSIDE, *Theory of groups of finite order*, 2^e éd., Cambridge, 1911.
- (XVIII) A. SPEISER, *Theorie der Gruppen von endlicher Ordnung*, 3^e éd., Berlin (Springer), 1937.
- (XIX) H. ZASSENHAUS, *Lehrbuch der Gruppentheorie*, Bd. I, Leipzig-Berlin (Teubner), 1937.
- (XX) B. L. van der WAERDEN, *Moderne Algebra*, 2^e éd., t. I, Berlin (Springer), 1937 ; t. II (*ibid.*), 1940.

§	n°	§	n°
$x + y, x \cdot y, xy, x \tau y, x \perp y$	1 1	$\frac{1}{\tau} x, x^{-1}, -x$	2 9
$X \tau Y, X + Y, XY (X, Y$ parties)	1 1	$\frac{-n}{\tau} x, x^{-n}, (-n)x (n entier$ positif)	2 9
$\prod_{\alpha \in A} x_\alpha, \prod_{\alpha} x_\alpha, \prod_{\alpha} x_\alpha \dots$	1 2	$1/y, \frac{1}{y}, x/y, \frac{x}{y}$	2 9
$\prod_{\alpha \in A} x_\alpha, \prod_{\alpha} x_\alpha, \prod_{\alpha} x_\alpha \dots$	1 2	$\alpha \perp x, \alpha \cdot x, x \cdot \alpha, x^\alpha (\alpha opérateur, x élément)$	3 1
$\sum_{\alpha \in A} x_\alpha, \sum_{\alpha} x_\alpha, \sum_{\alpha} x_\alpha \dots$	1 2	$A \perp X, AX, XA (A partie de l'ensemble des opérateurs, X partie de l'ensemble d'éléments)$	3 1
$\prod_{\alpha \in A} x_\alpha, \prod_{\alpha} x_\alpha, \prod_{\alpha} x_\alpha \dots$	1 2	$\alpha \perp X, \alpha X, X\alpha (\alpha opérateur, X partie)$	3 1
$\prod_{p \leq i \leq q} x_i, \prod_{i=p}^q x_i \dots$	1 2	$x \tau A (\tau loi interne, x élément, A partie)$	3 1
$x_p \tau x_{p+1} \tau \dots \tau x_q \dots$	1 2	$x \equiv y \text{ (mod. } \alpha\text{)}, x \equiv y \text{ (a)}$ (a, x, y, entiers rationnels)	4 3
$\tau x, \frac{n}{\tau} x, x^n, nx \dots$	1 3	$A^{-1} (A partie d'un groupe)$	6 1
$\tau X, \frac{\infty}{\tau} X (X partie) \dots$	1 3	$(G : H) (G groupe, H sous-groupe)$	6 2
$\sum_{i=p}^q \sum_{j=r}^s x_{ij}, \sum_{j=r}^s \sum_{i=p}^q x_{ij} \dots$	1 5	$G/H (G groupe (resp. groupe à opérateurs); H sous-groupe distingué (resp. sous-groupe stable distingué))$	6 3
$\prod_{0 \leq i < j \leq n} x_{ij}, \prod_{i < j} x_{ij} \dots$	1 5	et	6 11
$\prod_{0 \leq i_1 < i_2 < \dots < i_p \leq n} x_{i_1 i_2 \dots i_p} \dots$	1 5	$x \equiv y \text{ (mod. } H\text{)}, x \equiv y \text{ (H)}$ (H sous-groupe distingué)	6 3
$\prod_{i_1 < i_2 < \dots < i_p} x_{i_1 i_2 \dots i_p} \dots$	1 5	$y^x (x et y éléments d'un groupe)$	6 4
$\prod_{\alpha \in \emptyset} x_\alpha \dots$	2 1	$\mathfrak{S}_n, \mathfrak{A}_n \dots$	7 1
$\gamma_a, \delta_a \dots$	2 2	$G/H (G groupe, H sous-groupe quelconque)$	7 6
$Z, N^* \dots$	2 5	$\sum_{i=1}^n a_i (\alpha_i idéaux) \dots$	8 6
$-x (x entier rationnel) \dots$	2 5	$K^* (K corps) \dots$	9 1
$x \leq y (x et y entiers rationnels) \dots$	2 5	$Q, Q_+, Q_+^* \dots$	9 5
$xy (x et y entiers rationnels) \dots$	2 8	$x \leq y (x et y nombres rationnels) \dots$	9 5
		$ x , \operatorname{sgn} x (x nombre rationnel) \dots$	9 5

