N. BOURBAKI

ÉLÉMENTS DE MATHÉMATIQUE

N. BOURBAKI

ÉLÉMENTS DE
MATHÉMATIQUE

ALGÈBRE

Chapitres 1 à 3

Springer

2ème ed. Réimpression inchangée de l'édition originale de 1970

ISBN-10 3-540-33849-7 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-33849-9 Springer Berlin Heidelberg New York

Springer est membre du Springer Science+Business Media
springer.com

Maquette de couverture: WMXDesign GmbH, Heidelberg
Imprimé sur papier non acide 41/3100/YL - 5 4 3 2 1 0 -

Mode d'emploi de ce traité

NOUVELLE ÉDITION

1. Le traité prend les mathématiques à leur début, et donne des démonstrations complètes. Sa lecture ne suppose donc, en principe, aucune connaissance mathématique particulière, mais seulement une certaine habitude du raisonnement mathématique et un certain pouvoir d'abstraction. Néanmoins, le traité est destiné plus particulièrement à des lecteurs possédant au moins une bonne connaissance des matières enseignées dans la première ou les deux premières années de l'Université.

2. Le mode d'exposition suivi est axiomatique et procède le plus souvent du général au particulier. Les nécessités de la démonstration exigent que les chapitres se suivent, en principe, dans un ordre logique rigoureusement fixé. L'utilité de certaines considérations n'apparaîtra donc au lecteur qu'à la lecture de chapitres ultérieurs, à moins qu'il ne possède déjà des connaissances assez étendues.

3. Le traité est divisé en Livres et chaque Livre en chapitres. Les Livres actuellement publiés, en totalité ou en partie, sont les suivants:

Théorie des Ensembles	désigné par	E
Algèbre	„	A
Topologie générale	„	TG
Fonctions d'une variable réelle	„	FVR
Espaces vectoriels topologiques	„	EVT
Intégration	„	INT
Algèbre commutative	„	AC
Variétés différentielles et analytiques	„	VAR
Groupes et algèbres de Lie	„	LIE
Théories spectrales	„	TS

Dans les *six premiers* Livres (pour l'ordre indiqué ci-dessus), chaque énoncé ne fait appel qu'aux définitions et résultats exposés précédemment dans ce Livre ou dans les Livres *antérieurs*. A partir du septième Livre, le lecteur

trouvera éventuellement, au début de chaque Livre ou chapitre, l'indication précise des autres Livres ou chapitres utilisés (les six premiers Livres étant toujours supposés connus).

4. Cependant, quelques passages font exception aux règles précédentes. Ils sont placés entre deux astérisques: * . . . *. Dans certains cas, il s'agit seulement de faciliter la compréhension du texte par des exemples qui se réfèrent à des faits que le lecteur peut déjà connaître par ailleurs. Parfois aussi, on utilise, non seulement les résultats supposés connus dans tout le chapitre en cours, mais des résultats démontrés ailleurs dans le traité. Ces passages seront employés librement dans les parties qui supposent connus les chapitres où ces passages sont insérés et les chapitres auxquels ces passages font appel. Le lecteur pourra, nous l'espérons, vérifier l'absence de tout cercle vicieux.

5. A certains Livres (soit publiés, soit en préparation) sont annexés des *fascicules de résultats*. Ces fascicules contiennent l'essentiel des définitions et des résultats du Livre, mais aucune démonstration.

6. L'armature logique de chaque chapitre est constituée par les *définitions*, les *axiomes* et les *théorèmes* de ce chapitre; c'est là ce qu'il est principalement nécessaire de retenir en vue de ce qui doit suivre. Les résultats moins importants, ou qui peuvent être facilement retrouvés à partir des théorèmes, figurent sous le nom de « propositions », « lemmes », « corollaires », « remarques », etc.; ceux qui peuvent être omis en première lecture sont imprimés en petits caractères. Sous le nom de « scholie », on trouvera quelquefois un commentaire d'un théorème particulièrement important.

Pour éviter des répétitions fastidieuses, on convient parfois d'introduire certaines notations ou certaines abréviations qui ne sont valables qu'à l'intérieur d'un seul chapitre ou d'un seul paragraphe (par exemple, dans un chapitre où tous les anneaux considérés sont commutatifs, on peut convenir que le mot « anneau » signifie toujours « anneau commutatif »). De telles conventions sont explicitement mentionnées à la tête du *chapitre* dans lequel elles s'appliquent.

7. Certains passages sont destinés à prémunir le lecteur contre des erreurs graves, où il risquerait de tomber; ces passages sont signalés en marge par le signe  (« tournant dangereux »).

8. Les exercices sont destinés, d'une part, à permettre au lecteur de vérifier qu'il a bien assimilé le texte; d'autre part à lui faire connaître des résultats qui n'avaient pas leur place dans le texte; les plus difficiles sont marqués du signe ¶.

9. La terminologie suivie dans ce traité a fait l'objet d'une attention particulière. *On s'est efforcé de ne jamais s'écarter de la terminologie reçue sans de très sérieuses raisons.*

10. On a cherché à utiliser, sans sacrifier la simplicité de l'exposé, un langage rigoureusement correct. Autant qu'il a été possible, les *abus de*

langage ou de notation, sans lesquels tout texte mathématique risque de devenir pédantesque et même illisible, ont été signalés au passage.

11. Le texte étant consacré à l'exposé dogmatique d'une théorie, on n'y trouvera qu'exceptionnellement des références bibliographiques; celles-ci sont groupées dans des *Notes historiques*. La bibliographie qui suit chacune de ces Notes ne comporte le plus souvent que les livres et mémoires originaux qui ont eu le plus d'importance dans l'évolution de la théorie considérée; elle ne vise nullement à être complète.

Quant aux exercices, il n'a pas été jugé utile en général d'indiquer leur provenance, qui est très diverse (mémoires originaux, ouvrages didactiques, recueils d'exercices).

12. Dans la nouvelle édition, les renvois à des théorèmes, axiomes, définitions, remarques, etc. sont donnés en principe en indiquant successivement le Livre (par l'abréviation qui lui correspond dans la liste donnée au n° 3), le chapitre et la page où ils se trouvent. A l'intérieur d'un même Livre la mention de ce Livre est supprimée; par exemple, dans le Livre d'Algèbre,

E, III, p. 32, cor. 3

renvoie au corollaire 3 se trouvant au Livre de Théorie des Ensembles, chapitre III, page 32 de ce chapitre;

II, p. 23, *Remarque* 3

renvoie à la Remarque 3 du Livre d'Algèbre, chapitre II, page 23 de ce chapitre.

Les fascicules de résultats sont désignés par la lettre R; par exemple: EVT, R signifie « fascicule de résultats du Livre sur les Espaces vectoriels topologiques ».

Comme certains Livres doivent seulement être publiés plus tard dans la nouvelle édition, les renvois à ces Livres se font en indiquant successivement le Livre, le chapitre, le paragraphe et le numéro où se trouve le résultat en question; par exemple:

AC, III, § 4, n° 5, cor. de la prop. 6.

Au cas où le Livre cité a été modifié au cours d'éditions successives, on indique en outre l'édition.

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 vînt à s'appliquer à des éléments qui n'avaient plus aucun caractère « numérique », par exemple aux permutations d'un ensemble (voir Note historique de 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. Autre-

ment 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 particularité 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.*

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 d'action », 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 d'action dans E.

Conformément aux définitions générales (E, IV, p. 4), la donnée, dans un ensemble E, d'une ou plusieurs lois de composition ou lois d'action définit une *structure* sur E; c'est aux structures définies de cette manière que nous réserverons, 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* (E, IV, p. 4) de structures algébriques, caractérisées, d'une part par les lois de composition ou lois d'action 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 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) et celle d'*anneau* (à *deux* lois de composition), 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, interviennent une ou plusieurs lois d'action. 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'*algèbre 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, 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, la théorie des *modules et anneaux semi-simples*, étroitement liée à celle des *représentations linéaires des groupes*; d'autre part, la théorie des *formes quadratiques* et des *formes hermitiennes*, avec l'étude des groupes qui leur sont associés. Enfin, les *géometries élémentaires* (affine, projective, euclidienne, etc.) sont étudiées aux chap. II, VI et IX 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.

CHAPITRE 1

Structures algébriques

§ 1. LOIS DE COMPOSITION; ASSOCIATIVITÉ; COMMUTATIVITÉ

1. Lois de composition

DÉFINITION 1. — *Soit* E *un ensemble. On appelle loi de composition sur* E *une application* f *de* $E \times E$ *dans* E. *La valeur* $f(x, y)$ *de* f *pour un couple* $(x, y) \in E \times E$ *s'appelle le composé de* x *et de* y *pour cette loi. Un ensemble muni d'une loi de composition est appelé un magma.*

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). Parmi les signes dont l'emploi est le plus fréquent, citons $+$ et $.$, étant convenu en général que ce dernier peut s'omettre à volonté; avec ces signes, le composé de x et y s'écrira respectivement $x + y$, et $x.y$ 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 $.$ s'appelle le plus souvent *multiplication* (le composé $x.y = xy$ 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 3 du présent chapitre, on se servira ordinairement des signes $\top$ et $\bot$ pour noter des lois de composition quelconques.

