

STRUCTURES ALGÈBRIQUES *

1. INTRODUCTION

Depuis quelques décades, nous assistons à une véritable invasion des Mathématiques par l'Algèbre. En particulier, sous l'impulsion d'Emmy NOETHER (dans les années 1920 et suivantes), les mathématiciens ont pris de plus en plus nettement conscience du rôle joué par les notions fondamentales de l'Algèbre dans presque toutes les branches de la Mathématique ; et, mieux, de la possibilité d'utiliser au profit de l'analyse, par exemple, des théorèmes plus ou moins profonds d'algèbre pure. Cette utilisation, certes, n'est pas nouvelle (qu'on songe notamment au développement de la théorie de Lie à la fin du siècle dernier) ; ce qui est surtout nouveau, c'est la conscience qu'on en a.

Avec l'algébrisation actuelle des Mathématiques, nul chercheur ne peut plus se permettre d'ignorer un outil devenu indispensable : l'Algèbre moderne. En retour, l'Algèbre profite de cette situation : car la Topologie, l'Analyse lui posent constamment de nouveaux problèmes et suscitent des développements qu'on aurait à peine pu concevoir il y a quelque vingt ans.

L'enseignement des Mathématiques dans les classes secondaires doit se ressentir d'une telle évolution, tout au moins dans les classes terminales ; moins sans doute dans le sens d'une modification des programmes que dans la façon de présenter des théories classiques, en tenant compte d'une nouvelle optique. C'est sans doute la raison pour laquelle la Société Mathématique a pris l'initiative de cette série de conférences.

Mais qu'est-ce que l'Algèbre ? Il n'est pas facile, en quelques mots, d'en donner une définition qui la situe d'une manière précise par rapport au reste des Mathématiques. Certes, à chaque époque du développement scientifique, chaque mathématicien possède le sentiment assez net de ce qui est de l'Algèbre et de ce qui n'en est pas. Mais toute définition explicite court le risque de devenir périmée ou trop étroite au cours de l'évolution ultérieure de la science : en effet, il est impossible d'assigner à l'avance à l'Algèbre des limites à ne pas franchir (pas plus du reste qu'à toute branche de la science), car on ne connaît pas de moyen de prévoir les domaines nouveaux qui s'offriront à l'exploration.

En gros, on peut dire qu'en Algèbre, on étudie certaines *opérations* sur les éléments d'un ou plusieurs ensembles, sans avoir égard à la nature des éléments eux-mêmes. Tout ce que l'on aura pu dire d'un ensemble muni de certaines opérations pourra s'appliquer aussi bien à tout autre ensemble, pourvu qu'il lui soit *isomorphe* (on reviendra plus loin sur la notion d'isomorphie). Cette conception de l'Algèbre est celle qui prévaut depuis un siècle peut-être ; cependant, elle risque d'être dépas-

(*) Cette Conférence, prononcée le 9 février 1956 à l'Institut Henri-Poincaré, a ouvert le cycle de conférences sur l'Algèbre, organisé par la Société Mathématique de France, en accord avec l'A.P.M., à l'intention spéciale des professeurs de Mathématiques.

sée aujourd'hui, à la suite de progrès tout récents qui obligeront sans doute à élargir un cadre devenu trop étroit. Nous nous bornerons ici à illustrer sur quelques exemples la conception que j'appellerai classique, laissant à d'autres le soin, dans quelques dizaines d'années, de vous exposer les points de vue nouveaux qu'ouvrent certains développements actuels.

2. LA NOTION D'OPÉRATION

On rencontre cette notion dès les débuts de l'Arithmétique. Une opération est une loi qui, à deux éléments a et b , associe un élément c (qu'on appelle parfois la somme de a et de b , parfois leur produit, d'autres fois encore d'un autre nom). Au fond, il n'y a là rien d'autre que la notion de *fonction* : étant donnés trois ensembles A , B , C , on considère l'ensemble des couples (a, b) formés d'un élément $a \in A$ et d'un élément $b \in B$, ensemble qu'on appelle l'*ensemble-produit* de A et de B , et qu'on note $A \times B$; une opération sera alors simplement une fonction définie sur l'ensemble $A \times B$, et prenant ses valeurs dans l'ensemble C ; c'est, comme on dit aussi, une *application* de $A \times B$ dans C .