INDEX TERMINOLOGIQUE

	§ n°		§ n°
<i>Abélien (groupe)</i>	6 7	<i>Antomorphisme extérieur</i>	
— (groupe à opérateurs) ..	6 9	d'un groupe.....	7 4
<i>Addition</i>	1 1	— intérieur d'un groupe ..	6 4
— des entiers rationnels ..	2 5		
— modulo a	4 3	<i>Bilatère (idéal)</i>	8 5
<i>Additivement (loi notée) ..</i>	1 1		
<i>Algébrique (structure)</i>	4 1	<i>Caractéristique d'un anneau</i>	8 8
<i>Alterné (groupe)</i>	7 1	<i>Central (élément)</i>	1 5
<i>Anneau</i>	8 1	<i>Centre</i>	1 5
— à opérateurs	8 2	<i>Classe à droite suivant un sous-groupe</i>	6 3
— commutatif	8 1	— à gauche suivant un sous-groupe	6 3
— de carré nul	8 1	— d'imprimitivité	7 7
— des endomorphismes d'un groupe abélien	8 1	— d'intransitivité	7 5
— des entiers rationnels ..	8 1	<i>Commutateur de deux éléments</i>	6 8
— des fractions d'un anneau	9 4	<i>Commutateurs (groupe des)</i>	6 8
— des quotients d'un anneau	9 4	<i>Commutatif (anneau)</i>	8 1
— d'intégrité	8 3	— (corps)	9 1
— produit	8 10	— (groupe)	6 7
— quotient	8 5	<i>Commutative (loi interne)</i>	1 5
<i>Anneau (structure d')</i>	8 1	<i>Commutativité d'une loi interne</i>	1 5
<i>Anneaux opposés</i>	8 1		
— à opérateurs opposés	8 2	<i>Annulateur à droite</i>	
<i>Annulateur à droite</i>	8 5	— à gauche	
<i>Application invariante par un groupe de transformations</i>	7 4	<i>Compatible (relation d'équivalence) à droite avec une loi interne</i>	4 3
— produite par un opérateur	3 1	— à gauche avec une loi interne	4 3
— symétrique d'un groupe	6 1		
<i>Associative (loi externe)</i>	5 2	— avec une loi externe	4 3
— (loi interne)	1 3	— avec une loi interne	4 3
<i>Associativité d'une loi externe</i>	5 2	— avec une structure algébrique	4 3
— d'une loi interne	1 3	<i>Composant d'un élément dans un produit direct</i>	6 6
— (double)	5 3	<i>Composé de deux éléments</i>	1 1
<i>Automorphisme d'une structure algébrique</i>	4 1	— d'une famille finie	1 5

INDEX TERMINOLOGIQUE

<i>Composé d'une famille vide.</i>	2 1	<i>Double distributivité</i>	5 1
— d'une séquence	1 2	<i>Échangeables (éléments)</i>	1 5
— d'un opérateur et d'un élément	3 1	<i>Élément central</i>	1 5
<i>Composé direct de sous-anneaux</i>	8 11	— invariant par un opérateur	3 1
<i>Congruence modulo un entier rationnel</i>	4 3	— inversible	2 9
— modulo un idéal bilatère	8 5	— neutre	2 1
<i>Conjugués (éléments) dans un groupe</i>	7 5	— régulier	2 2
<i>Corps</i>	9 1	— symétrisable	2 3
— à opérateurs	9 1	— unité	2 1
— commutatif	9 1	— unité d'un anneau	8 1
— des fractions d'un anneau d'intégrité	9 4	<i>Éléments conjugués</i>	7 5
— des nombres rationnels	9 5	— échangeables	1 5
— des quotients d'un anneau d'intégrité	9 4	— inverses	2 9
— gauche	9 1	— opposés	2 9
<i>Covariant</i>	7 4	— permutables	1 5
<i>Cyclique (groupe)</i>	6 7	— symétriques	2 3
<i>Dédoubllement d'une loi de composition interne..</i>	3 2	<i>Endomorphisme</i>	4 4
<i>Degré d'un groupe de permutations</i>	7 1	<i>Engendré par une partie (idéal)</i>	8 6
<i>Dénominateur</i>	2 9	— — (sous-anneau)	8 4
<i>Dérivé (groupe)</i>	6 8	— — (sous-corps)	9 2
<i>Di-automorphisme</i>	4 1	— — (sous-groupe)	6 2
<i>Di-isomorphisme</i>	4 1	— — (sous-groupe stable)	6 10
<i>Direct (composé)</i>	8 11	<i>Engendrée par une partie (partie stable pour une loi interne)</i>	1 4
— (produit)	6 6	— — (partie stable pour une loi externe)	3 3
<i>Directe (somme)</i>	6 6	— — (partie stable pour une structure algébrique)	4 2
<i>Distingué (sous-groupe)</i>	6 3	<i>Ensemble d'opérateurs</i>	3 1
<i>Distributive (loi)</i>	5 1	— muni d'un groupe d'opérateurs	
<i>Distributivité à gauche</i>	5 1	+ rateurs	7 2
— à droite		<i>Entiers rationnels</i>	2 5
— par rapport à une loi interne		— — négatifs	2 5
— par rapport à l'ensemble de deux lois internes		— — opposés	2 5
— (double)		— — positifs	2 5
<i>Diviseur à droite</i>	8 3	— — strictement négatifs	2 5
— à droite de zéro	8 3	— — strictement positifs	2 5
— à gauche		<i>Équivalentes (suites de composition)</i>	6 14
— à gauche de zéro		<i>Espace homogène</i>	7 6
<i>Domaine d'opérateurs</i>	3 1	— — défini par un sous-groupe	7 6
<i>Double associativité</i>	5 3	<i>Extension d'un corps</i>	9 2
		— de permutations	7 3

