ALGEBRE (ETAT 3)
CHAPITRE I
STRUCTURES ALGEBRIQUES

Rédaction n° 033

Nombre de pages : 141

Nombre de feuilles : 141

ALGEBRE (Etat 3)

CHAPITRE I

STRUCTURES ALGEBRIQUES

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

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

Par abus de langage, on dira qu'une telle loi est donnée (ou définie) sur E . Les lois de composition internes les plus importantes sont celles qui sont définies pour tous les couples $(x,y) \in E \times E$: par abus de langage, on dira qu'une telle loi est définie partout sur E . Le plus souvent, quand il sera question d'une loi de composition interne, on supposera, sauf mention expresse du contraire, qu'elle est définie partout.

D'après nos définitions générales (Ens.R, § 8, n° 2), la donnée d'une loi de composition entre éléments d'un ensemble E détermine une structure sur cet ensemble : c'est là une espèce particulière des structures algèbriques dont la définition générale sera donnée au § 4 de ce chapitre. Une telle structure est dite déterminée sur E par la loi de composition $(x,y) \to f(x,y)$. Conformément aux mêmes définitions générales (Ens.R, § 8, n° 5), si E et E' sont deux ensembles, f(x,y) et f'(x',y') des lois de composition définies respectivement entre éléments de E et éléments de E' et sur des parties A de E × E et A' de E' × E' , un isomorphisme de E sur E' (par rapport aux structures déterminées par ces lois) sera une application bijective de E sur E'

dont l'extension à $E \times E$ applique A sur A' et telle que la relation $z=f(x,y)$ entraîne la relation $z'=f'(x',y')$ entre les éléments x',y',z' correspondant à x,y,z. S'il existe un tel isomorphisme, E et E' seront dits isomorphes (par rapport aux structures déterminées par les lois f,f').

Le composé de x et y se note souvent en écrivant x et y dans un ordre déterminé et les séparant par un signe caractéristique de la loi envisagée (signe qu'on pourra convenir d'omettre éventuellement). Parmi les signes dont l'emploi est le plus fréquent, citons dès maintenant + et ., 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'appellera le plus souvent <u>addition</u> (le composé $x+y$ s'appelant alors la <u>somme</u> de x et y), et on dira qu'elle est <u>notée additivement</u> ; une loi notée par . s'appellera le plus souvent <u>multiplication</u> (le composé $x.y = xy$ s'appelant alors <u>produit</u> de x et y), et on dira qu'elle est <u>notée multiplicativement</u>. Dans les raisonnements généraux des §§1,2,3 du présent chapitre, on se servira ordinairement des signes $\top$ et $\bot$ pour noter des lois de composition quelconques.

<u>Exemples</u>. 1) Les applications $(A,B) \to A \cup B$ et $(A,B) \to A \cap B$ sont des lois de composition internes (partout définies) entre parties d'un ensemble E .

2) Dans l'ensemble $\mathbb{N}$ des entiers naturels, l'addition, la multiplication, l'exponentiation sont des lois de composition partout définies (les composés de $x \in \mathbb{N}$ et $y \in \mathbb{N}$ par ces lois se notant respectivement $x+y, x.y=xy$ et x^y) : v.Ens., chap.III, § .

3) E étant un ensemble, l'application $(A,B) \to A \circ B$ est une loi de composition entre parties de $E \times E$ (Ens.R, §3, n°10) ; l'application $(f,g) \to f \circ g$ est une loi de composition entre applications de E dans E (Ens.R, § 2, n° 11).

4) Soit E un ensemble ordonné réticulé (Ens.R, § 6) : si on désigne par sup(x,y) la borne supérieure de l'ensemble formé des éléments x et y , l'application $(x,y) \to \sup(x,y)$ est une loi de composition entre éléments de E . De même pour la borne inférieure inf(x,y) . L'exemple 1) ci-dessus rentre dans celui-ci, en considérant $\mathfrak{P}(E)$ comme ordonné par inclusion.

5) Soit $(x,y) \to x \top y$ une loi de composition entre éléments de E , définie sur une partie A de $E \times E$. Si X et Y sont des parties de E , l'ensemble des éléments $x \top y$ de E pour $x \in X$, $y \in Y$, $(x,y) \in A$ (c'est-à-dire l'image par $(x,y) \to x \top y$ de la trace de $X \times Y$ sur A) est une partie de E qu'on désignera (pourvu que cette notation ne prête pas à confusion) par $X \top Y$: l'application $(X,Y) \to X \top Y$ est une loi de composition <u>partout définie</u>, entre parties de E .

Voici un exemple où le principe de notation qu'on vient de poser prêterait à confusion et ne devra donc pas s'appliquer. Supposons qu'il s'agisse de la loi de composition $A \cup B$ entre parties d'un ensemble E : d'après la règle formulée à l'ex. 5 on en déduit une loi de composition $(\mathscr{A}, \mathscr{B}) \to F(\mathscr{A}, \mathscr{B})$ entre parties de $\mathfrak{P}(E)$, $F(\mathscr{A}, \mathscr{B})$ étant l'ensemble des $A \cup B$ pour $A \in \mathscr{A}$, $B \in \mathscr{B}$; mais $F(\mathscr{A}, \mathscr{B})$ ne devra pas se noter $\mathscr{A} \cup \mathscr{B}$, cette notation ayant déja un sens différent (réunion de $\mathscr{A}$ et $\mathscr{B}$ considérées comme parties de $\mathfrak{P}(E)$).

Soit $(x,y) \to x \top y$ une loi de composition partout définie entre éléments de E : l'application $(x,y) \to y \top x$ sera aussi une loi de composition partout définie, qui sera dite opposée à la précédente. Si la loi $x \top y$ est définie sur une partie A de $E \times E$, on aura $(y,x) \in A$ chaque fois que $(x,y) \in {}^{-1}A$ (Ens.R, §3, n°4), donc $(x,y) \to y \top x$ sera une application de ${}^{-1}A$ dans E, qui s'appellera encore la loi de composition opposée à la précédente. En d'autres termes :

Définition 2. Deux lois de composition (partout définies ou non) entre éléments de E sont dites opposées si chacune se déduit de l'autre par composition avec la symétrie canonique de $E \times E$. Si l'une est partout définie, il en est de même de l'autre.

2. Lois de composition associatives. Définition 3. Une loi de composition $x \top y$ partout définie, entre éléments d'un ensemble E, est dite associative si l'on a, quels que soient x,y,z dans E :

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

Lorsque la loi $x \top y$ n'est pas partout définie, on dit parfois qu'elle est associative si la loi de composition $X \top Y$ qu'on en déduit (v.ci-dessus, ex.5) entre parties de E, et qui, elle, est partout définie, est associative ; d'autres fois, on dit qu'elle est associative si la relation $(x \top y) \top z = x \top (y \top z)$ est vérifiée chaque fois que les deux membres sont définis. Une partie des résultats qui suivent s'étend, avec des modifications convenables, aux lois associatives non partout définies.

Exemples. Parmi les exemples de lois de composition indiqués ci-dessus, les suivantes sont associatives : $A \cup B$ et $A \cap B$ (ex.1); $x+y$ et $x.y$ (ex.2) ; $A \circ B$ et $f \circ g$ (ex.3) ; $\sup(x,y)$ et $\inf(x,y)$ (ex.4). Si $x \top y$ est une loi associative entre éléments de E,

$X \top Y$ est une loi associative entre éléments de $\mathfrak{P}(E)$.

En revanche, l'exponentiation x^y entre entiers naturels (ex.2) n'est pas associative ; en effet $(2^1)^2 \neq 2^{(1^2)}$.

Lorsqu'on s'est donné une loi associative, il y a lieu de définir le composé d'éléments en nombre fini quelconque, pris dans un ordre déterminé ; on le définira par récurrence sur le nombre des éléments : $x \top y$ étant défini par la loi de composition, $x \top y \top z$ sera par définition la valeur commune de $(x \top y) \top z$ et $x \top (y \top z)$. Plus généralement :

Définition 4. On appelle séquence d'éléments de E une famille $(x_\alpha)_{\alpha \in A}$ d'éléments de E dont l'ensemble A des indices est un ensemble fini totalement ordonné. Les éléments x_α s'appellent les termes de la séquence (x_α). Deux séquences $(x_\alpha)_{\alpha \in A}$, $(x_\beta)_{\beta \in B}$ sont dites semblables si elles se déduisent l'une de l'autre par une application biunivoque croissante de A sur B .

On sait (Ens., chap.IV, §) qu'un ensemble fini non vide, totalement ordonné, admet toujours une application biunivoque croissante et une seule sur un intervalle $[0, n-1]$ de l'ensemble $\mathbb{N}$ des entiers naturels; toute séquence non vide est donc semblable à une suite finie et une seule admettant un tel intervalle pour ensemble d'indices.

Soient $x \top y$ une loi de composition associative sur E , $(x_\alpha)_{\alpha \in A}$ une séquence non vide d'éléments de E ; à toute partie non vide B de A , on peut faire correspondre un élément de E , qu'on notera $\top_{\alpha \in B} x_\alpha$, de la manière suivante :

1°- si $B = \{\beta\}$, on posera $\top_{\alpha \in B} x_\alpha = x_\beta$;

2°- si B a plus d'un élément et a pour plus petit élément β , et si B' désigne l'ensemble des éléments $> \beta$ dans B , on posera

$$\top_{\alpha \in B} x_\alpha = x_\beta \top \left(\top_{\alpha \in B'} x_\alpha \right) .$$

En effet, on voit par récurrence sur p que ces conditions déterminent d'une manière unique $\top_{a \in B} x_a$ pour toutes les parties B de A à p éléments, quel que soit $p \leqslant n$ si A est à n éléments.

Définition 5. L'élément $\top_{a \in A} x_a$, déterminé par les conditions ci-dessus, s'appelle le composé de la séquence $(x_a)_{a \in A}$ pour la loi $x \top y$.

Il est clair que deux séquences semblables ont même composé. Le composé d'une séquence à deux termes x_α, x_β (correspondant à $A = \{\alpha, \beta\}$, $\alpha < \beta$) n'est autre que $x_\alpha \top x_\beta$.

Du point de vue des notations, le composé d'une séquence se notera $\top_{a \in A} x_a$ pour une loi notée $\top$; $\perp_{a \in A} x_a$ pour une loi notée $\perp$; pour une loi notée + (addition) et pour une loi notée · (multiplication), il est d'usage de le désigner respectivement par les notations suivantes

$$\sum_{a \in A} x_a \qquad \text{et} \qquad \prod_{a \in A} x_a$$

(cette dernière devant cependant être évitée lorsqu'elle peut entraîner confusion avec le signe analogue de la Théorie des Ensembles).

Lorsqu'il s'agit d'une suite, ayant pour ensemble d'indices l'intervalle $\{n+1, n+p\}$ de $\mathcal{N}$, le composé de la suite se note également $\top_{i=n+1}^{n+p} x_i$, ou $x_{n+1} \top x_{n+1} \top \dots \top x_{n+p}$ et de même pour des lois notées $\perp$, + ou ·.