On dit parfois, par abus de langage, qu'une application d'une *partie* de $E \times E$ dans E est une loi de composition *non partout définie* dans E.

Exemples. — 1) Les applications $(X, Y) \mapsto X \cup Y$ et $(X, Y) \mapsto X \cap Y$ sont des lois de composition sur l'ensemble des parties d'un ensemble E.

2) Dans l'ensemble $\mathbf{N}$ des entiers naturels, l'addition, la multiplication, l'exponentiation sont des lois de composition (les composés de $x \in \mathbf{N}$ et de $y \in \mathbf{N}$ pour ces lois se notant respectivement $x + y$, xy ou $x.y$, et x^y) (E, III, p. 27–28).

3) Soit E un ensemble; l'application $(X, Y) \mapsto X \circ Y$ est une loi de composition sur l'ensemble des parties de $E \times E$ (E, II, p. 11, déf. 6); l'application $(f, g) \mapsto f \circ g$ est une loi de composition sur l'ensemble des applications de E dans E (E, II, p. 31).

4) Soit E un ensemble ordonné réticulé (E, III, p. 13); si on désigne par $\sup(x, y)$ la borne supérieure de l'ensemble $\{x, y\}$, l'application $(x, y) \mapsto \sup(x, y)$ est une loi de composition sur E. De même pour la borne inférieure $\inf(x, y)$. L'exemple 1 ci-dessus est un cas particulier de celui-ci, en considérant $\mathfrak{P}(E)$ comme ordonné par inclusion.

5) Soit $(E_i)_{i \in I}$ une famille de magmas. Notons $\top_i$ la loi de composition sur E_i. L'application

$$((x_i), (y_i)) \mapsto ((x_i \top_i y_i))$$

est une loi de composition sur le produit $E = \prod_{i \in I} E_i$, appelée *produit* des lois $\top_i$. L'ensemble E, muni de cette loi, s'appelle le *magma produit* des magmas E_i. En particulier, si tous les magmas E_i sont égaux à un même magma M, on obtient le *magma des applications de* I *dans* M.

Soit $(x, y) \mapsto x \top y$ une loi de composition sur un ensemble E. Etant données deux parties quelconques X, Y de E, on désignera par $X \top Y$ (pourvu que cette notation ne prête pas à confusion[1]) l'ensemble des éléments $x \top y$ de E, tels que $x \in X, y \in Y$ (autrement dit, l'image de $X \times Y$ par l'application $(x, y) \mapsto x \top y$).

Si $a \in E$, on écrit généralement $a \top Y$ au lieu de $\{a\} \top Y$, et $X \top a$ au lieu de $X \top \{a\}$. L'application $(X, Y) \mapsto X \top Y$ est une loi de composition sur l'ensemble des parties de E.

DÉFINITION 2. — *Soit* E *un magma. Notons* $\top$ *sa loi de composition. La loi de composition* $(x, y) \mapsto y \top x$ *sur* E *est dite opposée à la précédente. L'ensemble* E, *muni de cette loi, est appelé magma opposé de* E.

Soient E et E′ deux magmas; nous noterons leurs lois par le même signe $\top$. Conformément aux définitions générales (E, IV, p. 6), on appelle *isomorphisme de* E *sur* E′ une application bijective f de E sur E′, telle que

$$f(x \top y) = f(x) \top f(y) \tag{1}$$

pour tout couple $(x, y) \in E \times E$. On dit que E et E′ sont *isomorphes* s'il existe un isomorphisme de E sur E′.

Plus généralement:

DÉFINITION 3.—*On appelle homomorphisme, ou morphisme, de* E *dans* E′ *une application* f *de* E *dans* E′ *telle que la relation* (1) *soit vérifiée pour tout couple* $(x, y) \in E \times E$; *lorsque* E = E′, *on dit que* f *est un endomorphisme de* E.

L'application identique d'un magma E est un homomorphisme, le composé de deux homomorphismes est un homomorphisme.

Pour qu'une application f de E dans E′ soit un isomorphisme, il faut et il

[1] 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 $(A, B) \mapsto A \cup B$ entre parties d'un ensemble E; on en déduit une loi de composition $(\mathfrak{A}, \mathfrak{B}) \mapsto F(\mathfrak{A}, \mathfrak{B})$, 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 $\mathfrak{P}(E)$).

suffit que ce soit un homomorphisme bijectif, et f^{-1} est alors un isomorphisme de E′ sur E.

2. Composé d'une séquence d'éléments

Rappelons qu'une *famille* d'éléments d'un ensemble E est une application $\iota \mapsto x_\iota$ d'un ensemble I (dit ensemble d'indices) dans E; on dit qu'une famille $(x_\iota)_{\iota \in I}$ est *finie* si l'ensemble d'indices est *fini*.

On appelle *séquence* d'éléments de E une famille finie $(x_\iota)_{\iota \in I}$ d'éléments de E dont l'ensemble d'indices I est *totalement ordonné*.

En particulier, toute suite finie $(x_i)_{i \in H}$, où H est une partie finie de l'ensemble **N** des entiers naturels, peut être considérée comme une séquence, en munissant H de la relation d'ordre induite par la relation $m \leqslant n$ entre entiers naturels.

On dit que deux séquences $(x_i)_{i \in I}$ et $(y_k)_{k \in K}$ sont *semblables* s'il existe un isomorphisme φ d'ensembles ordonnés de I sur K tel que $y_{\varphi(i)} = x_i$ pour tout $i \in I$.

Toute séquence $(x_\alpha)_{\alpha \in A}$ est semblable à une suite finie convenable. En effet, il existe une bijection croissante de A sur un intervalle $[0, n]$ de **N**.

DÉFINITION 4. — *Soit* $(x_\alpha)_{\alpha \in A}$ *une séquence d'éléments d'un magma* E *dont l'ensemble d'indices* A *est non vide. On appelle composé (pour la loi* $\top$*) de la séquence* $(x_\alpha)_{\alpha \in A}$*, et on note* $\top_{\alpha \in A} x_\alpha$*, l'élément de* E *défini par récurrence sur le nombre d'éléments de* A*, de la façon suivante:*

1° *si* $A = \{\beta\}$, *alors* $\top_{\alpha \in A} x_\alpha = x_\beta$;

2° *si* A *a* $p > 1$ *éléments, si* β *est le plus petit élément de* A*, et si* $A' = A - \{\beta\}$, *alors* $\top_{\alpha \in A} x_\alpha = x_\beta \top (\top_{\alpha \in A'} x_\alpha)$.

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. Si $A = \{\lambda, \mu, \nu\}$ a trois éléments $(\lambda < \mu < \nu)$ le composé $\top_{\alpha \in A} x_\alpha$ est $x_\lambda \top (x_\mu \top x_\nu)$.

Remarque. — 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 ». Si on procédait « de gauche à droite », le composé de la séquence $(x_\lambda, x_\mu, x_\nu)$ ci-dessus serait $(x_\lambda \top x_\mu) \top x_\nu$.

Quand on utilise d'autres notations, le composé d'une séquence $(x_\alpha)_{\alpha \in A}$ s'écrit $\perp_{\alpha \in A} x_\alpha$ pour une loi notée $\perp$; pour une loi notée additivement, 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)[1].

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, $\sum_\alpha x_\alpha$ au lieu de $\sum_{\alpha \in A} x_\alpha$; de même pour les autres notations.

Pour une loi notée $\top$, le composé d'une *suite* (x_i), ayant pour ensemble d'indices un intervalle $[p, q]$ non vide de **N**, se note $\top_{p \leqslant i \leqslant q} x_i$, ou $\top_{i=p}^{q} x_i$; de même pour les lois notées par d'autres signes.

Soient E et F deux magmas, dont les lois sont notées $\top$, et f un homomorphisme de E dans F. Pour toute séquence $(x_\alpha)_{\alpha \in A}$ d'éléments de E, on a

$$f\Big(\top_{\alpha \in A} x_\alpha\Big) = \top_{\alpha \in A} f(x_\alpha). \tag{2}$$

3. Lois associatives

DÉFINITION 5. — *Une loi de composition $(x, y) \mapsto x \top y$ sur un ensemble* E *est dite associative si, quels que soient les éléments x, y, z de* E, *on a*

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

Un magma dont la loi est associative est appelé magma associatif.

La loi opposée à une loi associative est associative.

Exemples. — 1) L'addition et la multiplication des entiers naturels sont des lois de composition associatives sur **N** (E, III, p. 27, corollaire).

2) Les lois citées aux exemples 1), 3) et 4) de I, p. 1–2 sont associatives.