§ n°		§ n°
<i>Extension d'un produit de groupes de transformations</i>		<i>Groupe à opérateurs</i> 6 9
— de représentations d'un groupe sur des groupes de transformations	7 3	— — abélien 6 9
— — quotient 6 11		— — semi-simple 6 15
— — simple 6 14		<i>Groupes opposés</i> 6 1
<i>Extérieur (automorphisme)</i>	7 4	<i>Homogène (espace)</i> 7 6
<i>Externe (loi de composition)</i>	3 1	<i>Homologues (structures)</i> 4 1
— (homothétie)	8 2	<i>Homomorphes (structures)</i> .. 4 4
<i>Facteur d'un produit</i>	1 2	<i>Homomorphie (structures en)</i> .. 4 4
<i>Familles semblables</i>	1 2	— (théorème d') 4 4
<i>Fraction</i>	2 9	<i>Homomorphisme d'un anneau</i> 8 8
<i>Fractions (anneau des)</i>	9 4	— d'une structure algébrique 4 4
— (corps des)	9 4	— d'un groupe 6 4
<i>Gauche (corps)</i>	9 1	<i>Homomorphisme canonique</i> d'un anneau sur un anneau quotient ... 8 8
<i>Générateurs d'un idéal (système de)</i>	8 6	— — d'une structure algébrique sur une structure quotient 4 4
<i>Générateurs d'un sous-groupe (système de)</i>	6 2	— — d'un groupe sur un groupe quotient 6 4
<i>Groupe</i>	6 1	<i>Homothétie à droite d'un anneau</i>
— abélien	6 7	— à gauche d'un anneau ... 8 1
— additif des entiers modulo α	6 3	— d'un groupe à opérateurs
— additif des entiers rationnels	6 1	— externe d'un anneau à opérateurs 8 2
— alterné	7 1	<i>Idéal à droite</i>
— commutatif	6 7	— à gauche
— cyclique	6 7	— bilatère
— d'automorphismes d'une structure	7 4	— maximal
— de permutations	7 1	— nul
— des commutateurs	6 8	— principal
— dérivé	6 8	<i>Idempotent</i>
— de transformations	7 1	<i>Impaire (permutation)</i>
— fini	6 1	<i>Imprimitif (groupe)</i>
— imprimitif	7 7	<i>Imprimitivité (classe d')</i> ... 7 7
— infini	6 1	<i>Indice d'un sous-groupe</i> ... 6 3
— intransitif	7 5	<i>Induite (loi externe)</i>
— monogène	6 7	— (loi interne)
— multiplicatif d'un corps	9 1	— (structure algébrique) ... 4 2
— primitif	7 7	<i>Intégrité (anneau d')</i>
— produit	6 5	<i>Intérieur (automorphisme)</i> .. 6 4
— quotient	6 3	<i>Interne (loi de composition)</i> . 1 1
— simple	6 3	<i>Intransitif (groupe)</i>
— symétrique	7 1	<i>Intransitivité (classe d')</i> 7 5
— transitif	7 5	