On observera que la définition 5 reste légitime même s'il s'agit d'une loi non associative, mais partout définie. (Pour une loi non définie partout, on peut encore la conserver, mais on ne définira ainsi de composé que pour les séquences satisfaisant à certaines conditions). Cependant, l'intérêt de cette définition tient avant tout au théorème suivant, qui ne vaut que pour les lois associatives :

Théorème 1 (théorème d'associativité). Soit A fini non vide, totalement ordonné, réunion de parties non vides B_i $(1 \leqslant i \leqslant p)$ telles que $x \in B_i$, $y \in B_{i+1}$ entraîne $x < y$ quel que soit $i < p$; soit $(x_\alpha)_{\alpha \in A}$ une séquence d'éléments de E, ayant A pour ensemble d'indices ; on a alors, pour toute loi associative $\top$ donnée sur E :

$$\top_{\alpha \in A} x_\alpha = \top_{1 \leqslant i \leqslant p} \left(\top_{\alpha \in B_i} x_\alpha \right)$$

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

a) B_1 est réduit à un seul élément β. Soit $C = B_2 \cup B_3 \cup \ldots \cup B_p$. Le premier membre de l'égalité à démontrer n'est autre (par définition) que $x_\beta \top \left(\top_{\alpha \in C} x_\alpha \right)$; le second membre n'est autre (par définition) que $x_\beta \top \left(\top_{2 \leqslant i \leqslant p} \left(\top_{\alpha \in B_i} x_\alpha \right) \right)$: l'égalité résulte de ce que le théorème est supposé vrai (C étant à n-1 éléments) pour C et $B_2, B_3, \ldots, B_n$.

b) Sinon, soit β le plus petit élément de A (donc de B_1) ; soient A' l'ensemble des α β dans A, $B'_1 = A' \; B_1$; A' est à n-1 éléments et les conditions du théorème sont satisfaites par A' et $B'_1, B_2, \ldots, B_p$, donc on a par hypothèse

$$\top_{\alpha \in A'} x_\alpha = \left(\top_{\alpha \in B'_1} x_\alpha \right) \top \left(\top_{2 \leqslant i \leqslant p} \left(\top_{\alpha \in B_i} x_\alpha \right) \right)$$

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

$$\left(x_\beta \top \left(\top_{\alpha \in B'_1} x_\alpha \right) \right) \top \left(\top_{2 \leqslant i \leqslant p} \left(\top_{\alpha \in B_i} x_\alpha \right) \right)$$

ce qui n'est autre chose (par la définition 5) que le second membre de la formule du th.1, qui est donc démontré.

Un cas particulier du théorème général d'associativité est la formule

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

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

Lorsque tous les termes d'une séquence de n termes sont égaux à un même $x \in E$, leur composé se notera $\overset{n}{\top} x$ pour une loi notée $\top$, $\overset{n}{\perp} x$ pour une loi notée $\perp$, x^n pour une loi notée ., et le plus souvent nx pour une loi notée + (sauf certains cas où cette dernière notation pourrait prêter à confusion, v. § 3). Le théorème d'associativité devient, si $n, n_1, n_2, \dots, n_p$ sont les nombres d'éléments de A et des B_i respectivement (donc $n = n_1 + n_2 + \dots + n_p$), et si $x_\alpha = x$ quel que soit α :

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

donc en particulier, si $p=2$

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

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

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

Si X est une partie de E, on désignera, conformément aux notations ci-dessus, par $\overset{p}{\top} X$ l'ensemble $X_1 \top X_2 \top \dots \top X_p$ pour $X_1 = X_2 = \dots = X_p = X$: c'est donc l'ensemble de tous les composés $x_1 \top x_2 \top \dots \top x_p$ pour $x_1 \in X$, $x_2 \in X$, ..., $x_p \in X$. Il importe de ne pas confondre cet ensemble avec l'ensemble des éléments $\overset{p}{\top} x$ pour $x \in X$. On posera $\overset{\infty}{\top} X = \bigcup_{p \in \mathbb{N}, p>0} (\overset{p}{\top} X)$: c'est l'ensemble des composés de toutes les suites finies (donc aussi de toutes les séquences) dont tous les termes appartiennent à X.

3. Parties stables. Définition 6. Une partie A de E est dite stable pour une loi de composition entre éléments de E si le composé de deux éléments de A appartient à A chaque fois qu'il est défini.

Autrement dit, pour que A soit stable par rapport à une loi $\top$, il faut et il suffit que l'on ait $A \top A \subset A$.

L'intersection d'une famille de parties stables de E est évidemment stable, donc en particulier il existe une plus petite partie stable de E contenant une partie X donnée (Ens. R, § 6, n° 5), qui est dite engendrée par X.

Théorème 2. $\top$ étant une loi associative sur E, la partie stable de E engendrée par une partie X de E est $\overset{\infty}{\top} X$.

En effet, Z étant cette partie stable, on démontre par récurrence sur n que le composé de toute séquence de n termes appartenant à X appartient nécessairement à Z, donc $\overset{\infty}{\top} X \subset Z$. Réciproquement, si u et v sont des éléments de $\overset{\infty}{\top} X$, ils seront de la forme $u = x_0 \top x_1 \top \dots \top x_{n-1}$, $v = x_n \top x_{n+1} \top \dots \top x_{n+p}$, avec $x_i \in X$ $(0 \leqslant i \leqslant n+p)$, donc (par le th. 1) $u \top v = x_0 \top x_1 \top \dots \top x_{n+p} \in \overset{\infty}{\top} X$, d'où suit que $\overset{\infty}{\top} X$ est stable et contient donc Z.

Définition 7. $\top$ étant une loi de composition entre éléments de E, définie sur une partie A de $E \times E$, on appelle loi induite par la loi $\top$ sur une partie F de E la loi de composition entre éléments de F, définie sur l'ensemble des $(x,y) \in F \times F$ tels que $(x,y) \in A$, $x \top y \in F$, et qui, à un tel couple (x,y) fait correspondre le composé $x \top y$. La structure déterminée par cette loi sur F sera dite induite sur F par la structure déterminée par $\top$ sur E.

La loi induite par $\top$ sur F pourra (par abus de langage) être désignée par le même signe $\top$, quand cette notation ne prêtera pas

à confusion. Si la loi $\top$ est définie partout sur $E \times E$, et si F est une partie stable de E par rapport à cette loi, la loi induite par $\top$ sur F est définie partout.

4. Eléments permutables ; lois commutatives. Définition 8. $\top$ étant une loi de composition entre éléments de E, deux éléments x,y de E sont dits permutables (ou échangeables) si $x \top y$ et $y \top x$ sont définis et si $x \top y = y \top x$.

Définition 9. Une loi de composition entre éléments de E est dite commutative si deux éléments quelconques de E sont permutables.

Une loi commutative est identique à son opposée.

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

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

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

Proposition 1. $\top$ étant une loi associative, si un élément x est permutable avec chacun des éléments y et z, il l'est aussi avec $y \top z$

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

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

Proposition 2. Si tout élément d'une partie X de E est permutable (pour une loi associative $\top$) avec tout élément d'une partie Y de E , tout élément de la partie stable engendrée par X est permutable avec tout élément de la partie stable engendrée par Y .

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

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

Corollaire 1. Si x et y sont permutables pour la loi associative $\top$, 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 $x, m>0$ et $n>0$.

Corollaire 2. Si tous les éléments de X sont permutables deux à deux par rapport à une loi associative $\top$, la loi induite par $\top$ sur la partie stable engendrée par X est associative et commutative.

Définition 10. On appelle élément central de E , pour une loi de composition entre éléments de E , tout élément permutable avec tous les éléments de E . On appelle centre de E l'ensemble des éléments centraux.

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

La principale propriété des lois associatives et commutatives consiste en ce que les composés de toutes les séquences qu'on peut déduire

d'une séquence donnée par permutation sur les indices ont même valeur : ce qu'on va démontrer maintenant.

Définition 11. On appelle système d'éléments de E toute famille d'éléments de E dont l'ensemble d'indices est fini.

D'un système on déduit une séquence en ordonnant totalement l'ensemble d'indices, ou (ce qui revient au même, cf. Ens., chap.IV, §) en choisissant une correspondance biunivoque entre cet ensemble et un intervalle $[0,n-1]$ de $\mathbb{N}$.

Théorème 3. Soit $\top$ une loi de composition associative et commutative sur E ; soit $(x_\alpha)_{\alpha \in A}$ un système non vide d'éléments de E ; quelle que soit la manière dont on ordonne totalement A , le composé $\top_{\alpha \in A} x_\alpha$ a une même valeur.

Le théorème est vrai si A a un seul élément α_0 , le composé étant alors x_{α_0} . Montrons par récurrence sur p qu'il est vrai pour toute partie de A à p éléments : il suffira de montrer qu'il est vrai pour un ensemble d'indices à p éléments s'il est vrai pour toute partie de cet ensemble à moins de p éléments. Soit donc $A=\{\alpha_0,\alpha_1,\dots,\alpha_{p-1}\}$; pour un ordre quelconque de A , soit α_i le plus petit élément de A , A' l'ensemble des autres éléments de A ; on a $\top_{\alpha \in A} x = x_{\alpha_i} \top (\top_{\alpha \in A'} x_\alpha)$. Supposons d'abord $0<i<p-1$, et posons $B=\{\alpha_0,\alpha_1,\dots,\alpha_{i-1}\}$ et $C=\{\alpha_{i+1},\dots,\alpha_{p-1}\}$; le théorème étant supposé vrai pour A' , on a, en appliquant de plus le théorème d'associativité (puisque $A'=B \cup C$) :

$$\top_{\alpha \in A'} x_\alpha = (\top_{j=0}^{i-1} x_{\alpha_j}) \top (\top_{k=i+1}^{p-1} x_{\alpha_k})$$

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

$$\top_{a\in A} x_a = x_{a_i} \top \Big(\top_{j=0}^{i-1} x_{a_j}\Big) \top \Big(\top_{k=i+1}^{p-1} x_{a_k}\Big) = \Big(\top_{j=0}^{i-1} x_{a_j}\Big) \top x_{a_i} \top \Big(\top_{k=i+1}^{p-1} x_{a_k}\Big) = \top_{h=0}^{p-1} x_{a_h}$$

où le dernier membre est bien indépendant de l'ordre de A . Si i=0 ou i=p-1 , on trouve le même résultat mais d'une manière plus simple, les termes relatifs à B ou bien les termes relatifs à C disparaissant des formules. Le théorème est démontré.

Définition 12. Pour une loi associative et commutative sur E , on appelle composé d'un système non vide $(x_a)_{a\in A}$ d'éléments de E le composé de l'une quelconque des séquences obtenues en ordonnant totalement l'ensemble d'indices A du système.

Pour une loi notée $\top$, ce composé se notera $\top_{a\in A} x_a$; de même pour les autres notations.