THÉORÈME 1 (Théorème d'associativité). — *Soit* E *un magma associatif dont la loi est notée* $\top$. *Soit* A *un ensemble fini non vide, totalement ordonné, réunion d'une séquence de parties non vides $(B_i)_{i \in I}$ telles que les relations $\alpha \in B_i$, $\beta \in B_j$, $i < j$ entraînent $\alpha < \beta$; soit $(x_\alpha)_{\alpha \in A}$ une séquence d'éléments de* E, *ayant* A *pour ensemble d'indices. On a*

$$\top_{\alpha \in A} x_\alpha = \top_{i \in I} \Big(\top_{\alpha \in B_i} x_\alpha\Big). \tag{3}$$

[1] L'emploi de ce terme et de la notation $\prod_{\alpha \in A} x_\alpha$ devra être évité lorsqu'il risque de créer des confusions avec le produit des ensembles x_α défini en théorie des ensembles (E, II, p. 32). Cependant, lorsque les x_α sont des cardinaux, et que l'addition (resp. la multiplication) est la somme cardinale (resp. le produit cardinal), le cardinal désigné par $\sum_{\alpha \in A} x_\alpha$ (resp. $\prod_{\alpha \in A} x_\alpha$) avec la notation ci-dessus est la somme cardinale (resp. le produit cardinal) de la famille $(x_\alpha)_{\alpha \in A}$ (E, III, p. 25–26).

Démontrons le théorème par récurrence sur le cardinal n de A. Soient p le cardinal de I et h son plus petit élément; posons $J = I - \{h\}$. Si $n = 1$, on a nécessairement $p = 1$, puisque les B_i ne sont pas vides, et le théorème est évident. Sinon, le théorème étant supposé vrai pour un ensemble d'indices ayant au plus $n - 1$ éléments, distinguons deux cas:

a) B_h a un seul élément β. Posons $C = \bigcup_{i \in J} B_i$. Le premier membre de (3) est égal, par définition, à $x_\beta \top (\top_{\alpha \in C} x_\alpha)$; le second membre est égal, par définition, à

$$x_\beta \top (\top_{i \in J} (\top_{\alpha \in B_i} x_\alpha));$$

l'égalité résulte de ce que le théorème est supposé vrai pour C et $(B_i)_{i \in J}$.

b) Sinon, soit β le plus petit élément de A (donc de B_h); soit $A' = A - \{\beta\}$, et soit $B'_i = A' \cap B_i$ pour $i \in I$; on a $B'_i = B_i$ pour $i \in J$. L'ensemble A' a $n - 1$ éléments, et les conditions du théorème sont satisfaites par A' et ses parties B'_i; on a donc par hypothèse:

$$\top_{\alpha \in A'} x_\alpha = (\top_{\alpha \in B'_h} x_\alpha) \top (\top_{i \in J} (\top_{\alpha \in B_i} x_\alpha)).$$

Formons le composé de x_β et de chacun des deux membres: au premier membre, on obtient par définition $\top_{\alpha \in A} x_\alpha$; au second, on obtient, en utilisant l'associativité,

$$(x_\beta \top (\top_{\alpha \in B'_h} x_\alpha)) \top (\top_{i \in J} (\top_{\alpha \in B_i} x_\alpha))$$

ce qui est égal, d'après la définition 3, au second membre de la formule (3).

Pour une loi associative notée $\top$, le composé $\top_{p \leqslant i \leqslant q} x_i$ d'une suite $(x_i)_{i \in [p,q]}$ se note encore (lorsqu'aucune confusion n'est possible)

$$x_p \top \cdots \top x_q.$$

Un cas particulier du th. 1 est la formule

$$x_0 \top x_1 \top \cdots \top x_n = (x_0 \top x_1 \top \cdots \top x_{n-1}) \top x_n.$$

Considérons une séquence de n termes dont tous les termes sont égaux à un même élément $x \in E$. Le composé de cette séquence se note $\overset{n}{\top} x$ pour une loi notée $\top$, $\overset{n}{\perp} x$ pour une loi notée $\perp$. Pour une loi notée multiplicativement, le composé se note x^n et s'appelle *puissance n-ème* de x. Pour une loi notée additivement, le composé se note le plus souvent nx et s'appelle *n-uple* de x. Le théorème d'associativité, appliqué à une séquence dont tous les termes sont égaux, donne la formule

$$\overset{n_1 + n_2 + \cdots + n_p}{\top} x = (\overset{n_1}{\top} x) \top (\overset{n_2}{\top} x) \top \cdots \top (\overset{n_p}{\top} x).$$

En particulier, si $p = 2$,

$$\overset{m+n}{\top}\, x = (\overset{m}{\top}\, x) \top (\overset{n}{\top}\, x) \tag{4}$$

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

$$\overset{pm}{\top}\, x = \overset{p}{\top}\, (\overset{m}{\top}\, x). \tag{5}$$

Si X est une partie de E, on désigne parfois, conformément aux notations ci-dessus, par $\overset{p}{\top}\, X$ l'ensemble $X_1 \top X_2 \top \cdots \top X_p$ où

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

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

Z Il importe de ne pas confondre cet ensemble avec l'ensemble des $\overset{p}{\top} x$, où x parcourt X.

4. Parties stables. Lois induites

DÉFINITION 6. — *Une partie* A *d'un ensemble* E *est dite stable pour une loi de composition* $\top$ *sur* E *si le composé de deux éléments de* A *appartient à* A. *L'application* $(x, y) \mapsto x \top y$ *de* $A \times A$ *dans* A *s'appelle alors la loi induite sur* A *par la loi* $\top$. *L'ensemble* A, *muni de la loi induite par* $\top$, *s'appelle un sous-magma de* E.

Autrement dit, pour que A soit stable pour une loi $\top$, il faut et il suffit que $A \top A \subset A$. On identifie souvent une partie stable de E et le sous-magma correspondant.

L'intersection d'une famille de parties stables de E est stable; en particulier il existe une plus petite partie stable A de E contenant une partie X donnée; elle est dite *engendrée* par X et X est appelé un *système générateur* de A, ou *ensemble générateur* de A. On dit aussi que le sous-magma A est *engendré* par X.

PROPOSITION 1. — *Soient* E *et* F *deux magmas, et* f *un homomorphisme de* E *dans* F.

(i) *L'image par* f *d'une partie stable de* E *est une partie stable de* F.

(ii) *L'image réciproque par* f *d'une partie stable de* F *est une partie stable de* E.

(iii) *Soit* X *une partie de* E. *L'image par* f *de la partie stable de* E *engendrée par* X *est la partie stable de* F *engendrée par* $f(X)$.

(iv) *Si* g *est un second homomorphisme de* E *dans* F, *l'ensemble des éléments* x *de* E *tels que* $f(x) = g(x)$ *est une partie stable de* E.

Les assertions (i), (ii) et (iv) sont évidentes; démontrons (iii). Soient $\overline{X}$ la partie stable de E engendrée par X et $\overline{f(X)}$ la partie stable de F engendrée par $f(X)$. D'après (i), on a $\overline{f(X)} \subset f(\overline{X})$, et d'après (ii), on a $\overline{X} \subset f^{-1}(\overline{f(X)})$, d'où $f(\overline{X}) \subset \overline{f(X)}$.

PROPOSITION 2. — *Soient* E *un magma associatif et* X *une partie de* E. *Soit* X′ *l'ensemble des* $x_1 \top x_2 \top \cdots \top x_n$, *où* $n \geqslant 1$ *et où* $x_i \in X$ *pour* $1 \leqslant i \leqslant n$. *La partie stable engendrée par* X *est égale à* X′.

Il est immédiat, par récurrence sur n, que le composé d'une séquence de n termes appartenant à X appartient à la partie stable engendrée par X; il suffit donc de voir que X′ est stable. Or, si u et v sont deux éléments de X′, ils sont de la forme $u = x_0 \top x_1 \top \cdots \top x_{n-1}$, $v = x_n \top x_{n+1} \top \cdots \top x_{n+p}$ avec $x_i \in X$ pour $0 \leqslant i \leqslant n + p$; donc (I, p. 4, th. 1) $u \top v = x_0 \top x_1 \top \cdots \top x_{n+p}$ appartient à X′.

Exemples. — 1) Dans l'ensemble **N** des entiers naturels, la partie stable pour l'addition engendrée par {1} est l'ensemble des entiers $\geqslant 1$; pour la multiplication, l'ensemble {1} est stable.

2) Etant donnée une loi $\top$ sur un ensemble E, pour qu'une partie $\{h\}$ réduite à un seul élément soit stable pour la loi $\top$, il faut et il suffit que $h \top h = h$; on dit alors que h est *idempotent*. Par exemple, tout élément d'un ensemble ordonné réticulé est idempotent pour chacune des lois sup et inf.

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

5. Eléments permutables. Lois commutatives

DÉFINITION 7. — *Soit* E *un magma dont la loi est notée* $\top$. *On dit que deux éléments* x *et* y *de* E commutent (*ou sont* permutables) *si* $y \top x = x \top y$.

DÉFINITION 8. — *Une loi de composition sur un ensemble* E *est dite* commutative *si deux éléments quelconques de* E *commutent pour cette loi. Un magma dont la loi de composition est commutative est appelé* magma commutatif.

Une loi commutative est égale à son opposée.

Exemples. — 1) L'addition et la multiplication des entiers naturels sont des lois commutatives sur **N** (E, III, p. 27, corollaire).

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

3) Soit E un ensemble, de cardinal > 1. La loi $(f, g) \mapsto f \circ g$ entre applications de E dans E n'est pas commutative, comme on le voit en prenant pour f et g des applications constantes distinctes, mais l'application identique est permutable avec toute application.

4) Soit $(x, y) \mapsto x \top y$ une loi commutative sur E; la loi $(X, Y) \mapsto X \top Y$ entre parties de E est commutative.