§ n°		§ n°
<i>Invariant d'un groupe d'opérateurs</i>	7 4	<i>Loi de composition externe</i> — — — distributive par rapport à l'ensemble de deux lois internes .. 5 1
— d'un groupe relatif à des représentations sur des groupes de transformations	7 4	— — — induite 3 3
— (élément) par un opérateur	3 1	— — — partout définie .. 3 1
— (sous-groupe)	6 3	— — — produit 4 5
<i>Invariante (application)</i>	7 4	— — — quotient 4 3
<i>Inverse d'un élément</i>	2 9	<i>Loi de composition interne</i> .. 1 1
<i>Inversible (élément)</i>	2 9	— — — associative 1 3
<i>Inversions (nombre d')</i> d'une permutation	7 1	— — — commutative 1 5
<i>Isomorphie (théorèmes d')</i>	4 4	— — — doublement distributive par rapport à une autre..... 5 1
<i>Isomorphisme canonique</i> d'une partie d'un ensemble muni d'une structure algébrique dans cet ensemble ...	4 4	— — — induite 1 4
— d'un ensemble muni d'une structure algébrique dans un autre	4 4	— — — partout définie... 1 1
— d'un ensemble muni d'une structure algébrique sur un autre.	4 1	— — — produit 4 5
<i>Jordan-Hölder (suite de)</i>	6 14	— — — quotient 4 3
— (théorème de)	6 14	<i>Lois externes permutables</i> ... 5 3
<i>Juxtaposition de deux suites</i>	1 3	<i>Lois internes opposées</i> 1 1
<i>Krull (théorème de)</i>	8 7	<i>Longueur d'un groupe</i> 6 14
<i>Lemme de Zassenhaus</i>	6 14	— d'un mot
<i>Libre (monoïde)</i>	1 3	<i>Maximal (idéal)</i> 8 7
<i>Loi de composition externe</i> ..	3 1	<i>Monogène (groupe)</i>
— — — à droite déduite d'une loi interne....	3 2	<i>Monoïde</i> 1 3
— — — à gauche déduite d'une loi interne ...	3 2	— libre
— — — associative par rapport à une loi interne	5 2	<i>Mot</i> 1 3
— — — distributive à droite	5 1	<i>Multiple à droite</i>
— — — distributive à gauche	5 1	— à gauche
— — — distributive par rapport à une loi interne	5 1	<i>Multiplicatif (groupe)</i> d'un corps
		9 1
		<i>Multiplication</i>
		1 1
		— des entiers modulo α ... 4 3
		— des entiers rationnels... 2 8
		<i>Multiplicativement (loi notée)</i> 1 1
		<i>Négatif (entier rationnel)</i> ... 2 5
		— (nombre rationnel)..... 9 5
		<i>Neutre (élément)</i>
		2 1
		— (opérateur)
		3 1
		<i>Nombre d'inversions</i> d'une permutation
		7 1
		<i>Nombres rationnels</i> 9 5
		— — négatifs
		9 5
		— — positifs
		9 5
		— — strictement négatifs... 9 5
		— — strictement positifs .. 9 5
		<i>Numérateur</i>
		2 9

	§ n°		§ n°
Opérateur	3 1	Produit de structures algébriques.....	4 5
— neutre	3 1	— d'une séquence	1 2
Opérateurs (domaine d')	3 1	Produit direct de sous-groupes	6 6
— (ensemble d')	3 1	Prolongement d'une structure algébrique	4 2
Opposé d'un entier	2 5	— par symétrie d'une loi interne	2 4
— d'un élément	2 9	Quotient (anneau)	8 5
Opposées (lois internes)	1 1	— (groupe)	6 3
Opposés (anneaux)	8 1	— (groupe à opérateurs)	6 11
— (groupes)	6 1	— (loi externe)	4 3
Ordre d'un groupe	6 1	— (loi interne)	4 3
Origine	2 1	— (structure algébrique)	4 3
Paire (permutation)	7 1	Quotients (anneau des)	9 4
Partie stable (pour une loi externe)	3 3	— (corps des)	9 4
— — (pour une loi interne)	1 4	Rationnels (entiers)	2 5
— — (pour une structure algébrique)	4 2	— (nombres)	9 5
Partie stable engendrée par une partie : voir Engendrée (partie stable)		Réalisation d'un groupe	7 2
Partie symétrique	6 1	— transitive d'un groupe	7 6
Partout définie (loi interne)	1 1	Régulier (élément)	2 2
— (loi externe)	3 1	Relation d'équivalence compatible : voir Compatible (relation d'équivalence).	
Permutabilité de deux lois externes	5 3	Représentation	4 4
Permutables (éléments)	1 5	— biunivoque associée	4 4
— (lois externes)	5 3	— canonique sur une structure quotient	4 4
Permutation impaire	7 1	— canonique d'un produit de groupes de transformations dans un groupe symétrique	
— paire	7 1	— d'un groupe	6 4
Plus fine (suite de composition)	6 14	— d'un groupe à opérateurs	6 12
Plus grand commun diviseur (p.g.c.d.) de deux entiers	8 6	— d'un anneau	8 8
Plus petit commun multiple (p.p.c.m.) de deux entiers	8 6	Reste d'un entier modulo a	4 3
Poly-automorphisme	4 1	Restriction du domaine d'opérateurs d'une loi externe	3 3
Poly-isomorphisme	4 1	Schreier (théorème de)	6 14
Positifs (entiers rationnels)	2 5	Semblables (familles)	1 2
— (nombres rationnels)	9 5	— (séquences)	1 2
Primitif (groupe)	7 7	Semi-simple (groupe à opérateurs)	6 15
Principal (idéal)	8 6	Séquence	1 2
Produit d'anneaux	8 10		
— de deux éléments	1 1		
— de groupes	6 5		
— de lois externes	4 5		
— de lois internes	4 5		