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

Théorème 4. Soient $\top$ une loi associative et commutative sur E , $(x_a)_{a\in A}$ un système non vide d'éléments de E . Si A est réunion de parties non vides $B_1, B_2, \ldots, B_p$, deux à deux sans élément commun, on a

$$\top_{a\in A} x = \top_{i=1}^{p} \Big(\top_{a\in B_i} x_a\Big)$$

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

D'après le corollaire 2 de la prop.2, les th.3 et 4 s'appliquent encore s'il s'agit d'une loi associative et de systèmes d'éléments deux à deux permutables.

Exercices. *1) Montrer que les seuls entiers distincts >0 qui soient permutables pour la loi $(x,y)\to x^y$ sont 2 et 4 . *

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

3) Déterminer le centre pour la loi $f \circ g$ entre applications de E dans E .

4) La loi $\top$ étant définie sur E , on pose, pour h fixe dans E , $x \perp y = x \top h \top y$: montrer que si $\top$ est associative, $\perp$ l'est également.

5) Pour une loi associative $\top$ entre éléments de E , soit $h \in E$ tel que $h \top h = h$ (un tel élément est dit <u>idempotent</u>) : montrer que l'ensemble des éléments $h \top x \top h$, où $x \in E$, est une partie stable de E .

6) A étant un ensemble donné, soient E l'ensemble des suites finies d'éléments de A (séquences dont l'ensemble d'indices est une partie finie de $\mathcal{N}$) : si $S \in E$, $S' \in E$, la relation "S est semblable à S' " (déf.4) est une relation d'équivalence $\sum$ dans E : soit $L(A) = E / \sum$. Soit $S = (a_i)_{i \in I}$ une suite appartenant à E : si $I = I' \cup I''$, et si $j \in I'$, $k \in I''$ entraîne $j < k$, montrer que la classe d'équivalence de S dans E ne dépend que des classes auxquelles appartiennent les suites $S' = (a_i)_{i \in I'}$, $S'' = (a_i)_{i \in I''}$. La classe de S sera dite composée des classes de S' et S" par juxtaposition : montrer que c'est là une loi de composition associative entre éléments de L(A) , que L(A) est engendré par l'ensemble A' des classes formées de suites à un seul élément, et que A' est équipotent à A . On dit que L(A) est <u>le système associatif libre</u> déduit de A , et que les éléments de L(A) sont les <u>mots</u> formés avec les éléments de A . Montrer que les systèmes $L(A_1)$, $L(A_2)$ ainsi déduits de deux ensembles A_1, A_2 équipotents sont isomorphes. Si A est fini et à n éléments, L(A) s'appelle le système associatif libre à n générateurs, et, si $A = \{a_1, a_2, \ldots, a_n\}$, les éléments de L(A) sont appelés les mots formés avec les n signes a_i .

§ 2. Elément neutre ; éléments réguliers ; éléments inversibles.

1. Elément neutre. Définition 1. Pour une loi de composition $\top$ entre éléments de E , un élément e de E est dit élément neutre si $e\top x$ et $x\top e$ sont définis et égaux a x , quel que soit $x \in E$.

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

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

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

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

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

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

Si E contient un élément neutre e pour une loi $\top$, et si F est une partie stable de E qui contienne e , e est élément neutre pour la loi

induite par $\top$ sur F . Mais il peut se faire que la loi induite par $\top$ sur une partie stable F ait un élément neutre f sans que F contienne e , ou, même sans qu'il existe d'élément neutre pour $\top$ dans E .

Par exemple, si $\top$ est associative sur E , et si $h \top h = h$, h est élément neutre pour la loi induite par $\top$ sur l'ensemble des éléments $h \top x \top h$, $x \in E$ (cf. § 1, exerc. 4) ; il pourra en être ainsi sans que h soit élément neutre pour $\top$ dans E . En particulier, si $\top$ est la loi $\sup(x,y)$ sur un ensemble ordonné réticulé E , on pourra prendre pour h un élément quelconque de E .

Définition 2. Si e est élément neutre pour une loi associative entre éléments de E , on appellera composé d'une séquence vide d'éléments de E l'élément neutre e . De même pour le composé d'un système vide si la loi est associative et commutative.

Si donc $\emptyset$ est la partie vide d'un ensemble d'indices, on écrira, dans les conditions de la définition 2 , $\top_{\alpha \in \emptyset} x_\alpha = e$; on posera de même $\overset{0}{\top} x = e$ quel que soit x . Avec ces définitions, les théorèmes 1 et 4 du § 1 restent vrais si l'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 $m \geqslant 0$, $n \geqslant 0$.

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

2. Eléments réguliers. Définition 3. $\top$ étant une loi de composition, partout définie, entre éléments de E , on appelle translation à gauche correspondant à $a \in E$ l'application $x \to a \top x$ de E dans lui-même ; translation à droite l'application $x \to x \top a$.

Les noms "translation à droite", "translation à gauche" tiennent uniquement, bien entendu, à la notation habituelle de la plupart des lois de composition. Par passage d'une loi à la loi opposée, les translations à gauche deviennent translations à droite et réciproquement.

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

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

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

En effet : $\gamma_{x \top y}(z) = (x \top y) \top z = x \top (y \top z) = \gamma_x(\gamma_y(z))$

$\delta_{x \top y}(z) = z \top (x \top y) = (z \top x) \top y = \delta_y(\delta_x(z))$

Définition 4. $\top$ étant une loi de composition partout définie entre éléments de E , un élément $a \in E$ est dit régulier pour $\top$ si les translations à droite et à gauche correspondant à a sont des applications biunivoques de E dans lui-même.

Autrement dit, pour que a soit régulier, il faut et il suffit que chacune des relations $a \top x = a \top y$, $x \top a = y \top a$ entraîne $x = y$ (on dit qu'on peut "simplifier par a" ces égalités). Il s'ensuit que si X et Y sont des parties de E , chacune des relations $a \top X = a \top Y$, $X \top a = Y \top a$ entraîne $X = Y$.

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

2) S'il existe un élément neutre pour une loi $\top$, il est régulier pour cette loi.

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

Proposition 2. L'ensemble des éléments réguliers pour une loi associative est stable pour cette loi.

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

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

3. Eléments inverses. Définition 5. $\top$ étant une loi de com-position entre éléments de E , admettant un élément neutre e , on dit que $x \in E$ est inversible s'il existe x' tel que $x \top x' = x' \top x = e$, et un tel élément x' est dit inverse de x .

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

2) Dans l'ensemble des applications de E dans E , les éléments inversibles, pour la loi $f \circ g$, sont les applications

biunivoque de E sur E : pour une telle application f , l'application réciproque de f est inverse de f .

Proposition 3. Pour une loi associative $\top$ sur E , tout élément inversible x est régulier et a un seul inverse ; les translations à droite et à gauche correspondantes γ_x et δ_x , sont des applications biunivoques de E sur E .

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

Proposition 4. $\top$ étant une loi associative sur E , si $x\in E$ est tel que les translations à gauche et à droite γ_x, δ_x soient toutes deux des applications de E sur E , il existe un élément neutre pour $\top$, et x est inversible.

γ_x applique E sur E , donc il existe $e\in E$ tel que $\gamma_x(e)=x$, ou $x\top e=x$; δ_x applique E sur E , donc il existe, quel que soit $y\in E$, un $z\in E$ tel que $z\top x=y$; on a alors $y\top e=z\top x\top e=z\top x=y$. On voit de même (en échangeant γ et δ) qu'il existe e' tel que $e'\top y=y$ quel que soit y . Mais alors on a , d'une part $e'\top e=e'$, de l'autre $e'\top e=e$, donc $e=e'$, $y\top e=e\top y=y$ quel que soit y ; e est élément neutre. Alors, il existe x' et x" tels que $x\top x'=e$, $x"\top x=e$: donc $x"\top(x\top x')=x"$, $(x"\top x)\top x'=x'$, d'où $x'=x"$, et x' est inverse de x .

Proposition 5. Si, pour une loi associative $\top$, deux éléments x,y admettent des inverses x',y' , le composé $x\top y$ est inversible et a pour inverse $y'\top x'$; si chacun des éléments x_α d'une séquence $(x_\alpha)_{\alpha\in A}$

a un inverse x'_α, le composé $\top_{\alpha \in A} x_\alpha$ est inversible et a pour inverse $\top_{\alpha \in A'} x'_\alpha$, où A' est l'ensemble ordonné déduit de A obtenu en remplaçant l'ordre de A par l'ordre opposé.

Le premier point résulte de $(y' \top x') \top (x \top y) = y' \top (x' \top x) \top y = y' \top y = e$, et du calcul analogue pour $(x \top y) \top (x' \top y')$; le second s'en déduit par récurrence sur le nombre de termes de la séquence .

En particulier, si x a pour inverse x' , $\overset{n}{\top} x$ a pour inverse $\overset{n}{\top} x'$.

Corollaire. Pour une loi associative, l'ensemble des éléments inversibles est stable.

Proposition 6. Si, pour une loi associative, x et x' sont inverses l'un de l'autre, et si x est permutable avec y , il en est de même de x' .

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. L'inverse de tout élément inversible du centre appartient également au centre.

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

Proposition 7. Soit $\top$ une loi associative entre éléments de E , admettant un élément neutre e ; soient X une partie de E , et X" la partie stable de E engendrée par la réunion X' de X , de $\{e\}$, et de l'ensemble des inverses des éléments inversibles de X ; soient $Y \subset E$, et Y" formé à partir de Y comme X" l'est à partir de X .

Alors, si tout élément de X est permutable avec tout élément de Y , tout élément de X" est permutable avec tout élément de Y" .

4. Prolongement d'une loi associative et commutative. Un élément $x \in E$, inversible pour une loi $\top$, est régulier pour la loi induite par $\top$ sur toute partie stable de E. On peut se demander, réciproquement, si, E et $\top$ étant donnés, on peut plonger E dans un ensemble plus étendu $\overline{E}$ et définir sur $\overline{E}$ une loi de composition qui induise $\top$ sur E, et pour laquelle tout élément régulier de $\overline{E}$, ou tout au moins tout élément régulier de E, soit inversible. Il n'en est pas toujours ainsi ; mais on a du moins l'important théorème suivant :

Théorème 1. Soit $\top$ une loi de composition associative et commutative entre éléments d'un ensemble E. On peut définir un ensemble $\overline{E}$, une loi de composition associative et commutative $\overline{\top}$ entre éléments de $\overline{E}$, et une partie H de $\overline{E}$ stable pour la loi $\overline{\top}$, de manière à satisfaire aux conditions suivantes :

1° tout élément de $\overline{E}$, régulier pour la loi $\overline{\top}$, est inversible ;

2° E (avec la loi $\top$) est isomorphe à H (avec la loi induite sur H par $\overline{\top}$), par un isomorphisme qui, à tout élément régulier de E, fasse correspondre un élément de H régulier (donc inversible) dans $\overline{E}$;

3° $\overline{E}$ est engendré par la réunion de H et de l'ensemble H' des inverses des éléments réguliers de H.