DÉFINITION 9. — *Soient* E *un magma et* X *une partie de* E. *On appelle* commutant *de* X *dans* E *l'ensemble des éléments de* E *qui commutent avec chacun des éléments de* X.

Soient X et Y deux parties de E, X′ et Y′ leurs commutants respectifs. Si $X \subset Y$, on a $Y' \subset X'$.

Soit $(X_i)_{i \in I}$ une famille de parties de E, et pour tout $i \in I$ soit X_i' le commutant de X_i. Le commutant de $\bigcup_{i \in I} X_i$ est $\bigcap_{i \in I} X_i'$.

Soient X une partie de E, et X′ le commutant de X. Le commutant X″ de X′ est appelé le *bicommutant* de X. On a $X \subset X''$. Le commutant X‴ de X″ est égal à X′. En effet, X′ est contenu dans son bicommutant X‴, et la relation $X \subset X''$ entraîne $X''' \subset X'$.

PROPOSITION 3. — *Soit* E *un magma associatif dont la loi est notée* $\top$. *Si un élément x de* E *commute avec chacun des éléments y et z de* E, *il commute avec* $y \top z$.

En effet, on a

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

COROLLAIRE. — *Soit* E *un magma associatif. Le commutant d'une partie quelconque de* E *est une partie stable de* E.

DÉFINITION 10. — *On appelle* centre *d'un magma* E *le commutant de* E. *Un élément du centre de* E *est appelé élément* central *de* E.

Si E est un magma associatif, son centre est une partie stable d'après le cor. de la prop. 3, et la loi induite sur ce centre est commutative.

PROPOSITION 4. — *Soient* E *un magma associatif,* X *et* Y *deux parties de* E. *Si tout élément de* X *commute avec tout élément de* Y, *tout élément de la partie stable engendrée par* X *commute avec tout élément de la partie stable engendrée par* Y.

Soient X′ et X″ le commutant et le bicommutant de X. Ce sont des parties stables de E. On a $X \subset X''$ et $Y \subset X'$, donc X″ (resp. X′) contient la partie stable de E engendrée par X (resp. Y). Comme tout élément de X″ commute avec tout élément de X′, la proposition en résulte.

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

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

THÉORÈME 2 (théorème de commutativité). — *Soit* $\top$ *une loi de composition associative sur* E; *soit* $(x_\alpha)_{\alpha \in A}$ *une famille finie non vide d'éléments de* E, *deux à deux permutables*; *soient* B *et* C *deux ensembles totalement ordonnés ayant* A *pour ensemble sous-jacent. Alors* $\top_{\alpha \in B} x_\alpha = \top_{\alpha \in C} x_\alpha$.

Le théorème étant vrai si A a un seul élément β, raisonnons par récurrence sur le nombre p d'éléments de A. Soit p un entier > 1, supposons le théorème vrai lorsque $\operatorname{Card} A < p$ et démontrons-le pour $\operatorname{Card} A = p$. On peut supposer que A est l'intervalle $[0, p-1]$ de $\mathbf{N}$; le composé de la séquence $(x_\alpha)_{\alpha \in A}$ définie par a relation d'ordre naturelle sur A est $\top_{i=0}^{p-1} x_i$.

Ordonnons totalement A d'une autre manière, et soient 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 $P = \{0,1,\ldots,h-1\}$, et $Q = \{h+1,\ldots,p-1\}$; le théorème étant supposé vrai pour A', on a, en appliquant de plus le théorème d'associativité (puisque $A' = P \cup Q$)

$$\top_{\alpha\in A'} x_\alpha = \left(\top_{i=0}^{h-1} x_i\right) \top \left(\top_{i=h+1}^{p-1} x_i\right)$$

d'où, en composant x_h avec les deux membres, et par application répétée de la commutativité et de l'associativité de $\top$:

$$\top_{\alpha\in A} x_\alpha = x_h \top \left(\top_{\alpha\in A'} x_\alpha\right) = x_h \top \left(\top_{i=0}^{h-1} x_i\right) \top \left(\top_{i=h+1}^{p-1} x_i\right)$$

$$= \left(\top_{i=0}^{h-1} x_i\right) \top x_h \top \left(\top_{i=h+1}^{p-1} x_i\right) = \top_{i=0}^{p-1} x_i,$$

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 P ou bien les termes relatifs à Q n'apparaissant pas dans les 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 est par définition la valeur commune des composés de toutes les *séquences* obtenues en ordonnant totalement A de toutes les manières possibles. Ce composé se note encore $\top_{\alpha\in A} x_\alpha$ pour une loi notée $\top$; de même pour les autres notations.

THÉORÈME 3. — *Soient* $\top$ *une loi associative sur* E, $(x_\alpha)_{\alpha\in A}$ *une famille finie non vide d'éléments de* E *deux à deux permutables. Si* A *est réunion d'une famille de parties non vides* $(B_i)_{i\in I}$, *deux à deux disjointes, on a*

$$\top_{\alpha\in A} x_\alpha = \top_{i\in I}\left(\top_{\alpha\in B_i} x_\alpha\right). \tag{6}$$

En effet, cela résulte du th. 2 (I, p. 8) en ordonnant totalement A et I de façon que les B_i vérifient les conditions du th. 1 (I, p. 4).

Signalons deux cas particuliers importants de ce théorème:

1) Si $(x_{\alpha\beta})_{(\alpha,\beta)\in A\times B}$ est une famille finie d'éléments permutables d'un magma associatif dont l'ensemble d'indices est le produit de deux ensembles finis non vides A, B (« famille double »), on a

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

comme il résulte du th. 3 en considérant $A \times B$ comme réunion des ensembles $\{\alpha\} \times B$ d'une part, des ensembles $A \times \{\beta\}$ de l'autre.

Par exemple, 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

$$\text{(8)} \qquad \top_{\alpha \in A} (\overset{n}{\top} x_\alpha) = \overset{n}{\top} (\top_{\alpha \in A} x_\alpha).$$

Si B a deux éléments, on obtient le résultat suivant: soient $(x_\alpha)_{\alpha \in A}$, $(y_\alpha)_{\alpha \in A}$ deux familles non vides d'éléments de E. Si les x_α et les y_β sont deux à deux permutables, on a

$$\text{(9)} \qquad \top_{\alpha \in A} (x_\alpha \top y_\alpha) = (\top_{\alpha \in A} x_\alpha) \top (\top_{\alpha \in A} y_\alpha).$$

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 $\mathbf{N}$, 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.

2) Soit n un entier > 0 et soit A l'ensemble des couples d'entiers (i, j) tels que $0 \leqslant i \leqslant n$, $0 \leqslant j \leqslant n$ et $i < j$; le composé d'une famille $(x_{ij})_{(i,j) \in A}$ (pour une loi associative et commutative), se notera encore $\top_{0 \leqslant i < j \leqslant n} x_{ij}$ (ou simplement $\top_{i<j} x_{ij}$ si aucune confusion n'en résulte); le th. 3 donne ici les formules

$$\text{(10)} \qquad \top_{0 \leqslant i < j \leqslant n} x_{ij} = \overset{n-1}{\top_{i=0}} (\overset{n}{\top_{j=i+1}} x_{ij}) = \overset{n}{\top_{j=1}} (\overset{j-1}{\top_{i=0}} x_{ij}).$$

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 (10) pour une famille dont l'ensemble d'indices est l'ensemble S_p des *suites strictement croissantes* $(i_k)_{1 \leqslant k \leqslant p}$ de p entiers tels que $0 \leqslant i_k \leqslant n$ $(p \leqslant n + 1)$: dans ce dernier cas, le composé de la famille $(x_{i_1 i_2 \ldots i_p})_{(i_1, \ldots, i_p) \in S_p}$ se note

$$\top_{0 \leqslant i_1 < i_2 < \ldots < i_p \leqslant n} x_{i_1 i_2 \ldots i_p}, \quad \text{ou simplement} \quad \top_{i_1 < i_2 < \ldots < i_p} x_{i_1 i_2 \ldots i_p}.$$

PROPOSITION 5. — *Soient* E *et* F *des magmas dont les lois sont notées* $\top$, *et soient* f *et* g *des homomorphismes de* E *dans* F. *Soit* $f \top g$ *l'application* $x \mapsto f(x) \top g(x)$ *de* E *dans* F. *Si* F *est associatif et commutatif,* $f \top g$ *est un homomorphisme.*

En effet, quels que soient les éléments x et y de E, on a:

$$\begin{aligned}(f \top g)(x \top y) &= f(x \top y) \top g(x \top y) = f(x) \top f(y) \top g(x) \top g(y) \\ &= f(x) \top g(x) \top f(y) \top g(y) = ((f \top g)(x)) \top ((f \top g)(y)).\end{aligned}$$

6. Lois quotients

DÉFINITION 11. — *Soit* E *un ensemble. On dit qu'une loi de composition* $\top$ *et une relation*

d'équivalence R *dans* E *sont compatibles si les relations* $x \equiv x' \pmod{R}$ *et* $y \equiv y' \pmod{R}$ (*pour* x, x', y, y' *dans* E) *entraînent* $x \top y \equiv x' \top y' \pmod{R}$; *la loi de composition sur l'ensemble quotient* E/R *qui, aux classes d'équivalence de* x *et de* y, *fait correspondre la classe d'équivalence de* $x \top y$, *s'appelle la loi quotient de la loi* $\top$ *par* R. *L'ensemble* E/R, *muni de la loi quotient, s'appelle le magma quotient de* E *par* R.