	§ n°		§ n°
Séquences semblables	1 2	Suite de composition	6 14
Signature d'une permutation	7 1	— — plus fine qu'une autre	6 14
Signe d'un nombre rationnel	9 5	Suite de Jordan-Hölder	6 14
Simple (groupe)	6 3	Suites de composition équivalentes	6 14
— (groupe à opérateurs)	6 14	Sur-corps	9 2
Somme de deux éléments	1 1	Symétrie d'un groupe	6 1
— d'idéaux	8 6	Symétrique d'un élément	2 3
— d'une séquence	1 2	Symétrique (application)	6 1
Somme directe de sous-anneaux	8 11	— (partie)	6 1
— — de sous-groupes	6 6	— (groupe)	7 1
Sous-anneau	8 4	Symétrisable (élément)	2 3
— engendré par une partie	8 4	Symétrisation d'une loi interne	2 4
Sous-corps	9 2	— (théorème de)	2 4
— engendré par une partie	9 2	Symétrisé (ensemble)	2 4
Sous-groupe	6 2	Système de générateurs d'un idéal	8 6
— distingué	6 3	— — d'un sous-groupe	6 2
— engendré par une partie	6 2	Terme d'une somme	1 2
— invariant	6 3	Théorème d'associativité	1 3
— stable	6 10	— de commutativité	1 5
— stable engendré par une partie	6 10	— de Jordan-Hölder	6 14
Sous-jacente (structure algébrique)	4 1	— de Krull	8 7
Stable (partie) : voir Partie stable		— de Schreier	6 14
Stable (sous-groupe)	6 10	— de symétrisation	2 4
Strictement négatifs (entiers rationnels)	2 5	— d'homomorphie	4 4
— — (nombres rationnels)	9 5	Théorèmes d'isomorphie	4 4
Strictement positifs (entiers rationnels)	2 5	Transitif (groupe)	7 5
— — (nombres rationnels)	9 5	Transitive (réalisation)	7 6
Structure algébrique	4 1	Translation à droite	2 2
— — induite	4 2	— à gauche	2 2
— — produit	4 5	Transposition	7 1
— — quotient	4 3	Unité (élément)	2 1
— — sous-jacente	4 1	— (élément) d'un anneau	8 1
Structures algébriques homologues	4 1	Valeur absolue d'un nombre rationnel	9 5
Structure d'anneau	8 1	Zassenhaus (lemme de)	6 14
— de groupe	6 1	Zéro	2 1

RECTIFICATIONS AU FASCICULE IV

- P. 17, ligne 16 du bas, lire : « conques ; $(m, n, 1)$, m et n quelconques ; $(m, 2, 2)$, où m est quelconque. »
 P. 18, ligne 9 du haut, au lieu de : l'ensemble des parties de la diagonale Δ , lire : l'ensemble formé de la partie vide de $E \times E$ et de la diagonale Δ .
 P. 28, ligne 5 du bas, au lieu de : chap. V, lire : chap. VI.
 P. 29, Note de bas de page, ligne 2, au lieu de : chap. V, lire : chap. VI.
 P. 32, ligne 8 du bas, lire :

$$x + y + (-z), \quad x + (-y) + (-z), \quad x + (-y) + z + (-t)$$

- P. 58, remplacer les lignes 15 à 18 du haut, depuis : « Dans les mêmes conditions.. » par le texte suivant :

En supposant toujours la multiplication associative (mais non plus nécessairement commutative), soit A un ensemble fini totalement ordonné, $(S_\alpha)_{\alpha \in A}$ une séquence dont les éléments sont des familles finies $S_\alpha = (x_{\alpha\lambda})_{\lambda \in L_\alpha}$ d'éléments de E ; on a alors l'identité dite « formule générale de distributivité »....

- P. 58, après la ligne 20 du haut, ajouter :
 Lorsque la multiplication est *commutative*, on déduit de cette formule que, pour m et n entiers > 0 , et pour toute famille finie $(x_i)_{1 \leq i \leq m}$ d'éléments de E , on a

$$(x_1 + x_2 + \cdots + x_m)^n = \sum c_{p_1 p_2 \cdots p_m} x_1^{p_1} x_2^{p_2} \cdots x_m^{p_m}$$

la somme du second membre étant étendue à toutes les suites

$$(p_i)_{1 \leq i \leq m} \text{ de } m \text{ entiers } \geq 0 \text{ tels que } \sum_{i=1}^m p_i = n, \text{ et}$$

$$c_{p_1 p_2 \cdots p_m} = \frac{n!}{p_1! p_2! \cdots p_m!}$$

étant le nombre d'applications de $[1, n]$ sur $[1, m]$, prenant p_k fois la valeur k pour $1 \leq k \leq m$ (Ens., chap. III).