Un cas important est celui où les trois ensembles A , B , C sont les mêmes : on considère donc une application $f : A \times A \rightarrow A$. Une telle fonction s'appelle une *loi de composition interne*. Lorsque l'on suppose simplement $B = C$, on obtient ce qu'on appelle une *loi de composition externe* : c'est une application f de $A \times B$ dans B . Dans ce cas, chaque élément $a \in A$ définit une application de B dans B , à savoir celle qui à b associe $f(a, b)$; or, une application de B dans B , c'est ce qu'on appelle aussi une *transformation* de B . Ainsi, une loi externe associe à chaque élément de A une transformation de B ; l'ensemble A prend alors parfois le nom de *domaine d'opérateurs*. Et l'on dit que A *opère dans* B .

Voici des exemples de lois de composition : l'addition des nombres entiers associe à un couple d'entiers un entier ; de même, la multiplication des entiers ; ce sont des lois de composition internes dans l'ensemble des entiers. On peut en dire autant de l'addition et de la multiplication des fractions, ou des nombres réels, ou des nombres complexes, ou des polynômes à une ou plusieurs variables. En Géométrie élémentaire, on connaît la notion de *déplacement* : on sait que si on effectue successivement un déplacement a et un déplacement b , ce qu'on obtient est un déplacement c , qu'on appelle parfois le produit (ou le composé) de a et b ; ainsi, à un couple (a, b) de déplacements, on associe un déplacement c . Ceci est une loi de composition dans l'ensemble des déplacements.

Voici d'autres exemples : soient X et Y deux sous-ensembles d'un même ensemble E ; leur *intersection* $X \cap Y$ se compose des éléments de E qui appartiennent à la fois à X et à Y ; leur *réunion* $X \cup Y$ se compose des éléments de E qui appartiennent à l'un au moins des ensembles X et Y ; la loi qui, au couple (X, Y) , associe l'intersection $X \cap Y$, est une loi de composition interne dans l'ensemble A de tous les sous-ensembles de E ; de même, la loi qui, à X et Y , associe $X \cap Y$, est une loi de composition dans A .

Dans un autre ordre d'idées, considérons deux entiers a et b , et leur plus grand commun diviseur $d(a, b)$; l'application $(a, b) \rightarrow d(a, b)$ est une loi de composition dans l'ensemble des entiers. De même pour le plus petit commun multiple.

Donnons encore l'exemple des *mots*. Soit un ensemble E ; on appelle « mot » une suite finie $uvwxy$ d'éléments de E , distincts ou non ; il y a même un mot « vide », celui défini par une suite vide. Etant donnés deux mots $uvwxy$ et $pqrs$, on définit un nouveau mot en les écrivant à la suite l'un de l'autre : $uvwxyzpqrs$. Ceci est une loi de composition interne dans l'ensemble A des mots formés d'éléments de E . Si on compose un mot uvw avec le mot vide, on retrouve le même mot uvw .

Tous les exemples précédents sont des exemples de lois *internes*. Voici maintenant deux exemples de lois *externes*. Considérons, dans le plan (ou dans l'espace) de la géométrie élémentaire, un point O ; à chaque nombre réel t , associons l'homothétie de centre O et de rapport t : c'est une transformation. Nous avons ici une loi de composition externe dont le domaine d'opérateurs A est l'ensemble des nombres réels t , et pour lequel l'ensemble B est le plan (ou l'espace) de la géométrie.

Considérons encore les « figures » de l'espace (par exemple, les triangles) ; un déplacement transforme une figure dans une figure. Donc, si nous prenons pour A l'ensemble des déplacements, et pour B l'ensemble des figures de l'espace, nous avons une loi de composition externe dont le domaine d'opérateurs est l'ensemble des déplacements.

Dans ce qui suit, nous nous bornerons presque exclusivement à des lois de composition internes.

3. PROPRIÉTÉS DIVERSES POUR UNE LOI DE COMPOSITION INTERNE

Associativité : Une loi de composition, que nous noterons multiplicativement par exemple (ab) désignant le composé de a et b , est *associative* si, quels que soient a, b, c , on a $(ab)c = a(bc)$.

Toutes les lois internes que nous avons données en exemple sont associatives. Il est facile de donner un exemple de loi non associative : à chaque couple (a, b) de nombres réels, associons leur demi-somme $(a + b)/2$; on vérifie tout de suite que cette loi n'est pas associative.