Dire qu'une relation d'équivalence R dans E est compatible avec la loi de composition $f : E \times E \to E$, signifie que l'application f est compatible (au sens de E, II, p. 44) avec les relations d'équivalence produit $R \times R$ dans $E \times E$ (E, II, p. 46) et R dans E. Cela signifie aussi que le graphe de R est un sous-magma de $E \times E$.

Si la loi $\top$ est associative (resp. commutative), il en est de même de la loi quotient (on dit pour abréger que *l'associativité, ou la commutativité, se conserve par passage au quotient*).

L'application canonique du magma E dans le magma E/R est un homomorphisme.

Pour qu'une application g de E/R dans un magma F soit un homomorphisme, il faut et il suffit que le composé de g et de l'application canonique de E sur E/R soit un homomorphisme.

Les deux propositions suivantes se déduisent immédiatement des définitions:

PROPOSITION 6. — *Soient* E *et* F *deux magmas et* f *un homomorphisme de* E *dans* F. *Notons* $R\{x, y\}$ *la relation* $f(x) = f(y)$ *entre éléments* x, y *de* E. *Alors* R *est une relation d'équivalence dans* E *compatible avec la loi de* E *et l'application de* E/R *sur* f(E) *déduite de* f *par passage au quotient est un isomorphisme du magma quotient* E/R *sur le sous-magma* f(E) *de* F.

PROPOSITION 7. — *Soient* E *un magma et* R *une relation d'équivalence dans* E *compatible avec la loi de* E. *Pour qu'une relation d'équivalence* S *dans* E/R *soit compatible avec la loi quotient, il faut et il suffit que* S *soit de la forme* T/R, *où* T *est une relation d'équivalence dans* E, *entraînée par* R *et compatible avec la loi de* E. *L'application canonique de* E/T *sur* (E/R)/(T/R) (E, II, p. 46) *est alors un isomorphisme de magmas.*

PROPOSITION 8. — *Soient* E *un magma,* A *une partie stable de* E *et* R *une relation d'équivalence dans* E, *compatible avec la loi de* E. *Le saturé* B *de* A *pour* R (E, II, p. 44) *est une partie stable. Les relations d'équivalence* R_A *et* R_B *induites par* R *dans* A *et* B *respectivement sont compatibles avec les lois induites et l'application déduite de l'injection canonique de* A *dans* B *par passage aux quotients est un isomorphisme de magmas de* A/R_A *sur* B/R_B.

Notons $\top$ la loi de E. Si x et y sont deux éléments de B, il existe deux éléments x' et y' de A tels que $x \equiv x' \pmod{R}$ et $y \equiv y' \pmod{R}$; on a alors $x \top y \equiv x' \top y' \pmod{R}$ et $x' \top y' \in A$, d'où $x \top y \in B$. Ainsi B est une partie stable de E, et les autres assertions sont évidentes.

Soient M un magma, et $((u_\alpha, v_\alpha))_{\alpha \in I}$ une famille d'éléments de M × M. Considérons toutes les relations d'équivalence S dans M qui sont compatibles avec la loi de M, et telles que $u_\alpha \equiv v_\alpha$ (mod. S) pour tout $\alpha \in I$. L'intersection des graphes de ces relations est le graphe d'une relation d'équivalence R, qui est compatible avec la loi de M, et telle que $u_\alpha \equiv v_\alpha$ (mod R). Donc R est *la plus fine* (E, III, p. 4 et p. 8) des relations d'équivalence possédant ces deux propriétés. On l'appelle la relation d'équivalence compatible avec la loi de M *engendrée* par les (u_α, v_α).

PROPOSITION 9. — *On conserve les notations précédentes. Soit f un homomorphisme de* M *dans un magma tel que* $f(u_\alpha) = f(v_\alpha)$ *pour tout* $\alpha \in I$. *Alors f est compatible avec* R.

Soit T la relation d'équivalence associée à *f*. On a $u_\alpha \equiv v_\alpha$ (mod T) pour tout $\alpha \in I$, et T est compatible avec la loi de M, donc T est moins fine que R ; cela prouve la proposition.

§ 2. ÉLÉMENT NEUTRE; ÉLÉMENTS SIMPLIFIABLES; ÉLÉMENTS INVERSIBLES

1. Elément neutre

DÉFINITION 1. — *Pour une loi de composition* $\top$ *sur un ensemble* E, *un élément e de* E *est dit* élément neutre *si, pour tout* $x \in E$, *on a* $e \top x = x \top e = x$.

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

DÉFINITION 2. — *On appelle magma unifère un magma qui possède un élément neutre. Si* E, E' *sont des magmas unifères, on appelle homomorphisme* (ou *morphisme*) *unifère de* E *dans* E' *un homomorphisme du magma* E *dans le magma* E' *qui transforme l'élément neutre de* E *en l'élément neutre de* E'. *On appelle monoïde un magma unifère associatif.*

Si E, E' sont des monoïdes, on appelle *homomorphisme de monoïdes* ou *morphisme de monoïdes* de E dans E' un morphisme *unifère* de E dans E'.

Exemples. — 1) Dans l'ensemble **N** des entiers naturels, 0 est élément neutre pour l'addition et 1 est élément neutre pour la multiplication. Chacune de ces deux lois munit **N** d'une structure de monoïde commutatif (E, III, p. 27).

2) Dans l'ensemble des parties d'un ensemble E, $\varnothing$ 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; réciproquement, s'il existe un élément neutre pour cette loi, il est le plus petit élément de l'ensemble. De même pour le plus grand élément et la loi inf.

3) L'ensemble **N** ne possède pas d'élément neutre pour la loi $(x, y) \mapsto x^y$. Pour la loi $(X, Y) \mapsto X \circ Y$ entre parties de E × E, la diagonale Δ est l'élément neutre. Pour la loi $(f, g) \mapsto f \circ g$ entre applications de E dans E, l'application identique de E est l'élément neutre.

4) Soient E un magma et R une relation d'équivalence sur E, compatible avec la loi de E (I, p. 11). Si e est élément neutre de E, l'image canonique de e dans E/R est élément neutre du magma E/R.

L'application identique d'un magma unifère est un homomorphisme unifère; le composé de deux homomorphismes unifères en est un. Pour qu'une application soit un isomorphisme de magmas unifères, il faut et il suffit que ce soit un homomorphisme unifère bijectif et l'application réciproque est alors un homomorphisme unifère. Soient E et E′ des magmas unifères, e' l'élément neutre de E′; l'application constante de E dans E′ appliquant E en e' est un homomorphisme unifère, appelé *homomorphisme trivial.*

Le produit d'une famille de magmas unifères (resp. de monoïdes) est un magma unifère (resp. un monoïde).

Tout magma quotient d'un magma unifère (resp. d'un monoïde) est un magma unifère (resp. un monoïde).

Soient E un magma unifère, e son élément neutre. On appelle *sous-magma unifère* de E un sous-magma A de E tel que $e \in A$. Il est clair que e est élément neutre du magma A. Toute intersection de sous-magmas unifères de E est un sous-magma unifère de E. Si X est une partie de E, il existe donc un plus petit sous-magma unifère de E contenant X; on l'appelle le *sous-magma unifère de* E *engendré par* X; il est égal à $\{e\}$ si X est vide. Si E est un monoïde, on appelle *sous-monoïde* de E un sous-magma unifère de E.

Si F est un magma sans élément neutre, un sous-magma de F peut posséder un élément neutre. Par exemple, si F est associatif et si h est un élément idempotent de F (I, p. 7), l'ensemble des $h \top x \top h$, où x parcourt F est un sous-magma de F admettant h pour élément neutre.

Si E est un magma d'élément neutre e, il peut se faire qu'un sous-magma A de E tel que $e \notin A$ possède un élément neutre.

DÉFINITION 3. — *Soit* E *un magma unifère. On appelle composé de la famille vide d'éléments de* E *l'élément neutre de* E.

Si $(x_\alpha)_{\alpha \in \varnothing}$ est la famille vide d'éléments de E, son composé e se note encore $\top_{\alpha \in \varnothing} x_\alpha$. Par exemple, on écrit

$$\top_{q \leqslant i \leqslant p} x_i = e$$

lorsque $p < q$ ($p, q \in \mathbf{N}$). On pose de même $\overset{0}{\top} x = e$ quel que soit x. *Avec ces définitions, les théorèmes* 1 (I, p. 4) *et* 3 (I, p. 9) *du* § 1 *restent vrais dans un magma unifère, si on y supprime l'hypothèse que les ensembles* A *et* B_i *sont non vides.* De même, les formules $\overset{m+n}{\top} x = (\overset{m}{\top} x) \top (\overset{n}{\top} x)$ et $\overset{mn}{\top} x = \overset{m}{\top} (\overset{n}{\top} x)$ sont vraies alors pour $m \geqslant 0, n \geqslant 0$.