Pour $m = 2$, la formule précédente prend le nom de *formule du binôme*, et s'écrit

$$(x + y)^n = \sum_{p=0}^n \binom{n}{p} x^p y^{n-p}$$

les coefficients $\binom{n}{p} = \frac{n!}{p! (n-p)!}$ étant appelés *coefficients binomiaux*.

- P. 64, ligne 9 du bas, au lieu de : est un *monoïde*, lire : est un *monoïde non vide*.

- P. 64, ligne 11 du haut, avant « Montrer que... », ajouter : On suppose en outre que la relation $n \cdot x = 0$ (n entier quelconque $\neq 0$) entraîne $x = 0$ dans E.
 ligne 15 du haut, au lieu de : $1 \leq q \leq p$, lire : $1 \leq q < p$.
- P. 81, ligne 15 du haut, au lieu de : un groupe stable, lire : un sous-groupe stable.
- P. 89, ligne 17 du haut, au lieu de : H_i , lire : H_{i+1} .
- P. 91, lignes 1 et 2 du bas, au lieu de : « Pour que G soit isomorphe au produit $H \times (G/H)$ », lire : « Pour qu'il existe un sous-groupe K de G tel que G soit produit direct de H et de K ».
- P. 96, ligne 23 du haut, au lieu de : « si $G_{e,e}$ n'est pas vide, c'est... », lire : « $G_{e,e}$ est... ».
- P. 103, ligne 10 du haut, au lieu de : convenable, lire : invariante.
- P. 104, avant la ligne 9 du bas, ajouter : Pour tout $\gamma \in G$, l'ensemble des opérateurs $\alpha \in G$ qui laissent invariants tous les éléments de γA est le sous-groupe $\gamma H \gamma^{-1}$, la relation $\alpha \gamma x = \gamma x$ équivalant à $(\gamma^{-1} \alpha \gamma)x = x$.
- P. 104, ligne 2 de la note (*), au lieu de : chap. IV et VI, lire : chap. III et V.
- P. 106, lignes 5 et 6 du bas, au lieu de : « les restrictions à A des permutations du groupe Γ constituent », lire : « l'ensemble des restrictions à A des permutations du groupe Γ est ».
- P. 115, ligne 10 du haut, au lieu de : suffisante, lire : nécessaire.
- P. 120, après la ligne 2 du haut, ajouter : « on dit encore que a est divisible à droite (resp. à gauche) par b . »
- P. 127, ligne 16 du bas, au lieu de : chap. V, lire : chap. VI.
- P. 129, ligne 16 du haut, au lieu de : chap. II, lire : chap. V.
- P. 135, ligne 23, au lieu de : $B' + A \cdot B' \cdot A$, lire : $B' + A \cdot B' + B' \cdot A + A \cdot B' \cdot A$.
- P. 136, ligne 16 du haut, au lieu de : tout élément, lire : tout élément $\neq 0$.
- P. 137, ligne 1 du haut, au lieu de : élément unité, lire : élément unité e .
- P. 140, ligne 14 du haut, au lieu de : chap. IV et V, lire : chap. IV et VIII.
- P. 143, ligne 16 du haut, au lieu de : représentation, lire : expression.
- P. 146, ligne 11, au lieu de : Montrer que f , lire : Montrer que f ou $-f$.
- P. 152, ligne 13 du haut, au lieu de : chap. VI, lire : chap. V.
- P. 152, ligne 2 du bas, au lieu de : chap. V, lire : chap. VIII.
- P. 153, ligne 5 du bas, au lieu de : chapitre V, lire : chapitre VI.
- P. 154, ligne 3 du haut, au lieu de : chap. VI, lire : chap. V.
- P. 154, ligne 18 du haut, au lieu de chap. VII, lire : II^e partie.
- P. 154, note (**), ligne 4, au lieu de : chapitre VI, lire : chapitre V.
- P. 156, ligne 3 du haut, au lieu de : chap. II, V et VI, lire : chap. II, V et VII.
- P. 156, ligne 4 du haut, au lieu de : chap. II, III et VII, lire : chap. II et III.
- P. 156, ligne 20 du bas, au lieu de : chap. VII et VIII, lire : chap. VIII.
- P. 160, première colonne, avant la ligne 2 du bas, ajouter :
Associée (représentation biunivoque) 4 4.
- P. 160, deuxième colonne, ligne 1 du haut, au lieu de : *Antomorphisme*, lire : *Automorphisme*.
- P. 164, première colonne, après la ligne 9, ajouter : *Ordre d'un élément d'un groupe 6 7.*