Si une loi est associative, on peut définir le composé d'une suite finie quelconque d'éléments $a_1, \dots, a_n$, et démontrer un théorème général d'associativité : par exemple, on a :

$$(ab)(cdef)g = (abc)(de)(fg).$$

Commutativité : Une loi interne (notée multiplicativement pour fixer les idées) est *commutative* si l'on a : $ab = ba$, quels que soient a et b . Dans les exemples donnés plus haut, l'addition et la multiplication des nombres réels ou complexes, des polynômes, sont des lois commutatives ; de même, l'opération de réunion et d'intersection des ensembles est commutative ; la loi qui, à deux entiers, associe leur p.g.c.d. ou leur p.p.c.m., est commutative. Par contre, la composition des déplacements en géométrie n'est pas commutative ; la composition des « mots » n'est pas commutative.

Ainsi, il existe des lois associatives et non commutatives. Il y a

aussi des lois commutatives qui ne sont pas associatives, par exemple celle qui associe à deux nombres réels a et b leur demi-somme.

Lorsqu'une loi est à la fois commutative et associative, on peut définir le composé de n'importe quelle famille d'éléments, sans qu'il soit besoin de préciser dans quel ordre on les range.

Élément neutre : Étant donné une loi interne (notée multiplicativement pour fixer les idées), on appelle élément neutre un élément e tel que $ae = a$, $ea = a$ pour tout élément a . Il n'est pas certain qu'un tel élément existe ; mais, *s'il en existe un, il est unique* : car si e et e' sont deux éléments neutres, on a : $e = ee' = e'$.

Éléments inverses : Considérons une loi interne avec élément neutre e . On dit que a et b sont *inverses* si : $ab = ba = e$.

Si a possède au moins un inverse, et si la loi est associative, alors l'inverse de a est *unique* ; car si b et b' sont des inverses de a , on a :

$$b = be = b(ab') = (ba)b' = eb' = b'.$$

Lorsque la loi considérée est notée additivement (ce qui n'a lieu d'habitude que lorsque cette loi est commutative), on note généralement 0 (zéro) l'élément neutre, s'il existe ; on a donc :

$$a + 0 = 0 + a = a.$$

Dans ce cas, on dit « opposé » au lieu d'« inverse » : b et a sont opposés si $a + b = 0$.

4. STRUCTURE ALGÈBRIQUE DÉFINIE PAR UNE OU PLUSIEURS LOIS DE COMPOSITION

Soit E un ensemble. Une structure algébrique est définie sur E par la donnée d'une ou de plusieurs lois de composition. On donne un même nom à toutes les structures algébriques définies (sur n'importe quel ensemble) par un même nombre de lois satisfaisant à certaines conditions explicitement énumérées. Montrons cela sur des exemples.

Groupe : Une structure de groupe, sur un ensemble E , est définie par la donnée d'une seule loi de composition, qu'on astreint à satisfaire aux conditions (ou « axiomes ») qui vont être énumérées :

Axiome 1 : la loi est associative ;

Axiome 2 : il existe un élément neutre ;

Axiome 3 : chaque élément possède un inverse.

On dit alors que E , muni de cette loi de composition, est un *groupe*.

Par exemple, l'addition des entiers (positifs, négatifs ou nuls) est une loi de groupe ; il en est de même de l'addition des nombres réels, des nombres complexes, de l'ensemble des déplacements muni de la loi de composition qui a été explicitée plus haut. La multiplication des nombres réels ou complexes différents de zéro est une loi de groupe ; par contre, la multiplication des entiers positifs n'est pas une loi de groupe, car un entier n'a pas en général d'inverse. La loi d'intersection ou de réunion des ensembles n'est pas une loi de groupe ; de même, la loi de composition des « mots » n'est pas une loi de groupe.

Un groupe est dit commutatif (ou *abélien*) si sa loi de composition est commutative.

Anneau : Une structure d'anneau, sur un ensemble A , est définie par la donnée de deux lois de composition, appelées *addition* et *multiplication*, ces lois étant astreintes aux axiomes suivants :

Axiome 1 : l'addition est une loi de groupe abélien (on note 0 son élément neutre) ;

Axiome 2 : la multiplication est associative et possède un élément neutre, noté 1 (et appelé élément-unité) ; on suppose $1 \neq 0$;

Axiome 3 : la multiplication est *distributive* par rapport à l'addition :

$$a(b + c) = (ab) + (ac), \quad (b + c)a = (ba) + (ca).$$

Il s'ensuit facilement que le produit de tout élément par 0 est égal à 0 ; donc, 0 n'a pas d'inverse (pour la multiplication).