De plus, $\overline{E}$ est déterminé d'une manière unique (à un isomorphisme près) par ces conditions.

Soit E^* l'ensemble des éléments réguliers de E. Si E^* est vide, il suit de 3° que $\overline{E}$ doit être égal à H : alors $\overline{E}$ est nécessairement isomorphe à E ; mais E satisfaisant alors aux conditions du théorème, tout est démontré dans ce cas. Supposons donc $E^* \neq \emptyset$.

Si $\overline{E}$ satisfait aux conditions ci-dessus, tout élément de $\overline{E}$ est composé d'un système d'éléments de $H \cup H'$: par le th.4 du § 1, il est donc de la forme $u \,\overline{\top}\, v'$, où u est le composé d'un système d'éléments de H et v' d'un système d'éléments de H' ; H étant stable,

on a $u \in H$; par la prop.5 , on a $v' \in H'$. Donc tout élément de $\overline{E}$ est de la forme $u \overline{\top} v'$, où $u \in H$, et où v' est l'inverse d'un élément régulier v de H . Soit H^* l'ensemble des éléments réguliers de H ; à tout élément (u,v) de $H \times H^*$, faisons correspondre l'élément $u \overline{\top} v'$ de $\overline{E}$, v' désignant l'inverse de v : on a ainsi une application de $H \times H^*$ sur $\overline{E}$; à (u_1,v_1) et (u_2,v_2) dans $H \times H^*$ correspondra un même élément de $\overline{E}$ si l'on a $u_1 \overline{\top} v_1' = u_2 \overline{\top} v_2'$; v_1 étant régulier, cette relation est équivalente à $u_1 \overline{\top} v_1' \overline{\top} v_1 = u_2 \overline{\top} v_2' \overline{\top} v_1$, c'est-à-dire $u_1 = u_2 \overline{\top} v_2' \overline{\top} v_1$, puis (v_2 étant régulier) à $u_1 \overline{\top} v_2 = u_2 \overline{\top} v_2' \overline{\top} v_1 \overline{\top} v_2$, c'est-à-dire à $u_1 \overline{\top} v_2 = u_2 \overline{\top} v_1$; enfin, si (u_1,v_1) et (u_2,v_2) sont des éléments quelconques de $H \times H^*$, auquels correspondent dans $\overline{E}$ les éléments $w_1 = u_1 \overline{\top} v_1'$, $w_2 = u_2 \overline{\top} v_2'$, à $(u_1 \overline{\top} u_2, v_1 \overline{\top} v_2)$ correspondra (puisque l'inverse de $v_1 \overline{\top} v_2$ est $v_1' \overline{\top} v_2'$), l'élément $u_1 \overline{\top} u_2 \overline{\top} v_1' \overline{\top} v_2'$, c'est-à-dire $w_1 \overline{\top} w_2$.

Par l'isomorphisme entre E et H , à tout élément (x,y) de $E \times E^*$ correspond un élément $(u,v) \in H \times H^*$, puis $w = u \overline{\top} v' \in \overline{E}$; à deux éléments (x_1,y_1) et (x_2,y_2) correspond un même élément w de $\overline{E}$ si $x_1 \top y_2 = x_2 \top y_1$; et si à (x_1,y_1) et (x_2,y_2) correspondent respectivement w_1 et w_2 dans $\overline{E}$, à $(x_1 \top x_2, y_1 \top y_2)$ correspond $w_1 \overline{\top} w_2$. Enfin, si à $x \in E$ correspond $u \in H$, à tout élément de la forme $(x \top y, y)$ dans $E \times E^*$, où $y \in E^*$, correspond dans $H \times H^*$, l'élément $(u \overline{\top} v, v)$ où $v \in H^*$ correspond à y , puis dans $\overline{E}$, si v' est l'inverse de v , l'élément $(u \overline{\top} v) \overline{\top} v'$, c'est-à-dire u lui-même.

Or la relation $x_1 \top y_2 = x_2 \top y_1$ entre éléments (x_1,y_1) et (x_2,y_2) de $E \times E^*$ est une relation d'équivalence R : car elle est évidemment réflexive et symétrique ; et si $x_1 \top y_2 = x_2 \top y_1$, $x_2 \top y_3 = x_3 \top y_2$, on a $x_1 \top y_2 \top y_3 = x_2 \top y_1 \top y_3 = x_3 \top y_2 \top y_1$, donc (y_1 étant régulier), $x_1 \top y_3 = x_3 \top y_1$.

Il s'ensuit que, si $\overline{E}$ est défini, il existe une correspondance biunivoque entre $\overline{E}$ et l'ensemble quotient de $E \times E^*$ par la relation d'équivalence R. Réciproquement, supposons E donné ; appelons $\overline{E}$ le quotient de $E \times E^*$ par la relation R. Soient w_1, w_2 des éléments de $\overline{E}$; soient (x_1, y_1) et (x_2, y_2) des éléments des classes d'équivalence, dans $E \times E^*$, qui définissent respectivement w_1 et w_2 : la classe d'équivalence qui contient $(x_1 \top x_2, y_1 \top y_2)$ ne dépend que de w_1, w_2, car si on remplace (x_1, y_1) par un élément équivalent (x_3, y_3), on aura $x_1 \top y_3 = x_3 \top y_1$, donc $(x_1 \top x_2) \top (y_3 \top y_2) = (x_3 \top x_2) \top (y_1 \top y_2)$, et de même si on remplace (x_2, y_2) par (x_4, y_4) équivalent ; avec ces notations, on désignera par $w_1 \overline{\top} w_2$ la classe à laquelle appartient $(x_1 \top x_2, y_1 \top y_2)$: $\overline{\top}$ est une loi de composition entre éléments de $\overline{E}$, évidemment associative et commutative. Tous les éléments de $E \times E^*$, de la forme (z, z), où $z \in E^*$, sont équivalents, et réciproquement, si (x, y) est équivalent à (z, z), on a $x \top z = z \top y$, donc (z étant régulier), $x = y$; soit e la classe formée des éléments (z, z). Si $(x, y) \in E \times E^*$, et $z \in E^*$, $(x \top z, y \top z)$ est équivalent à (x, y) ; e est donc élément neutre dans $\overline{E}$ pour la loi $\overline{\top}$. Toute classe d'équivalence contenant un élément de la forme (y, z), où $y \in E^*$, $z \in E^*$, est un élément inversible de $\overline{E}$, ayant pour élément inverse la classe qui contient (z, y), car le composé de ces classes est la classe de $(y \top z, y \top z)$, c'est-à-dire l'élément neutre. Or, si la classe w qui contient $(x, y) \in E \times E^*$ est un élément régulier de $\overline{E}$, la relation $w \overline{\top} w_1 = w \overline{\top} w_2$ entre éléments de $\overline{E}$ doit entraîner $w_1 = w_2$, c'est-à-dire que (si (x_1, y_1) et (x_2, y_2) sont des éléments des classes w_1 et w_2) la relation $(x \top x_1) \top (y \top y_2) = (x \top x_2) \top (y \top y_1)$ doit entraîner $x_1 \top y_2 = x_2 \top y_1$: en particulier, pour $y_1 = y_2$, la relation

$x \top x_1 \top y \top y_1 = x \top x_2 \top y \top y_1$ (qui est équivalente à $x \top x_1 = x \top x_2$, puisque $y \top y_1$ est régulier) entraîne $x_1 \top y_1 = x_2 \top y_1$ (elle-même équivalente à $x_1 = x_2$ puisque y_1 est régulier) : autrement dit $x \top x_1 = x \top x_2$ entraîne $x_1 = x_2$, donc x est régulier et par suite w est inversible et a pour inverse la classe de (y,x). L'ensemble $\overline{E}$, avec la loi $\overline{\top}$, satisfait donc à la condition 1° du th.1 .

Soit $x \in E$, et considérons dans $E \times E^*$ l'ensemble des éléments de la forme $(x \top y, y)$, où $y \in E^*$: ils sont tous équivalents, et réciproquement si (x_1, y_1) est équivalent à l'un de ces éléments, on a $x \top y \top y_1 = x_1 \top y$, donc (y étant régulier) $x_1 = x \top y_1$; autrement dit les éléments $(x \top y, y)$ forment une classe d'équivalence, et si on fait correspondre cette classe à $x \in E$, on a une correspondance biunivoque entre E et l'ensemble H des classes de cette forme ; on vérifie immédiatement que H est stable pour $\overline{\top}$ dans $\overline{E}$, que la correspondance en question est un isomorphisme entre E et H, et qu'a tout x régulier dans E correspond ainsi un élément de H régulier dans $\overline{E}$: la condition 2° du th.1 est donc bien satisfaite. Enfin, si $w \in \overline{E}$ est la classe d'équivalence contenant $(x,y) \in E \times E^*$, c'est le composé, dans $\overline{E}$, de la classe qui contient $(x \top z, z)$, où $z \in E^*$, et de la classe qui contient $(z_1, y \top z_1)$ ou $z_1 \in E^*$: la première appartient à H, la seconde est l'inverse de la classe qui contient $(y \top z_1, z_1)$, et celle-ci est un élément régulier de H : la condition 3° est satisfaite.

Quant a l'unicité, soient $\overline{E}_1$, H_1 satisfaisant aux mêmes conditions que $\overline{E}$, H ; on notera aussi $\overline{\top}$ la loi de composition dans $\overline{E}_1$. Il y a, comme on l'a vu, correspondance biunivoque entre $\overline{E}_1$ et le quotient de $E \times E^*$ par la relation R, c'est-a-dire entre $\overline{E}_1$ et $\overline{E}$: le composé de deux éléments de $\overline{E}_1$ correspond, d'après ce qu'on a trouvé, au composé

dans $\overline{E}$, c'est-a-dire que la correspondance en question est un isomorphisme entre $\overline{E}_1$ et $\overline{E}$; enfin, si $u_1 \in H_1$ correspond à x dans l'isomorphisme entre E et H_1 , il correspondra comme on l'a vu à la classe de $E \times E^*$ qui contient $(x \top y, y)$ où $y \in E^*$, donc l'isomorphisme entre $\overline{E}$ et $\overline{E}_1$ applique bien H sur H_1 . Le théorème est ainsi complètement démontré.

En raison de l'importance du théorème, nous donnerons une seconde démonstration de l'existence de $\overline{E}$. Pour $y \in E^*$, soit M_y l'ensemble des éléments de E de la forme $x \top y$, où $x \in E$; soit $\mathcal{F}$ l'ensemble des parties de E qui contiennent une partie de la forme M_y . L'intersection de deux ensembles $M \in \mathcal{F}$, $M' \in \mathcal{F}$ appartient encore à $\mathcal{F}$, car s'il existe $y \in E^*$ tel que $x \top y \in M$ quel que soit $x \in E$, et $z \in E^*$ tel que $x \top z \in M'$ quel que soit $x \in E$, on aura $x \top (y \top z) \in M \cap M'$ quel que soit $x \in E$.