Soient E un magma unifère dont la loi est notée $\top$ et e son élément neutre. On appelle *support* d'une famille $(x_i)_{i \in I}$ d'éléments de E l'ensemble des indices

$i \in \mathrm{I}$ tels que $x_i \neq e$. Soit $(x_i)_{i \in \mathrm{I}}$ une famille *à support fini* d'éléments de E. Nous allons définir le composé $\top_{i \in \mathrm{I}} x_i$ dans les deux cas suivants:

a) l'ensemble I est totalement ordonné;
b) E est associatif et les x_i sont permutables deux à deux.

Dans ces deux cas, soit S le support de la famille (x_i). Si J est une partie finie de I contenant S, on a $\top_{i \in \mathrm{J}} x_i = \top_{i \in \mathrm{S}} x_i$, comme on le voit par récurrence sur le nombre d'éléments de J, en appliquant le th. 1 (I, p. 4) dans le cas a) et le th. 3 (I, p. 9) dans le cas b). On note $\top_{i \in \mathrm{I}} x_i$ la valeur commune des composés $\top_{i \in \mathrm{J}} x_i$ pour toutes les parties finies de I contenant S. Lorsque I est l'intervalle $[p, \to)$ de $\mathbf{N}$, on écrit aussi $\top_{i=p}^{\infty} x_i$.

Avec ces définitions et notations, les théorèmes 1 (I, p. 4) et 3 (I, p. 9) du § 1 et les remarques qui suivent le th. 3 (I, p. 9 et p. 10) s'étendent aux familles à support fini.

L'élément neutre, pour une loi notée *additivement*, se note souvent 0 et s'appelle *zéro* ou *élément nul* (ou parfois *origine*). Pour une loi notée *multiplicativement*, il se note souvent 1 et s'appelle *élément unité* (ou *unité*).

2. Eléments simplifiables

DÉFINITION 4. — *Etant donnée une loi de composition* $\top$ *sur un ensemble* E, *on appelle translation à gauche* (resp. *translation à droite*) *par un élément* $a \in \mathrm{E}$, *l'application* $x \mapsto a \top x$ (resp. $x \mapsto x \top a$) *de* E *dans lui-même.*

Par passage à la loi opposée, les translations à gauche deviennent translations à droite et réciproquement.

On note éventuellement γ_a, δ_a (ou $\gamma(a)$, $\delta(a)$) les translations à gauche et à droite par $a \in \mathrm{E}$; on a

$$\gamma_a(x) = a \top x, \qquad \delta_a(x) = x \top a.$$

PROPOSITION 1. — *Si la loi* $\top$ *est associative, on a, pour* $x \in \mathrm{E}$ *et* $y \in \mathrm{E}$,

$$\gamma_{x \top y} = \gamma_x \circ \gamma_y, \qquad \delta_{x \top y} = \delta_y \circ \delta_x.$$

En effet, pour tout $z \in \mathrm{E}$, on a:

$$\gamma_{x \top y}(z) = (x \top y) \top z = x \top (y \top z) = \gamma_x(\gamma_y(z))$$
$$\delta_{x \top y}(z) = z \top (x \top y) = (z \top x) \top y = \delta_y(\delta_x(z)).$$

Autrement dit, l'application $x \mapsto \gamma_x$ est un homomorphisme du magma E dans l'ensemble E^{E} des applications de E dans lui-même, muni de la loi $(f, g) \mapsto f \circ g$; l'application $x \mapsto \delta_x$ est un homomorphisme de E dans l'ensemble E^{E} muni de la loi opposée. Si E est un monoïde, ces homomorphismes sont unifères.

DÉFINITION 5. — *Un élément a d'un magma* E *est dit* simplifiable (*ou* régulier) à gauche (resp. à droite) *si la translation à gauche* (resp. *à droite*) *par a est injective. Un élément simplifiable à gauche et à droite est appelé élément simplifiable* (*ou régulier*).

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

Exemples. — 1) Tout entier naturel est simplifiable pour l'addition; tout entier naturel $\neq 0$ est simplifiable pour la multiplication.

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

PROPOSITION 2. — *L'ensemble des éléments simplifiables* (resp. *simplifiables à gauche*, resp. *simplifiables à droite*) *d'un magma associatif est un sous-magma.*

En effet, si γ_x et γ_y sont injectives, il en est de même de $\gamma_{x \top y} = \gamma_x \circ \gamma_y$ (I, p. 14, prop. 1). De même pour $\delta_{x \top y}$.

3. Eléments inversibles

DÉFINITION 6. — *Soient* E *un magma unifère,* $\top$ *sa loi de composition, e son élément neutre, x et x' deux éléments de* E. *On dit que x' est* inverse à gauche (resp. inverse à droite, resp. inverse) *de x si l'on a $x' \top x = e$* (resp. $x \top x' = e$, resp. $x' \top x = x \top x' = e$).

On dit qu'un élément x de E *est* inversible à gauche (resp. inversible à droite, resp. inversible) *s'il possède un inverse à gauche* (resp. *inverse à droite*, resp. *inverse*).

Un monoïde dont tous les éléments sont inversibles s'appelle un groupe.

On dit parfois *symétrique* et *symétrisable* au lieu d'*inverse* et *inversible*. Lorsque la loi de E est notée additivement, on dit généralement *opposé* au lieu d'*inverse*.

Exemples. — 1) Un élément neutre est son propre inverse.

2) Dans l'ensemble des applications de E dans E, un élément f est inversible à gauche (resp. inversible à droite) si f est une injection (resp. surjection). Les inverses à gauche (resp. inverses à droite) sont alors les rétractions (resp. sections) associées à f (E, II, p. 18, déf. 11). Pour que f soit inversible, il faut et il suffit que f soit une bijection. Son unique inverse est alors la bijection réciproque de f.

Soient E et F deux magmas unifères, et f un homomorphisme unifère de E dans F. Si x' est inverse de x dans E, $f(x')$ est inverse de $f(x)$ dans F. Par suite, si x est un élément inversible de E, $f(x)$ est un élément inversible de F.

En particulier, si R est une relation d'équivalence compatible avec la loi d'un

magma unifère E, l'image canonique dans E/R d'un élément inversible de E est inversible.

PROPOSITION 3. — *Soient* E *un monoïde et x un élément de* E.

(i) *Pour que x soit inversible à gauche* (resp. *à droite*), *il faut et il suffit que la translation à droite* (resp. *à gauche*) *par x soit surjective.*

(ii) *Pour que x soit inversible, il faut et il suffit qu'il soit inversible à gauche et inversible à droite. Dans ce cas, x possède un unique inverse, qui est aussi son unique inverse à gauche* (resp. *à droite*).

Si x' est un inverse à gauche de x, on a (I, p. 14, prop. 1)

$$\delta_x \circ \delta_{x'} = \delta_{x' \top x} = \delta_e = \mathrm{Id}_E$$

et δ_x est surjective. Réciproquement, si δ_x est surjective, il existe un élément x' de E tel que $\delta_x(x') = e$ et x' est inverse à gauche de x. On démontre de même l'autre assertion de (i).

Si x' (resp. x'') est un inverse à gauche (resp. à droite) de x, on a

$$x' = x' \top e = x' \top (x \top x'') = (x' \top x) \top x'' = e \top x'' = x''$$

d'où (ii).

Remarque. — Soient E un monoïde et x un élément de E. Si x est inversible à gauche, il est simplifiable à gauche; en effet, si x' est un inverse à gauche de x, on a

$$\gamma_{x'} \circ \gamma_x = \gamma_{x' \top x} = \gamma_e = \mathrm{Id}_E$$

et γ_x est injective. En particulier, si x est inversible, les translations à gauche et à droite par x sont *bijectives*. Réciproquement, supposons γ_x bijective; il existe $x' \in E$ tel que $xx' = \gamma_x(x') = e$; on a $\gamma_x(x'x) = (xx')x = x = \gamma_x(e)$, donc $x'x = e$, de sorte que x est inversible. On voit de même que si δ_x est bijective, x est inversible.

PROPOSITION 4. — *Soient* E *un monoïde, x et y deux éléments inversibles de* E, *d'inverses x' et y' respectivement. Alors y' ⊤ x' est inverse de x ⊤ y.*

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

COROLLAIRE 1. — *Soit* E *un monoïde; si chacun des éléments x_α d'une séquence $(x_\alpha)_{\alpha \in A}$ d'éléments de* E *a un inverse x'_α, le composé $\top_{\alpha \in A} x_\alpha$ a pour inverse $\top_{\alpha \in A'} x'_\alpha$, 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. 4 en raisonnant par récurrence sur le nombre d'éléments de A.

En particulier, si x et x' sont inverses, $\overset{n}{\top} x$ et $\overset{n}{\top} x'$ sont inverses, pour tout entier $n \geqslant 0$.

COROLLAIRE 2. — *Dans un monoïde, l'ensemble des éléments inversibles est stable.*

PROPOSITION 5. — *Si, dans un monoïde, x et x' sont inverses, et si x commute avec y, alors x' commute avec y.*

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

COROLLAIRE 1. — *Soient* E *un monoïde,* X *une partie de* E *et* X′ *le commutant de* X. *L'inverse de tout élément inversible de* X′ *appartient à* X′.