Un anneau est dit commutatif si sa multiplication est commutative.

Exemples d'anneaux : les entiers ≥ 0 et ≤ 0 ; les nombres réels ou complexes ; les polynômes à coefficients réels ou complexes.

Corps : Un corps est un anneau A qui satisfait à la condition supplémentaire suivante : tout élément $\neq 0$ possède un inverse pour la multiplication. Il revient au même de dire que l'ensemble des éléments non nuls de A forme un groupe pour la multiplication.

Exemples : les entiers ne forment pas un corps, les polynômes ne forment pas un corps ; les nombres rationnels, les nombres réels, les nombres complexes forment un corps.

Bien entendu, il existe toutes sortes de groupes, d'anneaux et de corps. Rappelons que GALOIS a déterminé tous les *corps finis*, c'est-à-dire ayant un nombre fini d'éléments ; le plus simple est le corps ayant seulement deux éléments, 0 et 1 , avec une addition et une multiplication évidentes (on a notamment $1 + 1 = 0$). Pour chaque nombre premier p et chaque exposant entier $f \geq 1$, il y a un corps ayant exactement p^f éléments, et un tel corps est *unique* ; si on note n l'entier p^f , tous les éléments x du corps satisfont à l'équation : $x^n - x = 0$ (ce qui donne l'exemple d'un polynôme à coefficients non nuls et qui s'annule pour toutes les valeurs de la variable ; ce polynôme est de degré n , et la variable ne peut prendre que n valeurs distinctes, puisqu'il n'y a que n éléments dans le corps). Si un entier n n'est pas de la forme p^f , il n'y a pas de corps ayant n éléments.

5. LA NOTION D'ISOMORPHISME

On vient de dire qu'il existe un seul corps ayant p^f éléments. Ce n'est pas tout à fait correct ; ce qui est vrai, c'est que si deux corps ont le même nombre d'éléments, ils sont *isomorphes*. Cela signifie qu'il existe entre les éléments de ces deux corps une correspondance biunivoque qui respecte l'addition et respecte aussi la multiplication. D'une manière générale, on a une notion d'*isomorphisme* pour deux ensembles E et E' munis chacun d'une structure algébrique ; par exemple, un

isomorphisme entre deux groupes est une correspondance biunivoque entre les éléments de ces groupes, qui respecte la loi de composition de chacun d'eux ; c'est ainsi que la fonction exponentielle $f(x) = a^x$ (où a est un nombre > 0 donné, $\neq 1$) est un isomorphisme du groupe additif des nombres réels sur le groupe multiplicatif des nombres positifs $\neq 0$, puisque $f(x + y) = f(x)f(y)$. On a de même la notion d'isomorphisme de deux anneaux A et A' : c'est une correspondance biunivoque qui respecte l'addition, la multiplication, et met en correspondance les éléments unité de A et de A' .

En fait, les êtres algébriques ne sont étudiés qu'à un *isomorphisme près*. C'est dans la nature des choses, puisqu'on ne s'intéresse qu'aux propriétés des opérations étudiées. La question ne se pose pas de savoir si, lorsque deux mathématiciens parlent de l'anneau des entiers, ils parlent des mêmes êtres : car les propriétés qu'ils reconnaissent à cet anneau ont pour conséquence que deux anneaux jouissant de ces propriétés sont nécessairement isomorphes.

6. CONSTRUCTION DE NOUVEAUX ÊTRES ALGÈBRIQUES

A PARTIR D'ÊTRES DÉJÀ DONNÉS : EXEMPLE DE L'ANNEAU DES POLYNÔMES

Nous supposons donné un anneau commutatif A (par exemple, le corps des nombres réels, ou l'anneau des entiers, etc...). On va définir un nouvel anneau, appelé l'*anneau des polynômes* (formels), à une lettre X . Ses éléments s'écrivent symboliquement $\sum_{n \geq 0} a_n X^n$, où les a_n sont

des éléments de A , nuls sauf un nombre fini ; la notation X^n n'a pour le moment aucune signification, c'est une écriture formelle. Ce qui définit un « polynôme », c'est donc simplement la suite des « coefficients » $a_0, a_1, \dots, a_n, \dots$, tous nuls sauf un nombre fini. On définit, dans l'ensemble des polynômes, une addition : la « somme » du polynôme