TABLE DES MATIÈRES

INTRODUCTION	I-IV
CHAPITRE I. — <i>Structures algébriques</i>	1
§ 1. Lois de composition internes ; associativité ; commutativité....	1
§ 2. Élément neutre ; éléments réguliers ; éléments symétriques	18
§ 3. Lois de composition externes	37
§ 4. Structures algébriques	41
§ 5. Relations entre lois de composition	56
§ 6. Groupes et groupes à opérateurs	64
§ 7. Groupes de transformations	98
§ 8. Anneaux et anneaux à opérateurs	115
§ 9. Corps	139
 Note historique	149
Index des notations	159
Index terminologique	160
Définitions et axiomes du chapitre I	Dépliant I
Lexique des principales notations d'une loi de composition interne.....	Dépliant II

DÉFINITIONS ET AXIOMES DU CHAPITRE I

Lois de composition internes (§§ 1 et 2)

Loi associative :

Une loi de composition interne τ entre éléments de E , partout définie, est associative si l'on a

$$(x \tau y) \tau z = x \tau (y \tau z)$$

quels que soient x, y, z de E .

Eléments permutables :

Deux éléments x et y d'un ensemble E muni d'une loi interne τ sont permutables si $x \tau y$ et $y \tau x$ sont définis et égaux entre eux.

Loi commutative :

Une loi de composition interne τ entre éléments de E est commutative si, pour tout couple (x, y) d'éléments de E tel que $x \tau y$ soit défini, $y \tau x$ est aussi défini et égal à $x \tau y$.

Partie stable :

Une partie A d'un ensemble E muni d'une loi de composition interne est stable si le composé de deux éléments de A , chaque fois qu'il est défini, appartient à A .

Elément neutre :

Un élément e d'un ensemble E muni d'une loi interne τ est élément neutre pour cette loi si, pour tout $x \in E$, $e \tau x$ et $x \tau e$ sont définis et égaux à x . Pour une loi notée multiplicativement, l'élément neutre prend souvent le nom d'*élément unité* (ou *unité*) ; pour une loi notée additivement, le nom de *zéro*, ou *origine*.

Elément régulier :

Pour une loi interne τ partout définie sur un ensemble E , un élément $a \in E$ est régulier si chacune des relations $a \tau x = a \tau y$, $x \tau a = y \tau a$ entraîne $x = y$.

Eléments symétriques :

Pour une loi interne τ sur un ensemble E , admettant un élément neutre e , deux éléments x et x' sont symétriques si $x \tau x'$ et $x' \tau x$ sont définis et égaux à e . Pour une loi notée multiplicativement, deux éléments symétriques prennent souvent le nom d'*éléments inverses* ; pour une loi notée additivement, le nom d'*éléments opposés*.

DÉFINITIONS ET AXIOMES DU CHAPITRE I

Lois de composition externes (§ 3)

Partie stable :

Une partie A d'un ensemble E muni d'une loi de composition externe \perp est stable si le composé $\alpha \perp x$ d'un opérateur α et d'un élément $x \in A$ appartient à A chaque fois que ce composé est défini.

Structures algébriques (§ 4)

Définition d'une représentation :

Une application f d'un ensemble E muni d'une structure algébrique, dans un ensemble F muni d'une structure algébrique homologue, est une *représentation* si, les lois de composition correspondantes étant notées du même signe :

1^o pour chaque loi interne τ , $f(x) \tau f(y)$ est défini chaque fois que $x \tau y$ est défini, et satisfait à

$$f(x \tau y) = f(x) \tau f(y);$$

2^o pour chaque loi externe \perp , $\alpha \perp f(x)$ est défini chaque fois que $\alpha \perp x$ est défini, et satisfait à

$$f(\alpha \perp x) = \alpha \perp f(x).$$

Homomorphisme ; endomorphisme :

Une représentation f de E dans F s'appelle aussi un *homomorphisme* de E dans F lorsque les lois de composition qui définissent la structure de E sont partout définies ; on dit que c'est un homomorphisme de E sur F si $f(E) = F$. Un homomorphisme de E dans E s'appelle un *endomorphisme* de E.

Relations entre lois de composition (§ 5)

Distributivité d'une loi externe \perp (partout définie, entre opérateurs $\alpha \in \Omega$ et éléments de E) par rapport à une loi interne τ (entre éléments de E) :

La loi \perp est distributive par rapport à la loi τ si, chaque fois que $x \tau y$ est défini, le composé $(\alpha \perp x) \tau (\alpha \perp y)$ est défini pour tout $\alpha \in \Omega$ et satisfait à

$$\alpha \perp (x \tau y) = (\alpha \perp x) \tau (\alpha \perp y).$$

Double distributivité d'une loi interne \perp (partout définie sur E) par rapport à une loi interne τ (définie sur E) :

La loi \perp est doublement distributive par rapport à la loi τ si, chaque fois que $y \perp z$ est défini, $(x \perp y) \tau (x \perp z)$ et $(y \perp x) \tau (z \perp x)$ sont définis et satisfaisent à

$$\begin{aligned} x \perp (y \tau z) &= (x \perp y) \tau (x \perp z) \\ (y \tau z) \perp x &= (y \perp x) \tau (z \perp x). \end{aligned}$$

Groupes (§ 6)

Axiomes d'un groupe :

Un groupe est un ensemble muni d'une loi de composition interne partout définie qui satisfait aux conditions suivantes :

1) elle est associative ;

DÉFINITIONS ET AXIOMES DU CHAPITRE I

Groupe abélien :

Un groupe est dit *abélien* si sa loi de composition est *commutative*.