COROLLAIRE 2. — *Dans un monoïde, l'inverse d'un élément central inversible est un élément central.*

4. Monoïde des fractions d'un monoïde commutatif

Dans ce n°, on notera e l'élément neutre d'un monoïde E, et x^* l'inverse d'un élément inversible x de E.

Soient E un monoïde *commutatif*, S une partie de E et S′ le sous-monoïde de E engendré par S.

Lemme 1. — *Dans* E × S′, *la relation* $R\{x, y\}$ *que voici:*

« il existe a, b dans E et p, q, s dans S′ tels que $x = (a, p), y = (b, q)$, et $aqs = bps$ » *est une relation d'équivalence compatible avec la loi du monoïde produit* E × S′.

Il est immédiat que R est réflexive et symétrique. Soient $x = (a, p), y = (b, q)$ et $z = (c, r)$ des éléments de E × S′ tels que l'on ait $R\{x, y\}$ et $R\{y, z\}$. Il existe donc deux éléments s et t de S′ tels que

$$aqs = bps, \qquad brt = cqt,$$

d'où l'on déduit

$$ar(stq) = bpsrt = cp(stq)$$

donc $R\{x, z\}$, car stq appartient à S′. La relation R est donc transitive.

Soient par ailleurs $x = (a, p)$, $y = (b, q)$, $x' = (a', p')$ et $y' = (b', q')$ des éléments de E × S′ tels que l'on ait $R\{x, y\}$ et $R\{x', y'\}$. Il existe s et s' dans S′ tels que

$$aqs = bps, \qquad a'q's' = b'p's'$$

d'où l'on déduit $(aa')(qq')(ss') = (bb')(pp')(ss')$, donc $R\{xx', yy'\}$ car $ss' \in S'$. La relation d'équivalence R est donc compatible avec la loi de composition de E × S′.

Le magma quotient (E × S′)/R est un monoïde commutatif.

DÉFINITION 7. — *Soient* E *un monoïde* commutatif, S *une partie de* E *et* S′ *le sous-monoïde de* E *engendré par* S. *On note* E_S *et l'on appelle monoïde des fractions*[1] *de* E *associé à* S (*ou à dénominateurs dans* S) *le monoïde quotient* (E × S′)/R, *où la relation d'équivalence* R *est décrite comme dans le lemme* 1.

Pour $a \in E$ et $b \in S'$, la classe de (a, p) modulo R se note en général a/p et

[1] On dit aussi *monoïde des différences* si la loi de E est notée additivement.

s'appelle la *fraction* de *numérateur* a et *dénominateur* p. On a donc par définition $(a/p).(a'/p') = aa'/pp'$. Les fractions a/p et a'/p' sont égales si et seulement s'il existe s dans S′ avec $spa' = sp'a$; s'il en est ainsi, il existe σ et σ' dans S′ avec $a\sigma = a'\sigma'$ et $p\sigma = p'\sigma'$. En particulier, on a $a/p = sa/sp$ pour $a \in A$ et s, p dans S′. L'élément neutre de E_S est la fraction e/e.

On posera $a/e = \varepsilon(a)$ pour tout $a \in E$. Ce qui précède montre que ε est un homomorphisme de E dans E_S, dit *canonique*. Pour tout $p \in S'$, on a $(p/e).(e/p) = e/e$, donc e/p est inverse de $\varepsilon(p) = p/e$; tout élément de $\varepsilon(S')$ est donc inversible. On a $a/p = (a/e)(e/p)$, d'où

$$a/p = \varepsilon(a).\varepsilon(p)^* \tag{1}$$

pour $a \in A$ et $p \in S$; le monoïde E_S est donc engendré par $\varepsilon(E) \cup \varepsilon(S)^*$.

PROPOSITION 6. — *Les notations sont celles de la déf.* 7 *et* ε *désigne l'homomorphisme canonique de* E *dans* E_S.

(i) *Soient* a *et* b *dans* E; *pour qu'on ait* $\varepsilon(a) = \varepsilon(b)$, *il faut et il suffit qu'il existe* $s \in S'$ *avec* $sa = sb$.

(ii) *Pour que* ε *soit injectif, il faut et il suffit que tout élément de* S *soit simplifiable.*

(iii) *Pour que* ε *soit bijectif, il faut et il suffit que tout élément de* S *soit inversible.*

L'assertion (i) est claire, et entraîne que ε est injectif si et seulement si tout élément de S′ est simplifiable; mais l'ensemble des éléments simplifiables de E étant un sous-monoïde de E (I, p. 15, prop. 2), il revient au même de dire que tout élément de S est simplifiable.

Si ε est bijective, tout élément de S est inversible, car $\varepsilon(S)$ se compose d'éléments inversibles de E_S. Réciproquement, supposons tout élément de S inversible; alors tout élément de S′ est inversible (I, p. 16, cor. 2), donc simplifiable. Alors ε est injectif d'après (ii) et l'on a $a/p = \varepsilon(a.p^*)$ d'après (1), donc ε est surjectif.

THÉORÈME 1. — *Soient* E *un monoïde commutatif,* S *une partie de* E, E_S *le monoïde de fractions associé à* S *et* $\varepsilon: E \to E_S$ *l'homomorphisme canonique. Soit de plus* f *un homomorphisme de* E *dans un monoïde* F (*non nécessairement commutatif*), *tel que tout élément de* $f(S)$ *soit inversible dans* F. *Il existe un homomorphisme* $\bar{f}$ *et un seul de* E_S *dans* F *tel que* $f = \bar{f} \circ \varepsilon$.

Si $\bar{f}$ est un homomorphisme de E_S dans F tel que $f = \bar{f} \circ \varepsilon$, on a $\bar{f}(a/p) = \bar{f}(\varepsilon(a)\varepsilon(p)^*) = \bar{f}(\varepsilon(a))\bar{f}(\varepsilon(p))^* = f(a)f(p)^*$ pour $a \in E$ et $p \in S'$, d'où l'unicité de $\bar{f}$.

Soit g l'application de $E \times S'$ dans F définie par $g(a, p) = f(a).f(p)^*$. Montrons que g est un homomorphisme de $E \times S'$ dans F. Tout d'abord, on a $g(e, e) = f(e)f(e)^* = e$. Soient (a, p) et (a', p') deux éléments de $E \times S'$; comme a' et p commutent dans E, $f(a')$ et $f(p)$ commutent dans F, d'où $f(a')f(p)^* = {}^*(pf)f(a')$ d'après I, p. 16, prop. 5. On a par ailleurs $f(pp')^* = f(p'p)^* = (f(p')f(p))^* = f(p)^*f(p')^*$ d'après I, p. 16, prop. 4, d'où

$$g(aa', pp') = f(aa')f(pp')^* = f(a)f(a')f(p)^*f(p')^* = f(a)f(p)^*f(a')f(p')^*$$
$$= g(a,p)g(a',p').$$

Montrons que g est compatible avec la relation d'équivalence R dans $E \times S'$; si (a,p) et (a',p') sont congrus mod. R, il existe $s \in S'$ avec $spa' = sap'$, d'où $f(s)f(p)f(a') = f(s)f(a)f(p')$. Comme $f(s)$ est inversible, on en déduit $f(p)f(a') = f(a)f(p')$, puis, après multiplication à gauche par $f(p)^*$ et à droite par $f(p')^*$,

$$g(a',p') = f(a')f(p')^* = f(p)^*f(a) = f(a)f(p)^* = g(a,p).$$

Il existe donc un homomorphisme $\bar{f}$ de E_S dans F tel que $\bar{f}(a/p) = g(a,p)$ d'où $\bar{f}(\varepsilon(a)) = \bar{f}(a/e) = f(a)f(e)^* = f(a)$. On a donc $\bar{f} \circ \varepsilon = f$.

COROLLAIRE. — *Soient* E *et* F *deux monoïdes commutatifs*, S *et* T *des parties de* E *et* F *respectivement, f un homomorphisme de* E *dans* F *tel que* $f(S) \subset T$, *et* $\varepsilon: E \to E_S$, $\eta: F \to F_T$ *les homomorphismes canoniques. Il existe un homomorphisme* $g: E_S \to F_T$ *et un seul tel que* $g \circ \varepsilon = \eta \circ f$.

En effet, l'homomorphisme $\eta \circ f$ de E dans F_T transforme tout élément de S en un élément inversible de F_T.

Remarques. — 1) Le th. 1 peut encore s'énoncer en disant que (E_S, ε) est solution du problème d'application universelle pour E, relativement aux monoïdes, aux homomorphismes de monoïdes, et aux homomorphismes de E dans les monoïdes qui transforment les éléments de S en éléments inversibles (E, IV, p. 23). Il en résulte (*loc. cit.*) que toute autre solution de ce problème est isomorphe de façon unique à (E_S, ε).

2) Pour l'existence d'une solution du problème d'application universelle ci-dessus, il est inutile de supposer le monoïde E commutatif, ainsi qu'il résulte de E, IV, p. 23 et p. 24 (cf. I p. 121, exerc. 17).