Cela posé, considérons l'ensemble Φ des applications f dans E de l'un quelconque des ensembles de $\mathcal{F}$, qui possèdent la propriété suivante : quel que soit $y \in E^*$, il existe $z \in E^*$ tel que $f(M_z) \subset M_y$. Nous définirons comme suit une relation d'équivalence entre éléments de Φ : une application dans E de $M \in \mathcal{F}$ et une application dans E de $M' \in \mathcal{F}$ seront dites équivalentes s'il existe $M'' \in \mathcal{F}$, contenu dans $M \cap M'$, sur lequel elles coïncident ; on vérifie immédiatement que c'est bien la une relation d'équivalence ; soit Ψ l'ensemble quotient de Φ par cette relation. Entre éléments de Ψ , nous définirons comme suit une loi de composition : étant donnés deux éléments de Ψ , c'est-a-dire deux classes d'équivalence dans Φ (par rapport à la relation définie plus haut), soient f,g

appartenant respectivement à ces deux classes ; supposons f définie sur $M \in \mathfrak{F}$, il y a $y \in E^*$ tel que $M_y \subset M$; soit f_1 la restriction de f à M_y, qui est équivalente à f. Soit g défini sur $M' \in \mathfrak{F}$: il existera $z \in E^*$ tel que $g(M_z) \subset M_y$; soit g_1 la restriction de g à $M''=M' \cap M_z$, qui est équivalente à g et applique M'' dans M_y ; alors $f_1 \circ g_1$ est une application de M'' dans E, dont on voit facilement qu'elle appartient à Φ et que sa classe ne dépend que des classes de f_1 et g_1, c'est-à-dire de f et g : la classe à laquelle appartient $f_1 \circ g_1$ sera par définition le composé des classes de f et g ; on vérifie immédiatement que cette loi de composition est associative et admet un élément neutre, à savoir la classe à laquelle appartient l'application identique de E sur E.

A tout $a \in E$ correspond la translation $x \to a \top x$, qui est une application appartenant à Φ ; soit φ_a la classe d'équivalence à laquelle appartient cette translation : la correspondance entre a et φ_a est biunivoque, car pour que les translations $x \to a_1 \top x$, $x \to a_2 \top x$ appartiennent à une même classe d'équivalence, il faut qu'il y ait un M_y sur lequel elles coïncident, d'où en particulier, si $z \in E^*$ $a_1 \top y \top z = a_2 \top y \top z$, donc $a_1 = a_2$. De la prop.1 résulte alors que la correspondance entre a et φ_a est un isomorphisme.

Si $b \in E^*$, φ_b admet un inverse dans Ψ, à savoir la classe d'équivalence φ'_b dans Φ à laquelle appartient l'application $b \top x \to x$ de M_b dans E, car le composé de φ_b et φ'_b est la classe à laquelle appartient l'application $b \top x \to b \top x$ de M_b dans E, c'est-à-dire l'élément neutre de Ψ, et le composé de φ'_b et φ_b

est la classe à laquelle appartient l'application identique de E sur E , donc encore l'élément neutre.

Cela étant, on vérifiera facilement que la partie stable de Ψ engendrée par l'ensemble des φ_a et des φ'_b a bien toutes les propriétés énoncées pour $\overline{E}$ dans le th. 1 .

5. Applications. Dans les applications du th.1, il sera le plus souvent commode (cf.Ens.II, § 8, n°5) d'identifier l'ensemble E avec l'ensemble ci-dessus désigné par H ; ce qui permet (par abus de langage) de dire qu'on a "plongé E dans $\overline{E}$ " . Cette convention de langage sera appliquée en particulier dans les deux importants exemples suivants.

I. Entiers rationnels. Prenons pour E l'ensemble $\mathbb{N}$ des entiers naturels, avec la loi de composition + . Tous les éléments sont réguliers. On pourra donc plonger $\mathbb{N}$, d'une manière et d'une seule (à un isomorphisme près) dans un ensemble qu'on notera $\mathbb{Z}$, muni d'une loi de composition qu'on notera encore + , où tous les éléments soient inversibles, et qui soit engendré par $\mathbb{N}$ et par les inverses des éléments de $\mathbb{N}$. Les éléments de $\mathbb{Z}$, qu'on appelle entiers rationnels sont en correspondance biunivoque avec les classes d'équivalence déterminées dans $\mathbb{N}\times\mathbb{N}$ par la relation entre (m_1,n_1) et (m_2,n_2) qui s'écrit : $m_1+n_2=m_2+n_1$. L'élément m de $\mathbb{N}$ correspond ainsi à la classe ensemble des éléments de $\mathbb{N}\times\mathbb{N}$ de la forme $(m+n,n)$, où $n\in\mathbb{N}$; son inverse dans $\mathbb{Z}$ correspond à la classe des éléments $(n,m+n)$. Mais tout élément (p,q) de $\mathbb{N}\times\mathbb{N}$ peut s'écrire sous la forme $(m+n,n)$ si $p\geqslant q$, et sous la forme $(n,m+n)$ si $p\leqslant q$; il s'ensuit que $\mathbb{Z}$ est réunion de $\mathbb{N}$ et de l'ensemble des inverses des éléments de $\mathbb{N}$. D'ailleurs, l'élément neutre 0 est le seul élément de $\mathbb{N}$ inversible dans $\mathbb{N}$.

Il s'ensuit que si l'on note -m l'élément de $\mathbb{Z}$ inverse de l'élément m de $\mathbb{N}$ pour $m \neq 0$, $\mathbb{Z}$ est réunion de $\mathbb{N}$ et de l'ensemble des éléments -m pour $m \in \mathbb{N}$, $m \neq 0$. Par la correspondance ci-dessus définie $m \in \mathbb{N}$ correspond à la classe dans $\mathbb{N} \times \mathbb{N}$ qui contient (m,0) , et -m à la classe qui contient (0,m) ; on en déduit facilement (en tenant compte de ce qui a été dit dans la démontration du th.1) la loi de composition de ces éléments ; pour $m \in \mathbb{N}$, $n \in \mathbb{N}$, $n \neq 0$:

a) Si $m \geqslant n$, on a $m+(-n)=p$, p étant l'élément de $\mathbb{N}$ tel que $m=n+p$.

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

c) Si $m \neq 0$, on a $(-m)+(-n)=-(m+n)$.

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

On convient d'ordonner $\mathbb{Z}$ en écrivant, pour $a \in \mathbb{Z}$, $b \in \mathbb{Z}$, $a \geqslant b$ s'il existe $m \in \mathbb{N}$ tel que $a=b+m$. C'est bien là une relation d'ordre, car elle est évidemment transitive ; et si $a=b+m$, $b=a+n$, $m \in \mathbb{N}$, $n \in \mathbb{N}$, on a $m+n=0$, d'où $m=n=0$, $a=b$; et $\mathbb{Z}$ est totalement ordonné par cette relation, car soient $a \in \mathbb{Z}$, $b \in \mathbb{Z}$, et c tel que $a=b+c$ (on a $c=a+b'$, b' étant l'inverse de b pour la loi +) : si $c \in \mathbb{N}$, on a $a \geqslant b$; sinon, c est de la forme -m , $m \in \mathbb{N}$, et l'on a $a+m=b+(-m)+m=b$, donc $b \geqslant a$ (et même $b > a$ car $m \neq 0$). Enfin, il est clair que l'ordre ainsi défini sur $\mathbb{Z}$ induit sur $\mathbb{N}$ l'ordre qui a été défini dans Ens., chap.III.

II . Nombres rationnels positifs. Prenons pour E l'ensemble $\mathbb{N}$, la loi de composition étant cette fois la multiplication $\cdot$: tous les éléments sauf 0 sont réguliers. L'ensemble Q_+ (bien déterminé à un isomorphisme près) dans lequel $\mathbb{N}$ se trouve alors plongé par application du th.1 est dit ensemble des nombres rationnels positifs si $\mathbb{N}^*$

désigne l'ensemble des éléments $\neq 0$ de $\mathcal{N}$, Q_+ est en correspondance biunivoque avec le quotient de $\mathcal{N} \times \mathcal{N}^*$ par la relation entre (p_1,q_1) et (p_2,q_2) qui s'écrit $p_1q_2=p_2q_1$. On convient de désigner par $\frac{p}{q}$ ou bien par p/q l'élément de Q_+ qui correspond ainsi à la classe contenant (p,q) dans $\mathcal{N} \times \mathcal{N}^*$. Si $r \in Q_+$, $s \in Q_+$, on dira que r est <u>multiple</u> de s s'il existe $m \in \mathcal{N}$ tel que $r=ms$: on voit comme plus haut que c'est là une relation d'ordre dans Q_+ (mais Q_+ n'est pas totalement ordonné par cette relation). Il est inutile de donner ici plus de détails au sujet de Q_+, car on retrouvera cet ensemble plus loin (§) comme partie de l'ensemble Q des <u>nombres rationnels</u> (dans lequel on définira les deux lois de composition + et ·).

6. <u>Notations de l'élément inverse</u>. L'ensemble Z défini plus haut permet de poser une notation qui comprend comme cas particulier la notation $\overset{n}{\top} x$ définie au § 1 . On a déjà dit que si, pour une loi associative il existe un élément neutre e, on pose $\overset{0}{\top} x = e$; <u>si de plus x est inversible et a pour inverse x'</u>, on posera par définition $\overset{-n}{\top} x = \overset{n}{\top} x'$ quel que soit $n \in \mathcal{N}$, $n \neq 0$: alors $\overset{a}{\top} x$ est défini quel que soit $a \in Z$, et on a en particulier $\overset{-1}{\top} x = x'$. On vérifie immédiatement que l'on a, quels que soient $a \in Z$, $b \in Z$:

$$\overset{a+b}{\top} x = (\overset{a}{\top} x) \top (\overset{b}{\top} x) .$$

Notons dès maintenant que la relation $\overset{ab}{\top} x = \overset{a}{\top} (\overset{b}{\top} x)$ est également valable dans les mêmes conditions, si l'on définit comme suit la multiplication entre éléments de Z (cf. § 3) : pour $m \in \mathcal{N}$, $n \in \mathcal{N}$, m.n est le produit déjà défini (<u>Ens.</u>, chap. III) entre éléments de $\mathcal{N}$; et l'on pose $(-m).n=n.(-m)=-(mn)$, $(-m).(-n)=mn$.