Sous-groupe :

Une partie H d'un groupe G (noté multiplicativement) est un sous-groupe de G si les relations $x \in H$ et $y \in H$ entraînent $xy^{-1} \in H$.

Sous-groupe distingué :

Un sous-groupe H d'un groupe G est distingué si $xHx^{-1} = H$ pour tout $x \in G$.

Groupe à opérateurs :

On appelle groupe à opérateurs un groupe muni d'une ou plusieurs lois externes, distributives par rapport à la loi (interne) du groupe.

Anneaux et corps (§§ 8 et 9)

Axiomes d'un anneau :

Un anneau est un ensemble A muni de deux lois de composition internes partout définies et satisfaisant aux conditions suivantes :

1^o la première loi (notée en général additivement et appelée *addition*) est une loi de groupe abélien ;

2^o la deuxième loi (notée en général multiplicativement et appelée *multiplication*) est associative, et doublement distributive par rapport à l'addition.

Un anneau est dit *commutatif* si la multiplication est commutative.

Anneau à opérateurs :

On appelle anneau à opérateurs un anneau A muni d'une ou de plusieurs lois externes, distributives par rapport à l'addition dans A, et telles en outre que, si l'on note $(\alpha, x) \rightarrow ax$ l'une quelconque de ces lois, on ait identiquement

$$\alpha(xy) = (\alpha x)y = x(\alpha y).$$

Sous-anneau :

Une partie B d'un anneau à opérateurs A est un sous-anneau de A si B est un sous-groupe du groupe additif de A, stable pour la multiplication et pour les lois externes.

Anneau d'intégrité :

Un anneau d'intégrité est un anneau *commutatif* sans « diviseur de zéro » (c'est-à-dire tel que la relation $ab = 0$ entraîne $a = 0$ ou $b = 0$).

Idéaux dans un anneau :

Dans un anneau à opérateurs A, une partie α de A est un *idéal à gauche* (resp. à droite) si α est un sous-groupe du groupe additif de A, stable pour les lois externes, et si en outre $z \alpha \subseteq \alpha$ (resp. $\alpha z \subseteq \alpha$) pour tout $z \in A$. Un *idéal bilatère* est une partie de A qui est à la fois idéal à gauche et idéal à droite.

Axiomes d'un corps :

Un corps est un anneau tel que l'ensemble des éléments $\neq 0$ forme un

LEXIQUE DES PRINCIPALES NOTATIONS
D'UNE LOI DE COMPOSITION INTERNE

NOTATION GÉNÉRALE	NOTATION MULTIPLICATIVE	NOTATION ADDITIVE
<i>Compose</i> $x \tau y$ de x et de y	<i>Produit</i> $x \cdot y$ (ou xy) de x et de y	<i>Somme</i> $x + y$ de x et de y
<i>Compose</i> $\prod_{\alpha \in A} x_\alpha$ d'une séquence $(x_\alpha)_{\alpha \in A}$	<i>Produit</i> $\prod_{\alpha \in A} x_\alpha$ d'une séquence $(x_\alpha)_{\alpha \in A}$	<i>Somme</i> $\sum_{\alpha \in A} x_\alpha$ d'une séquence $(x_\alpha)_{\alpha \in A}$
$\tau^m x$ (m entier > 0)	x^m	$m \cdot x$ (ou mx)
<i>Élément neutre</i> e	<i>Élément unité</i> (parfois noté 1)	<i>Zéro</i> (ou <i>origine</i>) noté 0.
$\tau^e x (= e)$	$x^0 (= 1)$	$0 \cdot x (= 0)$
<i>Éléments symétriques</i>	<i>Éléments inverses</i>	<i>Éléments opposés</i>
$\tau^{-1} x$	$x^{-1} \left(\frac{1}{x} \right)$ lorsque la multiplication est <i>commutative</i>	$-x$
$x \tau (\tau^{-1} y)$	$xy^{-1} \left(\frac{x}{y} \right)$ lorsque la multiplication est <i>commutative</i>	$x - y$
$\tau^a x (a \in \mathbb{Z})$	x^a	$a \cdot x$ (ou ax)