$\sum_{n \geq 0} a_n X^n$ et du polynôme $\sum_{n \geq 0} b_n X^n$ est, par définition, le polynôme

$\sum_{n \geq 0} (a_n + b_n) X^n$, dont les coefficients sont les sommes $a_n + b_n$. Il est

immédiat que cette addition est commutative et associative, possède un élément neutre 0 (le polynôme dont tous les coefficients sont nuls), et que tout polynôme possède un « opposé » ; autrement dit, l'ensemble des polynômes est un *groupe* pour l'addition.

Appelons *monôme de degré p* un polynôme $\sum_n a_n X^n$ dont tous les coefficients a_n sont nuls pour $n \neq p$; on peut convenir d'écrire simplement $a_p X^p$ pour désigner un tel monôme. On voit que tout polynôme

$\sum_n a_n X^n$ est la somme de ses monômes $a_n X^n$ des différents degrés. Ceci justifie *à posteriori* la notation employée.

La *multiplication* des polynômes se définit comme suit : on définit d'abord le produit d'un monôme $a X^p$ et d'un monôme $b X^q$ comme le monôme $\binom{a \ b}{p \ q} X^{p+q}$ dont le degré est la somme $p + q$ des degrés des deux monômes, et dont le coefficient $\binom{a \ b}{p \ q}$ est le produit des coefficients a et b . Pour définir le produit de deux polynômes $\sum_n a_n X^n$ et $\sum_n b_n X^n$, on décompose chacun d'eux en ses monômes des différents degrés, on fait les produits de ces monômes deux à deux, et on ajoute tous ces produits ; ceci donne la formule suivante : le produit est le polynôme $\sum_{n=0} c_n X^n$, avec $c_n = \sum_{p+q=n} a_p b_q$.

On vérifie que, muni de l'addition et de la multiplication ainsi définies, l'ensemble $A[X]$ des polynômes en X est un anneau commutatif, qui a pour élément unité le monôme de degré 0 dont le coefficient est 1. Ainsi se trouve défini l'anneau des polynômes à une lettre X (et à coefficients dans un anneau commutatif donné A).

X est un pur symbole. Mais on va pouvoir lui substituer des « valeurs ». Etant donné un élément $x \in A$, convenons d'associer à chaque monôme $a_n X^n$ l'élément $a_n x^n$ de A (produit du coefficient a_n par la puissance n -ième de x) ; puis associons à un polynôme $\sum_n a_n X^n$ la somme des $a_n x^n$. On trouve ainsi un élément de A , qu'on appelle la « valeur » du polynôme quand on substitue à X la valeur x . Lorsque x varie dans A , la « valeur » d'un polynôme donné est une *fonction* de x , à valeurs dans A ; ainsi, *chaque polynôme définit une fonction*, mais il faut se garder de confondre dès l'abord le polynôme formel et la fonction qu'il définit.

Choisissons maintenant un élément $\alpha \in A$, et, à chaque polynôme $\sum_n a_n X^n$, associons sa valeur $\sum_n a_n \alpha^n \in A$. On obtient une application f de l'anneau $A[X]$ dans l'anneau A ; cette application associe à la somme de deux polynômes la somme de leurs valeurs, et au produit de deux polynômes le produit de leurs valeurs ; on a précisément choisi une définition de l'addition et de la multiplication des polynômes formels, de manière à assurer cette propriété de l'application f . Ainsi, si u et v désignent deux polynômes, on a :

$$f(u + v) = f(u) + f(v), \quad f(uv) = f(u)f(v), \quad f(1) = 1.$$

Chaque fois qu'on a deux anneaux B et A et une application f de B dans A qui satisfait à ces conditions, on dit que f est un *homomorphisme* de B dans A . La notion d'homomorphisme peut se généraliser à d'autres espèces de structures algébriques ; en gros, un homomorphisme est une application qui respecte les lois de composition.