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

soit additivement, soit multiplicativement :

a) Sauf indication formelle du contraire, on n'emploiera le signe + que lorsqu'il s'agira de noter une loi associative et commutative entre éléments d'un ensemble E pour laquelle tous les éléments de E soient réguliers. Pour une loi ainsi notée, on conviendra, si $x \in E$, de considérer $+x$ comme une notation désignant l'élément x lui-même ; et $-x$ comme désignant, si x est inversible l'élément inverse de x, qui, pour une loi ainsi notée, sera plus souvent appelé élément opposé à x. En outre, on notera le composé $x+(-y)$ sous la forme abrégée $x-y$. Enfin, dans tous les cas où on notera nx (pour $n \in \mathbb{N}$, $n \neq 0$) le composé d'une séquence de n éléments tous égaux à x, on conviendra, lorsqu'il existe dans E un élément neutre, que $0x$ désignera cet élément neutre (lui-même le plus souvent noté 0 comme il a été dit) ; et, quand x a un opposé $-x$, on notera $-nx$ l'élément $n(-x)=-(nx)$

b) Sauf indication formelle du contraire, on n'emploiera le signe · que lorsqu'il s'agira de noter une loi associative. Pour une loi ainsi notée, on notera x^a, pour $a \in \mathbb{Z}$, l'élément qui, pour une loi notée T, a été désigné plus haut par $\overset{a}{T}x$ (de sorte qu'en particulier l'inverse de x se notera x^{-1}).

c) Désormais, dans les raisonnements généraux relatifs aux lois de composition associatives, on se servira le plus souvent de la notation multiplicative (ou éventuellement additive quand les conditions indiquées en a) sont satisfaites).

Exercices. 1) Soit T une loi de composition sur E. Désignant par F l'ensemble "somme" (Ens. E, § 4, n° 5) de E et d'un ensemble $\{e\}$ à un élément, et identifiant E et $\{e\}$ avec les parties correspondantes de F, montrer qu'on peut, d'une manière et

d'une seule, définir sur F une loi de composition qui induise sur E la loi $\top$, et pour laquelle e soit élément neutre ; et que cette loi est associative si $\top$ est associative. (S'il n'y a pas d'élément neutre pour $\top$ dans E , on dit que F se déduit de E "par adjonction d'un élément neutre").

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

(N-B. Tous les exercices suivants se rapportent à des lois associatives qu'on notera multiplicativement ; e désignera toujours l'élément neutre).

3) Soit a tel que $ax=ay$ entraîne $x=y$, et soit a' tel que $aa'=e$; montrer que a' est inverse de a .

4) Montrer que la relation $x_1x_2\ldots x_n=e$ entre éléments <u>réguliers</u> x_i entraîne toutes les relations $x_{i+1}\ldots x_nx_1x_2\ldots x_i=e$ $(1\leqslant i<n)$ qui s'en déduisent par "permutation circulaire". En déduire que le composé d'une séquence d'éléments réguliers est inversible, chaque terme est inversible.

5) Pour une loi associative sur un ensemble <u>fini</u>, tout élément régulier est inversible.

6) Etant donnés une loi $\cdot$ sur E et un $x\in E$, soit A l'ensemble des x^n pour $n\in\mathcal{N}^*$ (c'est-à-dire $n\in\mathcal{N}$; $n\neq 0$) ; s'il existe un élément neutre, soit B l'ensemble des x^n pour $n\in\mathcal{N}$; si de plus x est inversible, soit C l'ensemble des x^a pour $a\in\mathbb{Z}$. Montrer que, si A (ou resp. B et C) est infini, il est isomorphe (avec la loi induite par $\cdot$) à $\mathcal{N}^*$ (ou resp. à $\mathcal{N}$ ou à $\mathbb{Z}$) muni de la loi $+$.

7) Les notations étant celles de l'exerc. 6, on suppose A fini : montrer que A contient un idempotent h (v.exerc.5 du § 1) et un seul (on observera que si x^p et x^q sont indempotents on a $x^p=x^{pq}$, $x^q=x^{pq}$, donc $x^p=x^q$) et que si $x^p=h$, l'ensemble des x^n pour $n \geqslant p$ est une partie stable D de E telle que, pour la loi induite par $\circ$ sur D , h est élément unité et tous les éléments de D sont inversibles.

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

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

$$x \circ (yz) = (x \circ y).(z \circ (x \circ y)).(x \circ z)$$

$$(x \circ y).(z \circ (x \circ y)).(z \circ x)^{-1}.(y \circ z).(x \circ (y \circ z)).(x \circ y)^{-1}.$$
$$.(z \circ x)(y \circ (z \circ x)).(y \circ z)^{-1} = e$$

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

§ 3. Lois de composition externes ; structures algèbriques.

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

Comme pour les lois internes, le cas de beaucoup le plus important est celui des lois définies partout, c'est-à-dire définies sur $A = \Omega \times E$; et le plus souvent, on pourra supposer qu'il en est ainsi, sauf mention expresse du contraire.

Parmi les notations les plus fréquemment adoptées pour le composé de a et x, citons les notations multiplicative à gauche $a.x$ (le signe $\cdot$ pouvant s'omettre à volonté), multiplicative à droite $x.a$, et exponentielle x^a.

Exemples. 1) $\cdot$ étant comme toujours une loi associative entre éléments d'un ensemble E, $(n,x) \to x^n$ est une loi de composition externe partout définie entre éléments de $\mathbb{N}^*$ et éléments de E ; pour $a \in \mathbb{Z}$, $(a,x) \to x^a$ est une loi entre $\mathbb{Z}$ et E, non partout définie si les éléments de E ne sont pas tous inversibles. Ce qui précède s'applique aux lois $(n,x) \to nx$ et $(a,x) \to ax$ pour un E où est donnée une loi écrite additivement.

2) Avec les notations d'Ens.R, § 3, n°10, $A \circ B$ est une loi (partout définie) entre parties A de $E \times E$ et parties B de $E \times F$, les premières étant les opérateurs de la loi ; $B \circ C$ est une loi entre parties C de $F \times F$ (opérateurs de la loi) et parties B de $E \times F$.

3) Une loi de composition $\top$ étant donnée dans E, on notera $x \top A$, pour $x \in E$, $A \subset E$, l'ensemble des $x \top y$ pour $y \in A$ (c'est-à-dire l'ensemble $\{x\} \top A$) : c'est là une loi de composition entre éléments de E (opérateurs de la loi) et parties de E.

4) Une loi externe $\perp$ étant donnée entre Ω et E, soit $\Xi \top X$, pour $\Xi \subset \Omega$, $X \subset E$, l'ensemble des $\alpha \perp x$ pour $\alpha \in \Xi$, $x \in X$: c'est là une loi de composition entre parties de Ω et parties de E.

Une loi de composition externe $\alpha \perp x$ étant donnée entre $\alpha \in \Omega$ et $x \in E$, $f_\alpha(x) = \alpha \perp x$ est une application dans E d'une partie de E, à savoir de l'ensemble des x pour lesquels $\alpha \perp x$ est défini. Réciproquement, soit $(f_\alpha)_{\alpha \in \Omega}$ une famille d'application de parties de E dans E,

ayant Ω comme ensemble d'indices : $(\alpha,x) \to f_\alpha(x)$ est une loi de composition entre Ω et E . Il est donc complètement équivalent de se donner une telle famille (f_α), ou de se donner une loi de composition entre Ω et E .

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

1° une loi interne pour laquelle le composé de x et y est $x \top y = f(x,y)$;

2° la loi interne opposée à la précédente (§ 1, n°1), pour laquelle le composé de x et y est $y \top x = f(y,x)$;

3° une loi externe entre opérateurs $x \in E$ et éléments $y \in E$, pour laquelle le composé de x et y est $x \top y = f(x,y)$; cette loi est dite la loi externe à gauche déduite de la loi $\top$;

4° une loi externe entre opérateurs $x \in E$ et éléments $y \in E$, pour laquelle le composé de x et y est $y \top x = f(y,x)$: cette loi est dite la loi externe à droite déduite de $\top$; c'est aussi la loi externe à gauche déduite de la loi interne opposée à $\top$.

Pour une loi $\top$ partout définie dans E , la loi externe à gauche déduite de $\top$ est celle qui correspond (de la manière dite plus haut) à la famille des translations à gauche $(\gamma_x)_{x \in E}$; la loi externe à droite est celle qui correspond à la famille des translations à droite δ_x .

On dira que les deux lois externes déduites d'une loi interne sont obtenues par dédoublement de cette loi. Chaque fois que le fait que le domaine des opérateurs Ω est identique à E risquerait de produire des confusions, on le remplacera par un ensemble E' en correspondance biunivoque avec E , le composé de $x' \in E'$ et de $y \in E$ étant $f(x,y)$, si x est l'élément de E qui correspond à $x' \in E'$. Naturellement, on transportera en même temps à E' , le cas échéant, toutes les structures qu'on se sera donnée sur E (Ens. R, § 8, n° 5).

3. Parties stables. Par analogie avec les définitions du § 1, on est conduit à poser les définitions suivantes :

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

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

L'intersection d'une famille de parties stables de E est évidemment stable, donc il existe une plus petite partie stable contenant une partie donnée de E .

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

Si aucune confusion n'est à craindre, la loi induite par $\perp$ pourra être désignée (par abus de langage) par le même signe. Lorsqu'on parlera (sans autre indication) de la loi induite par $\perp$ sur une

partie F de E , on sous-entendra toujours que $\Phi = \Omega$. Si la loi $\perp$ est partout définie sur $\Omega \times E$, et si F est une partie stable de E par rapport à cette loi, la loi induite par $\perp$ sur F (et à plus forte raison la loi incuite par $\perp$ entre une partie Φ et Ω et F) est partout définie.

4. Structures algèbriques. L'objet de l'Algèbre est l'étude d'une ou plusieurs lois de composition, internes ou externes, simultanément données entre éléments d'un ou plusieurs ensembles. Le plus souvent, tous ces ensembles sauf un sont considérés comme ensembles auxiliaires, ce qui conduit à poser la définition suivante :

Définition 4. Par une structure algèbrique sur un ensemble E , on entendra la structure définie sur E par une ou plusieurs lois de composition internes entre éléments de E , et une ou plusieurs lois de composition externes entre des domaines d'opérateurs Ω , Θ,... et E , ces lois pouvant être assujetties à satisfaire à certaines conditions (p.ex. l'associativité n la commutativité, etc.) ou à avoir entre elles certaines relations (v. plus loin).

Ces conditions ou relations (qui constituent les axiomes de la structure algèbrique), ainsi que la donnée des domaines Ω, Θ,... caractérisent l'espèce de structure envisagée.

On définira ainsi, dans ce chapitre et les suivants, les structures de groupe, de groupe à opérateurs, d'anneau, de module, de corps, etc..

La définition ci-dessus entraîne naturellement une notion d'isomorphisme pour une structure algèbrique : un isomorphisme entre E et E' étant une correspondance biunivoque entre E et E' telle que les lois internes sur E' , et les lois externes entre Ω , Θ ,... et E' se déduisent des lois correspondantes pour E par transport de structure

au moyen de la correspondance en question (Ens. R, § 8, n° 5). Plus rarement, on aura affaire à un transport de structure entre les ensembles E, Ω , $\textcircled{H}$,..., d'une part, et des ensembles E', Ω', $\textcircled{H}'$,..., de l'autre (cf. Ens. R, § 8, n°5) : on dira alors qu'on a affaire à un poly-isomorphisme (di-isomorphisme s'il n'y a qu'un seul ensemble auxiliaire).