Mentionnons deux cas particuliers importants de monoïdes de fractions.

a) Soit $\overline{E} = E_E$. Comme le monoïde $\overline{E}$ est engendré par l'ensemble $\varepsilon(E) \cup \varepsilon(E)^*$ qui se compose d'éléments inversibles, tout élément de $\overline{E}$ est inversible (I, p. 16, cor. 2). Autrement dit, $\overline{E}$ est un groupe commutatif. De plus d'après le th. 1, tout homomorphisme f de E dans un groupe G se factorise de manière unique sous la forme $f = \bar{f} \circ \varepsilon$ où $\bar{f}: \overline{E} \to G$ est un homomorphisme. On dit que $\overline{E}$ est le *groupe des fractions de* E (ou *groupe des différences de* E dans le cas de la notation additive).

b) Soit $\Phi = E_\Sigma$, où Σ se compose des éléments simplifiables de E. D'après I, p. 18, prop. 6, (ii), l'homomorphisme canonique de E dans Φ est injectif; on en profitera pour identifier E à son image dans Φ. Par suite, E est un sous-monoïde de Φ, tout élément simplifiable de E a un inverse dans Φ, et tout élément de Φ est de la forme $a/p = a.p^*$ avec $a \in E$ et $p \in \Sigma$; on a $a/p = a'/p'$ si et seulement si l'on a $ap' = pa'$. On voit facilement que les éléments inversibles de Φ sont les fractions a/p avec a et p simplifiables et que p/a est l'inverse de a/p.

Soit maintenant S un ensemble d'éléments simplifiables de E, et soit S' le sous-monoïde de E engendré par S. Si a/p et a'/p' sont deux éléments de E_S, on a $a/p = a'/p'$ si et seulement si $ap' = pa'$ (car $sap' = spa'$ entraîne $ap' = pa'$ pour tout $s \in S'$). On peut donc identifier E_S au sous-monoïde de Φ engendré par $E \cup S^*$.

Lorsque tout élément de E est simplifiable, on a $\Phi = \overline{E}$ et E est un sous-monoïde du groupe commutatif Φ. Inversement, si E est isomorphe à un sous-monoïde d'un groupe, tout élément de E est simplifiable.

5. Applications: I. Entiers rationnels

Considérons le monoïde commutatif **N** des entiers naturels, la loi de composition étant l'addition; tous les éléments de **N** sont simplifiables pour cette loi (E, III, p. 37, cor. 3). Le groupe des différences de **N** se note **Z**; ses éléments sont appelés les *entiers rationnels*; sa loi s'appelle *addition des entiers rationnels* et se note encore $+$. L'homomorphisme canonique de **N** dans **Z** est injectif, et nous identifierons chaque élément de **N** à son image dans **Z**. Les éléments de **Z** sont, par définition, les classes d'équivalence déterminées dans $\mathbf{N} \times \mathbf{N}$ par la relation $m_1 + n_2 = m_2 + n_1$ entre (m_1, n_1) et (m_2, n_2); un élément m de **N** est identifié avec la classe formée des éléments $(m + n, n)$ où $n \in \mathbf{N}$; il admet pour opposé dans **Z** la classe des éléments $(n, m + n)$. Tout élément (p, q) de $\mathbf{N} \times \mathbf{N}$ peut s'écrire sous la forme $(m + n, n)$ si $p \geqslant q$, sous la forme $(n, m + n)$ si $p \leqslant q$; il s'ensuit que **Z** est *la réunion de* **N** *et de l'ensemble des opposés des éléments de* **N**. L'élément neutre 0 est le seul élément de **N** dont l'opposé appartienne à **N**.

Pour tout entier naturel m, on note $-m$ l'entier rationnel opposé de m, et on note $-\mathbf{N}$ l'ensemble des éléments $-m$ pour $m \in \mathbf{N}$. On a

$$\mathbf{Z} = \mathbf{N} \cup (-\mathbf{N}) \quad \text{et} \quad \mathbf{N} \cap (-\mathbf{N}) = \{0\}.$$

Pour $m \in \mathbf{N}$, on a $m = -m$ si et seulement si $m = 0$.

Soient m et n deux entiers naturels;

a) si $m \geqslant n$, on a $m + (-n) = p$, où p est l'élément de **N** tel que $m = n + p$;

b) si $m \leqslant n$, on a $m + (-n) = -p$, où p est l'élément de **N** tel que $m + p = n$;

c) on a $(-m) + (-n) = -(m + n)$.

Les propriétés b) et c) résultent de I, p. 16, prop. 4; comme $\mathbf{Z} = \mathbf{N} \cup (-\mathbf{N})$, l'addition de **N** et les propriétés a), b) et c) caractérisent entièrement l'addition de **Z**.

Plus généralement on désigne par $-x$ l'opposé d'un entier rationnel quelconque x; le composé $x + (-y)$ se note, de façon abrégée, $x - y$ (cf. I, p. 23).

La relation d'ordre $\leqslant$ entre entiers naturels est caractérisée par la propriété suivante: on a $m \leqslant n$ si et seulement s'il existe un entier $p \in \mathbf{N}$ tel que $m + p = n$ (E, III, p. 29, prop. 13 et p. 36, prop. 2). La relation $y - x \in \mathbf{N}$ entre entiers rationnels x et y est une relation *d'ordre total* sur **Z**, qui prolonge la relation

d'ordre $\leqslant$ sur $\mathbf{N}$. En effet, pour tout $x \in \mathbf{Z}$, on a $x - x = 0 \in \mathbf{N}$; si $y - x \in \mathbf{N}$ et $z - y \in \mathbf{N}$, on a $z - x = (z - y) + (y - x) \in \mathbf{N}$ car $\mathbf{N}$ est stable pour l'addition; si $y - x \in \mathbf{N}$ et $x - y \in \mathbf{N}$, on a $y - x = 0$, car 0 est le seul élément de $\mathbf{N}$ dont l'opposé appartienne à $\mathbf{N}$; quels que soient les entiers rationnels x et y, on a $y - x \in \mathbf{N}$ ou $x - y \in \mathbf{N}$, car $\mathbf{Z} = \mathbf{N} \cup (-\mathbf{N})$; enfin si x et y sont des entiers naturels, on a $y - x \in \mathbf{N}$ si et seulement s'il existe $p \in \mathbf{N}$ tel que $x + p = y$. Cette relation d'ordre est encore notée $\leqslant$.

Lorsqu'on considérera désormais $\mathbf{Z}$ 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 identifiés aux entiers $\geqslant 0$: on les appelle encore entiers *positifs*; les entiers $\leqslant 0$, opposés 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 note parfois $\mathbf{N}^*$.

Soient x, y et z trois entiers rationnels; on a $x \leqslant y$ si et seulement si $x + z \leqslant y + z$. En effet $x - y = (x + z) - (y + z)$. On exprime cette propriété en disant que la relation d'ordre de $\mathbf{Z}$ est *invariante par translation.*

6. Applications: II. Multiplication des entiers rationnels

Lemme 2. — *Soient* E *un monoïde et* x *un élément de* E.

(i) *Il existe un unique homomorphisme* f *de* $\mathbf{N}$ *dans* E *tel que* $f(1) = x$, *et l'on a* $f(x) = \overset{n}{\top} x$ *pour tout* $n \in \mathbf{N}$.

(ii) *Si* x *est inversible, il existe un unique homomorphisme* g *de* $\mathbf{Z}$ *dans* E *tel que* $g(1) = x$ *et* g *coïncide avec* f *dans* $\mathbf{N}$.

Posons $f(n) = \overset{n}{\top} x$ pour tout $n \in \mathbf{N}$; les formules $\overset{0}{\top} x = e$ et $(\overset{m}{\top} x) \top (\overset{n}{\top} x) = \overset{m+n}{\top} x$ (I, p. 13) expriment que f est un homomorphisme de $\mathbf{N}$ dans E, et l'on a évidemment $f(1) = x$. Si f' est un homomorphisme de $\mathbf{N}$ dans E tel que $f'(1) = x$, on a $f = f'$ d'après I, p. 6, prop. 1 (iv).

Supposons x inversible. D'après I, p. 16, cor. 2, $f(n) = \overset{n}{\top} x$ est inversible pour tout entier $n \geqslant 0$. Par construction, $\mathbf{Z}$ est le groupe des différences de $\mathbf{N}$, donc (I, p. 18, th. 1), f se prolonge de manière unique en un homomorphisme g de $\mathbf{Z}$ dans E. Si g' est un homomorphisme de $\mathbf{Z}$ dans E tel que $g'(1) = x$, la restriction f' de g' à $\mathbf{N}$ est un homomorphisme de $\mathbf{N}$ dans E tel que $f'(1) = x$. On a donc $f' = f$, d'où $g' = g$.

Nous appliquerons le lemme 2 au cas où le monoïde E est $\mathbf{Z}$; pour tout entier $m \in \mathbf{Z}$, il existe donc un endomorphisme f_m de $\mathbf{Z}$ caractérisé par $f_m(1) = m$. Lorsque $m \in \mathbf{N}$, l'application $n \mapsto mn$ de $\mathbf{N}$ dans $\mathbf{N}$ est un endomorphisme du magma $\mathbf{N}$ (E, III, p. 27, corollaire); donc $f_m(n) = mn$ pour m, n dans $\mathbf{N}$.

On peut donc prolonger la multiplication dans $\mathbf{N}$ en une multiplication dans