Pour en revenir aux polynômes, on peut généraliser ce qui précède. Soit A' un anneau contenant A ; on peut substituer à la lettre X une valeur x appartenant à A' (et non plus seulement à A) ; alors, chaque polynôme $\sum_n a_n X^n$ prend une valeur $\sum_n a_n x^n$ qui est un élément de A' . Ceci définit encore un homomorphisme de l'anneau $A[X]$ dans l'anneau A' , pourvu toutefois que x commute avec les éléments de A , c'est-à-dire que l'on ait $ax = xa$ pour tout $a \in A$. Exemple : supposons que A soit le corps des nombres réels ; soit E l'espace vectoriel formé des vecteurs d'origine O dans l'espace à trois dimensions ; les applications linéaires de E dans E forment un anneau (on sait définir la somme de deux applications linéaires ; et on prend comme produit de deux applications linéaires celle qu'on obtient en les composant) ; cet anneau A' contient l'anneau A de toutes les homothéties de centre O , anneau qu'on identifie au corps des scalaires. Cela étant, si, dans un polynôme $\sum_n a_n X^n$ à coefficients réels, on substitue à X une application linéaire x de E dans E , on trouve $\sum_n a_n x^n$ qui est encore une application linéaire de E dans E . Cette loi qui à chaque polynôme associe une application linéaire est d'une grande importance dans l'étude des transformations linéaires d'un espace vectoriel. On voit sur cet exemple l'intérêt que l'on retire de la notion de polynôme formel, qui permet de substituer à la « variable » X des êtres autres que les éléments de l'anneau des coefficients. Un autre exemple serait fourni par la substitution à X d'opérateurs différentiels, tels qu'ils se présentent dans la théorie des équations différentielles linéaires.

7. STRUCTURE-QUOTIENT

Dans la construction de nouvelles structures algébriques à partir de structures déjà connues (par exemple : construction du corps des nombres rationnels à partir de l'anneau des entiers, ou du corps des nombres complexes à partir du corps des nombres réels), on a souvent besoin de la notion de *relation d'équivalence*. On dit qu'une relation $R(x, y)$ entre éléments x et y d'un ensemble E est une relation d'équivalence si :

- 1° $R(x, x)$ est toujours vraie (« réflexivité ») ;
- 2° $R(x, y)$ entraîne $R(y, x)$ (« symétrie ») ;
- 3° $R(x, y)$ et $R(y, z)$ entraînent $R(x, z)$ (« transitivité »).

Voici des exemples de relation d'équivalence qui se présentent en Algèbre :

1) Soit m un entier donné ; la relation entre deux entiers x et y , qui s'écrit :

la différence $x - y$ est divisible par m ,
est une relation d'équivalence.

2) Plus généralement, soit G un groupe noté multiplicativement (on note x^{-1} l'inverse d'un élément x) ; soit H un sous-groupe de G , c'est-à-dire un sous-ensemble qui contient l'élément neutre e , et est tel

que $x \in H$ et $y \in H$ entraînent $x^{-1}y \in H$. La relation $x^{-1}y \in H$ entre éléments x et y de G est une relation d'équivalence dans G . Le cas de l'exemple 1 est celui où G est le groupe additif des entiers ≥ 0 ou ≤ 0 , et où H est le sous-groupe formé des multiples de m (on utilise alors la notation additive pour la loi de composition).

3) Soient (a, b) et (a', b') deux couples d'entiers tels que $b \neq 0$, $b' \neq 0$. Convenons de dire qu'ils sont équivalents si $ab' = a'b$. Il faut vérifier que ceci est bien une relation d'équivalence ; il est évident que cette relation est réflexive et symétrique, et tout revient à montrer qu'elle est transitive. Soient donc trois couples (a, b) , (a', b') , (a'', b'') , tels que $ab' = a'b$, $a'b'' = a''b'$; il s'agit de prouver que $ab'' = a''b$. Or, multiplions les deux membres de $ab' = a'b$ par b'' , et tenons compte de l'associativité et de la commutativité de la multiplication : $ab'b'' = a'bb'' = ba'b''$, ce qui, d'après $a'b'' = a''b'$, est égal à $ba''b'$. Ainsi, $ab'b'' = ba''b'$, d'où $b'(ab'' - a''b) = 0$, et comme $b' \neq 0$ et qu'un produit ne peut être nul que si l'un des facteurs est nul, on conclut bien $ab'' = a''b$.

On observera que la démonstration précédente serait valable, plus généralement, si, au lieu de considérer des couples d'entiers, on prenait des couples (a, b) d'éléments d'un anneau A , avec $b \neq 0$, pourvu que A satisfasse aux conditions suivantes : A est un anneau commutatif tel qu'un produit uv ne puisse être nul sans que u ou v soit nul ; un tel anneau s'appelle un *anneau d'intégrité*.