Un isomorphisme de E sur lui-même s'appellera, comme toujours, un automorphisme de E ; un poly-isomorphisme de E, Ω , $\textcircled{H}$,... sur eux-mêmes s'appellera poly-automorphisme (di-automorphisme s'il n'y a qu'un seul ensemble auxiliaire).

Définition 5. E étant muni d'une structure algèbrique conformément à la déf.4, une partie A de E sera dite stable (par rapport à la structure de E) si elle est stable par rapport à chacune des lois internes ou externes qui définissent la structure de E .

L'intersection d'une famille quelconque de parties stables de E est encore une partie stable ; donc en particulier il existe une plus petite partie stable contenant une partie donnée X de E , qui sera dite engendrée par X .

Définition 6. E étant muni d'une structure algèbrique conformément à la déf.4, on appelle structure induite par cette structure sur une partie F de E celle qui est définie sur F par les lois internes et externes induites sur F par les lois qui définissent la structure de E .

Naturellement, pour que la structure induite sur F soit de la même espèce que celle qu'on s'est donnée sur E , il faudra que les lois induites sur F satisfassent aux conditions et relations caractéristiques de l'espèce de structure dont il s'agit ; il n'en sera pas ainsi

en général si F est une partie quelconque de E (on verra par exemple au § 4 que la structure induite sur une partie F d'un groupe E par la structure de groupe de E ne sera pas en général une structure de groupe).

5. Structures quotients. On considèrera dans ce qui suit des relations d'équivalence R,S,..., entre éléments d'ensembles pourvus de structures algèbriques. Comme il a été dit dans Ens. R, § 5, n°2, la relation R entre éléments x,y s'écrira $x \equiv y \pmod{R}$ ou simplement $x \equiv y$ quand on n'a pas de confusion à craindre avec une autre relation.

Définition 7. Une loi de composition interne $\top$ étant définie entre éléments d'un ensemble E , on dira qu'une relation d'équivalence R entre éléments de E est compatible avec la loi $\top$ si les relations $x \equiv x' \pmod{R}$, $y \equiv y' \pmod{R}$, $z = x \top y$, $z' = x' \top y'$ entraînent $z \equiv z' \pmod{R}$; la loi qui, aux classes d'équivalence de x et y fait correspondre la classe de z , est une loi de composition interne entre éléments de l'ensemble quotient E/R , qui s'appellera le quotient de la loi $\top$ par R .

La loi quotient de $\top$ par R est évidemment associative si $\top$ est associative, commutative si $\top$ est commutative ; elle a un élément neutre si $\top$ en a un (à savoir la classe d'équivalence à laquelle appartient celui-ci) ; à deux éléments inverses l'un de l'autre pour $\top$ dans E correspondent dans E/R des éléments inverses l'un de l'autre pour la loi quotient, donc à un élément inversible dans E correspond un élément inversible dans E/R . En revanche, a un élément règulier dans E ne correspond pas nécessairement un élément régulier dans E/R (v. les exemples plus loin).

Définition 8. Une loi de composition externe $\perp$ étant définie entre des opérateurs $\alpha \in \Omega$ et les éléments d'un ensemble E, on dira qu'une relation d'équivalence R entre éléments de E est compatible avec la loi $\perp$ si les relations $x \equiv x' \pmod{R}$, $y = \alpha \perp x$, $y' = \alpha \perp x'$ entraînent $y \equiv y' \pmod{R}$; la loi qui, à α et à la classe d'équivalence de x, fait correspondre la classe de y, est une loi externe entre opérateurs $\alpha \in \Omega$ et éléments de E/R, qui s'appellera quotient de la loi $\perp$ par la relation R.

Si une relation R est compatible avec une loi interne $\top$, elle est compatible aussi, d'une part avec la loi opposée, d'autre part avec les deux lois externes qui s'en déduisent par dédoublement. Par passage au quotient sur ces quatre lois, on obtient deux lois internes, opposées l'une de l'autre, entre éléments de E/R, et deux lois externes entre opérateurs qui sont les éléments de E, et les éléments de E/R. Réciproquement, si $\top$ est une loi interne partout définie, soit R une relation d'équivalence compatible avec chacune des lois externes qui s'en déduit ; alors, si $x \in E$, $y \in E$, et $x \equiv x' \pmod{R}$, on a $x' \top y \equiv x \top y \pmod{R}$, si $y \equiv y' \pmod{R}$, $x' \top y' \equiv x' \top y \pmod{R}$; donc $x' \top y' \equiv x \top y \pmod{R}$, R est compatible avec $\top$.

On dira pour abréger, qu'une relation R est compatible à gauche (resp. à droite) avec une loi interne $\top$, si elle est compatible avec la loi externe à gauche (resp. à droite) déduite de $\top$. On a donc la proposition :

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

Définition 9. Soit E un ensemble muni d'une structure algèbrique définie par des lois de composition internes ou externes ; on dira qu'une relation d'équivalence R entre éléments de E est compatible avec la structure de E si elle l'est avec toutes ces lois ; la structure définie sur le quotient E/R par les quotients de ces lois par R s'appelle la structure quotient par R de celle de E , et E/R muni de cette structure s'appelle le quotient par R de l'ensemble E muni de la structure donnée.

Naturellement, pour que la structure quotient ainsi définie sur E/R soit de la même espèce que celle qui a été donnée sur E , il faudra que les lois quotients sur E/R satisfassent aux conditions caractéristiques de cette espèce de structure : ce qu'il y aura lieu de vérifier dans chaque cas (il en est bien ainsi par exemple pour les groupes quotients, anneaux quotients, etc.., qui seront définis dans la suite de ce chapitre).

Exemples. 1) Soit A une partie d'un ensemble E : soit X_A la trace sur A de $X \in E$. La relation d'équivalence $X_A = Y_A$ entre parties X,Y de E est compatible avec la structure déterminée sur $\mathfrak{P}(E)$ par les lois $\cup$, $\cap$, et le quotient de $\mathfrak{P}(E)$, muni de cette structure, par la relation précédente est isomorphe à $\mathfrak{P}(A)$, muni de la structure définie par les lois $\cup$, $\cap$.

2) Soit $a \in \mathcal{N}$: la relation entre $m \in \mathcal{N}$, $n \in \mathcal{N}$ "il existe $p \in \mathcal{N}$ tel que $m=n+pa$ ou $n=m+pa$ " est une relation d'équivalence compatible avec l'addition et la multiplication sur $\mathcal{N}$, qui s'écrit le plus souvent $m \equiv n \pmod{a}$ ou bien $m \equiv n \ (a)$. Si $a \neq 0$, a est régulier pour la multiplication dans $\mathcal{N}$, mais l'élément correspondant dans le quotient de $\mathcal{N}$ par cette relation (qui est la classe à laquelle appartient 0) n'est pas régulier pour la loi quotient de la multiplication. (v.plus loin une étude plus approfondie de cet exemple).

6. Représentations ; homomorphismes. Définition 10. Soient E et F des ensembles munis de structures algèbriques de même espèce, et f une application de E dans F . Les lois de composition correspondantes dans E et F étant notées d'un même signe, f s'appellera une représentation de E dans F si :

1) pour chacune des lois de composition internes $\top$ données sur E et F , les relations $x'=f(x)$, $y'=f(y)$, $z=x\top y$ entraînent $f(z)=x'\top y'$;

2) pour chacune des lois externes $\perp$ données sur E et F , les relations $x'=f(x)$, $y=\alpha\perp x$ (où α est un opérateur de $\perp$) entraînent $f(y)=\alpha\perp x'$.

Théorème 1. Les notations étant celles de la déf. 10, et les lois qui définissent les structures de E et F étant supposées définies partout, l'image f(E) de E dans F est une partie stable de F , et f(E), avec la structure induite par celle de F , est isomorphe au quotient de E par la relation d'équivalence $f(x)=f(y)$, relation qui est compatible avec la structure de E .

Le théorème est évident à partir des définitions.

Dans tout ce qui va suivre, on supposera que toutes les lois de composition qui interviendront sont partout définies, de façon que le th.1 soit applicable. Cela étant, une représentation de E dans F s'appelle souvent aussi un homomorphisme de E dans F ; on dit que c'est un homomorphisme de E sur F si $f(E)=F$: dans ce cas F est isomorphe au quotient de E par une certaine relation d'équivalence. On dit que la représentation f est un isomorphisme de E dans F si f est biunivoque : f(E) est alors isomorphe à E . Enfin, un homomorphisme de E dans lui-même s'appelle un endomorphisme de E . L'application canonique de E sur E/R , R étant compatible avec la structure de E ,

s'appellera l'homomorphisme canonique de E sur E/R .

7. Les théorèmes d'isomorphisme. Proposition 2. f étant l'homomorphisme canonique de E , muni d'une structure algèbrique, sur le quotient E/R de E par une relation R compatible avec sa structure, pour qu'une application g de E/R dans un ensemble F muni d'une structure de même espèce soit une représentation, il faut et il suffit que $g \circ f$ soit une représentation de E dans F .

Vérification immédiate (on examine séparément le cas des lois internes et des lois externes).

Si S est la relation $g(x')=g(y')$ dans E/R , T la relation $g(f(x))=g(f(y))$ dans E , S est le quotient T/R de T par R (Ens.R, §5,n°9) ; et il y a isomorphisme entre l'image de E/R par g , ou (ce qui revient au même) l'image de E par $g \circ f$, et les quotients (E/R)/S et E/T . Si g est l'homomorphisme canonique de E/R sur (E/R)/S , on a le théorème suivant :

Théorème 2 (Premier théorème d'isomorphisme). E/R étant le quotient d'un ensemble E , muni d'une structure algèbrique, par une relation d'équivalence R compatible avec sa structure, toute relation d'équivalence S dans E/R , compatible avec la structure de E/R , est de la forme T/R , où T est une relation d'équivalence dans E , compatible avec la structure de E , et réciproquement ; et dans ces conditions, la correspondance canonique entre E/T et (E/R)/(T/R) est un isomorphisme.

f étant toujours l'homomorphisme canonique de E sur E/R , soit A une partie stable de E , avec la structure induite par celle de E ; la restriction de f à A est évidemment une représentation de A dans E/R ; d'après le th.1 , f(A) est isomorphe au quotient A/R_A de A par la relation R_A induite par R dans A (Ens.R , § 5, n°5) .

Si B est la partie de E obtenue en saturant A pour la relation R (Ens.R, § 5, n° 6), B est encore une partie stable de E : car soient $x \in B$, $y \in B$, c'est-à-dire qu'il existe $x' \in A$, $y' \in A$ tels que $x \equiv x'$ et $y \equiv y'$ (mod.R) ; on aura, pour l'une des lois internes $\top$ qui définissent la structure de E , $x' \top y' \in A$ et $x \top y \equiv x' \top y'$ (mod.R), donc $x \top y \in B$; de même pour les lois externes. Comme B/R_B est isomorphe à f(B), et que f(B)=f(A), on a le théorème :

Théorème 3 (Second théorème d'isomorphisme). A étant une partie stable de l'ensemble E muni d'une structure algèbrique, et R une relation d'équivalence dans E compatible avec cette structure, l'ensemble B déduit de A en le saturant pour R est stable; et, si R_A , R_B sont les relations induites par R sur A et sur B , elles sont compatibles avec les structures induites sur A et sur B par celles de E , et il y a isomorphisme entre les quotients A/R_A et B/R_B .