Exemple d'anneau d'intégrité : Soit A un anneau commutatif, et soit $A[X]$ l'anneau des polynômes à une lettre X . Soient P et Q deux polynômes $\neq 0$, c'est-à-dire dont les coefficients ne sont pas tous nuls ; on a donc $P = a_p X^p + a_{p+1} X^{p+1} + \dots, a_p \neq 0$, et $Q = b_q X^q + b_{q+1} X^{q+1} + \dots, b_q \neq 0$. Alors, le produit PQ est la somme du monôme $\binom{a_p b_q}{p \quad q} X^{p+q}$ et de monômes de degré $> p + q$. Si l'anneau A des coefficients est un anneau d'intégrité (par exemple si A est un corps), le produit $a_p b_q$ est $\neq 0$, donc le polynôme produit PQ n'est pas nul, et on a ainsi prouvé que l'anneau $A[X]$ est aussi un anneau d'intégrité. On peut alors définir une relation d'équivalence entre couples (P, Q) et (P', Q') de polynômes (avec $Q \neq 0, Q' \neq 0$), c'est-à-dire finalement l'équivalence des fractions rationnelles, et ceci sans faire appel à la notion de fonction, mais d'une manière purement formelle qui ramène l'équivalence des fractions rationnelles à l'identité formelle des polynômes.

Revenons maintenant à la théorie générale des relations d'équivalence. Soit R une relation d'équivalence dans un ensemble E ; si x est un élément de E , on appelle *classe* de x l'ensemble de tous les éléments équivalents à x . Les conditions 1°, 2° et 3° montrent que x appartient à la classe de x , et que si x et y sont deux éléments de E , les classes de x et de y sont ou bien identiques, ou bien sans élément commun. On note E/R l'ensemble de toutes les classes, qu'on appelle aussi l'ensemble-quo-

tient de E par la relation d'équivalence R ; on dit aussi que E/R s'obtient en *identifiant* les éléments de E équivalents suivant R .

Reprenons alors les exemples 1), 2), 3) de relations d'équivalence donnés ci-dessus. Dans le cas 1), une classe d'équivalence s'appelle un *entier modulo m* ; l'ensemble-quotient s'appelle l'ensemble des entiers modulo m . Dans le cas 2), une classe d'équivalence s'appelle une classe de G suivant le sous-groupe H ; la classe d'un $x \in G$ se compose des éléments xu , où u parcourt H ; on la note xH . Dans le cas 3), une classe d'équivalence s'appelle précisément une *fraction* (ou « fraction rationnelle » si A est l'anneau des polynômes).

8. LOI DE COMPOSITION COMPATIBLE AVEC UNE RELATION D'ÉQUIVALENCE

Soit R une relation d'équivalence dans un ensemble E ; supposons donnée une loi de composition interne dans E (notée multiplicativement pour fixer les idées). Si la classe d'équivalence du composé xy ne dépend que des classes de x et de y , on obtient une loi de composition dans l'ensemble E/R des classes.

Exemples : Soient x et y deux entiers, et considérons leur somme $x + y$; la classe de $x + y$ modulo m ne change pas si on remplace x par un x' tel que $x - x'$ soit divisible par m ; elle ne change pas non plus si on remplace y par un y' tel que $y - y'$ soit divisible par m . D'où l'*addition des entiers modulo m* ; c'est une loi de composition commutative et associative dans l'ensemble des entiers modulo m . De même, la classe du produit xy ne dépend que des classes de x et de y ; d'où la *multiplication des entiers modulo m* . On vérifie tout de suite que les entiers modulo m forment un *anneau commutatif*. C'est d'ailleurs un *corps* si l'entier m est *premier*.

Soit maintenant à définir la *multiplication des fractions* : dans l'ensemble des couples (a, b) tels que $b \neq 0$, considérons la loi de composition $(a, b)(a', b') = (aa', bb')$; elle est commutative et associative, et admet pour élément neutre $(1, 1)$. On vérifie que la classe d'équivalence de (aa', bb') ne dépend que des classes de (a, b) et de (a', b') ; d'où le produit de deux fractions. La multiplication des fractions est donc commutative et associative ; de plus, chaque élément qui n'est pas dans la classe de $(0, 1)$ possède un inverse, car le produit de (a, b) et (b, a) , pour $a \neq 0$ et $b \neq 0$, est équivalent à $(1, 1)$.

Remarque : Il est facile de définir l'*addition des fractions*, en utilisant une loi de composition, dans l'ensemble des couples (a, b) , qui n'est définie entre (a, b) et (a', b') que si $b = b'$, à savoir : $(a, b) + (a', b) = (a + a', b)$. Cette loi passe au quotient. Alors, muni de l'addition et de la multiplication, l'ensemble des fractions de A est un anneau, et même un *corps* Q ; de plus, si à chaque élément $a \in A$, on associe la fraction, classe de $(a, 1)$, on constate qu'on obtient un isomorphisme f de l'anneau A sur un sous-anneau du corps Q . On dit que f permet d'identifier A à un sous-anneau du corps Q (par exemple, on identifie l'anneau des entiers à un sous-anneau du corps des nombres rationnels, et l'anneau des polynômes en X à un sous-anneau du corps des fractions rationnelles en X).

Dernier exemple : groupe fondamental (ou « groupe de Poincaré ») *d'un espace topologique* X.

Nous ne définirons pas ce qu'on appelle espace topologique, et nous nous contenterons de penser à quelques exemples : espace euclidien ordinaire, surface d'une sphère, surface d'un tore, disque muni de trous, etc...

Précisons la notion de *chemin*, ou *d'arc de courbe*, dans un espace X : c'est défini par la donnée d'une application continue $t \rightarrow f(t)$ du segment $[0,1]$ de la droite numérique, dans l'espace X. On notera que $f(t)$ peut prendre la même valeur pour des valeurs distinctes du « paramètre » t ; cela ne nous gêne pas.

Choisissons désormais un point M de l'espace X ; un *lacet* d'origine M est, par définition, un chemin $t \rightarrow f(t)$ tel que $f(0) = M$ et $f(1) = M$. Dans l'ensemble L des lacets d'origine M, définissons une loi de composition : étant donné un lacet f et un lacet g , nous définissons le lacet h par la condition :

$h(t) = f(2t)$ pour $0 \leq t \leq 1/2$, $h(t) = g(2t - 1)$ pour $1/2 \leq t \leq 1$; autrement dit, on parcourt le lacet f pendant la première moitié du « temps », puis le lacet g pendant la seconde moitié du temps. Cette loi *n'est pas associative*, car si on a trois lacets f, g, h , le lacet $(fg)h$ s'obtient en parcourant f pendant le premier quart du temps, g pendant le second quart, et h pendant la deuxième moitié ; tandis que le lacet $f(gh)$ s'obtient en parcourant f pendant la première moitié du temps, g pendant le troisième quart, et h pendant le dernier quart.

Introduisons maintenant une *relation d'équivalence* R dans l'ensemble L des lacets : un lacet f sera dit équivalent à un lacet g (ou *homotope* à g) s'il existe une *déformation continue* de f dans g , au moyen d'une famille continue de lacets d'origine M ; d'une façon précise, cela signifie qu'il existe une fonction continue $F(t, u)$ de deux variables t et u variant dans $[0,1]$, telle que :

$$F(t, 0) = f(t), \quad F(t, 1) = g(t), \quad F(0, u) = F(1, u) = M.$$

On vérifie que c'est bien une relation d'équivalence, et que la composition des lacets est compatible avec cette relation ; ainsi, dans l'ensemble L/R des *classes de lacets*, on obtient une loi de composition, qui cette fois est associative. On peut montrer que c'est une *loi de groupe*, dont l'élément neutre e est la classe d'équivalence du lacet f tel que $f(t) = M$ pour $0 \leq t \leq 1$ (lacet qui consiste à rester au point M sans en bouger) ; si on a un lacet f , le lacet f' défini par : $f'(t) = f(1 - t)$ (même lacet, mais parcouru « en sens inverse »), jouit de la propriété suivante : les classes de f et de f' sont *inverses* dans le groupe L/R des classes de lacets.

Le groupe qu'on vient de définir (groupe fondamental de l'espace X au point M) joue un rôle important en Topologie, et aussi en théorie des fonctions (fonctions automorphes). On voit sur ce dernier exemple comment les notions de l'Algèbre s'introduisent dans d'autres domaines des Mathématiques.

Henri CARTAN,
Professeur à la Sorbonne.