8. Prolongement d'une représentation. Avant de donner des exemples des résultats généraux qui précèdent, nous donnerons un théorème très utile sur les représentations des ensembles à loi interne associative et commutative définis par application du th.1 du § 2 . On notera multiplicativement la loi qui intervient dans ce théorème, et on identifiera les ensembles notés H et E dans l'énoncé de celui-ci.

Théorème 4. Soit $\overline{E}$ pourvu d'une loi associative et commutative $\circ$, pour laquelle tous les éléments réguliers soient inversibles, et engendré par la réunion d'une partie stable E de $\overline{E}$ et de l'ensemble des inverses des éléments réguliers de E ; soit f un homomorphisme de E dans un ensemble F muni d'une loi associative, qui à tout élément régulier de E fasse correspondre un élément inversible de F : alors f peut, d'une manière et d'une seule, être prolongé en un homomorphisme de $\overline{E}$ dans F .

L'image f(E) dans F est isomorphe à un ensemble quotient de E, donc sur f(E) la loi induite par celle qui est donnée dans F (et qu'on notera aussi par $\cdot$) est commutative. D'autre part, il résulte de la démonstration du th.1 du §2 que tout élément de $\bar{E}$ est de la forme xy^{-1}, où $x \in E$ et où y est un élément régulier de E ; si $xy^{-1}=x'y'^{-1}$, on a $xy'=x'y$, donc (par l'homomorphisme) $f(x)f(y')=f(x')f(y)$, et par suite, f(y) et f(y') étant inversibles par hypothèse, et aussi permutables entre eux et avec f(x) et f(x') : $f(x)f(y)^{-1}=f(x')f(y')^{-1}$; donc $f(x)f(y)^{-1}$ ne dépend que de xy^{-1} ; si d'ailleurs $w=xy^{-1} \in E$, on aura $x=wy$, $f(x)=f(w)f(y)$, donc $f(w)=f(x)f(y)^{-1}$. En posant $f(xy^{-1})=f(x)f(y)^{-1}$ on prolonge donc à $\bar{E}$ l'application f de E dans F ; et on vérifie, par un calcul analogue aux calculs ci-dessus, que ce prolongement est une représentation. L'unicité résulte de ce que tout homomorphisme f de $\bar{E}$ dans F satisfait à $f(xy^{-1})=f(x)f(y)^{-1}$.

9. Applications. I. Multiplication des entiers rationnels. Considérons l'ensemble $\mathbb{Z}$ des entiers rationnels (§2, n°5), et l'ensemble $\mathbb{N} \subset \mathbb{Z}$, avec la structure définie sur eux par la seule loi +. Si $m \in \mathbb{N}$, on a (Ens., chap.III) l'identité $m(x+y)=mx+my$ pour $x \in \mathbb{N}$, $y \in \mathbb{N}$ qui exprime que l'application $x \to mx$ de $\mathbb{N}$ dans lui-même est une représentation. On peut donc aussi la considérer comme représentation de $\mathbb{N}$ dans $\mathbb{Z}$, et à ce titre lui appliquer le th.4 : on peut donc la prolonger en une représentation de $\mathbb{Z}$ dans $\mathbb{Z}$, qu'on notera encore $x \to mx$, mx étant par conséquent défini sur $\complement\mathbb{N}$, d'après la démonstration du th.4, par $m(-x)=-mx$, $x \in \mathbb{N}^*$.

Déterminon maintenant toutes les représentations f de $\mathbb{Z}$ dans $\mathbb{Z}$ (les endomorphismes de $\mathbb{Z}$). Soit $f(1)=m$, et soit d'abord $m \geqslant 0$.

On a $f(x+1)=f(x)+m$, d'où s'ensuit, par récurrence, que pour $x \in \mathcal{N}$, $f(x)=mx$; par application du th.4 à $\mathbb{Z}$ et $\mathcal{N}$, on a donc $f(x)=mx$ quel que soit $x \in \mathbb{Z}$. D'autre part, si $m=-n$, $n \in \mathcal{N}^*$, $x \to -f(x)$, application composée de $x \to -x$ (qui est évidemment une représentation) et de f , est une représentation qui applique 1 sur $n > 0$, donc $-f(x)=nx$, et $f(x)=-nx$ quel que soit $x \in \mathbb{Z}$: on posera encore, par définition, $f(x)=mx$, c'est-à-dire que l'on pose $(-n)x=-(nx)$ pour $n \in \mathcal{N}^*$, $x \in \mathbb{Z}$.

On a ainsi défini le produit mx quels que soient $m \in \mathbb{Z}$, $x \in \mathbb{Z}$. On a , pour $m \in \mathcal{N}$, $n \in \mathcal{N}$ (et même plus généralement pour $m \in \mathbb{Z}$, $n \in \mathbb{Z}$) : $m(-n)=-mn$, $(-m)n=-mn$, $(-m)(-n)=mn$, d'où l'on conclut immédiatement que la multiplication est associative et commutative dans $\mathbb{Z}$; et par la manière même dont on a obtenu le produit, on a $m(x+y)=mx+my$, d'où (par la commutativité), $(m+n)x=mx+nx$ quels que soient m,n,x,y ; et $m.0=0.m=0$, $m.1=1.m=m$.

On verra au § comment ce qui précède se généralise à la définition de l'anneau des endomorphismes d'un groupe abélien.

II. <u>Relations d'équivalence dans</u> $\mathbb{Z}$. Soit $a \in \mathbb{Z}$: la relation entre éléments x,y de $\mathbb{Z}$ qui s'énonce "il existe $z \in \mathbb{Z}$ tel que $x-y=az$" est une relation d'équivalence que l'on convient, une fois pour toutes, d'écrire $x \equiv y \pmod{a}$ ou plus brièvement $x \equiv y \ (a)$, et qui s'appelle une <u>congruence modulo a</u> . En remplaçant a par $-a$, on obtient une relation équivalente, donc on pourra supposer $a \geqslant 0$; pour $a=0$, $x \equiv y \ (0)$ entraîne $x=y$, donc on n'aura une relation distincte de l'égalité que si $a \neq 0$: aussi suppose-t-on souvent que $a>0$ sauf indication formelle du contraire. Pour $a > 0$, le quotient de $\mathbb{Z}$ par la congruence $x \equiv y \ (a)$ est un ensemble fini à a éléments,

dit ensemble des entiers rationnels modulo a , comme il résultera de la proposition suivante :

Si $a > 0$ et $x \in \mathbb{Z}$, on peut, d'une manière et d'une seule, trouver $q \in \mathbb{Z}$ et $r \in [0, a-1]$ tels que $x = qa+r$.

En effet, si $x = qa+r$, avec $0 \leqslant r \leqslant a-1$, on a $qa \leqslant x < (q+1)a$, d'où $ma \leqslant x$ pour $m \leqslant q$ et $ma > x$ pour $m > q$, et par suite q (s'il existe) est bien déterminé somme le plus grand élément de l'ensemble M des m tels que $ma \leqslant x$. Réciproquement, M est non vide (car il contient $m=0$ si $x \geqslant 0$ et il contient $m=x$ si $x < 0$) : si $m \in M$, il existe n tel que $m+n \notin M$ (il suffit de prendre $n > x-ma$) donc $m+z \notin M$ chaque fois que $z \geqslant n$; par suite, si p est le plus grand entier de l'intervalle $[0, n-1]$ tel que $m+p \in M$, $q = m+p$ sera le plus grand élément de M ; on aura alors $qa \leqslant x < (q+1)a$, donc $0 \leqslant r = x-qa \leqslant a-1$ ce qui démontre la proposition.

r s'appelle le reste de x modulo a ; pour que $x \equiv y$ (a) , il faut et il suffit que x et y aient même reste modulo a ; il s'ensuit que le quotient de $\mathbb{Z}$ par cette relation est en correspondance biunivoque avec l'intervalle $[0, a-1]$, c'est donc un ensemble à a éléments. Il est clair que c'est aussi le quotient de $\mathbb{N}$ par la relation $x \equiv y$ (a) induite sur $\mathbb{N}$ par la précédente.

Quel que soit $a \in \mathbb{Z}$, la relation $x \equiv y$ (a) est compatible aussi bien avec l'addition qu'avec la multiplication, comme on le vérifie immédiatement : par passage au quotient, on obtient donc pour $a > 0$ des opérations qui s'appelleront addition et multiplication modulo a .

La relation $x \equiv 0$ (mod.a) s'énoncera aussi "x est multiple de a" , "a est diviseur de x" , "a divise x" . Si $a \equiv 0$ (b) , la congruence $x \equiv y$ (a) entraîne $x \equiv y$ (b) . Il s'ensuit que l'ensemble des entiers

modulo b , pour $b > 0$, avec la structure définie par l'addition et la multiplication, est isomorphe, pour $a > 0$, a multiple de b , au quotient de l'ensemble des entiers modulo a , avec la structure analogue, par une relation d'équivalence (quotient de la congruence modulo b par la congruence modulo a) qu'on écrit aussi, par abus de langage, $x \equiv y \ (b)$.

Le th.3 montre que l'ensemble des entiers modulo a , avec la structure définie par l'addition et la multiplication, s'obtient également en faisant le quotient de $\mathscr{N}$ (avec la structure analogue) par la congruence modulo a .

10. Produits de structures algèbriques. Définition 11. Soit $(E_\iota)_{\iota \in I}$ une famille d'ensembles E_ι , pourvus tous de structures algèbriques d'une même espèce, et soit $E = \prod_{\iota \in I} E_\iota$ leur produit. Chacune des lois (internes ou externes) caractéristique de cette espèce de structure étant notée sur tous les E_ι par un même signe, soit, pour une loi interne $\top$ et pour $x=(x_\iota) \in E$, $y=(y_\iota) \in E$, $x \top y=(x_\iota \top y_\iota)$ chaque fois que $x_\iota \top y_\iota$ est défini quel que soit ι ; soit, pour une loi externe $\perp$, pour un opérateur α relatif à $\perp$, et pour $x=(x_\iota)$, $\alpha \perp x=(\alpha \perp x_\iota)$ chaque fois que $\alpha \perp x_\iota$ est défini quel que soit ι ; la structure déterminée sur E par les lois de composition ainsi définies à partir des lois données sur les E_ι s'appelle le produit des structures des E_ι ; et E , muni de cette structure, s'appelle le produit des E_ι munis des structures données.

Naturellement, il y aura lieu, ici encore, de s'assurer dans chaque cas si la structure produit est ou non de la même espèce que les structures données, c'est-à-dire si les lois définies sur E satisfont aux conditions caractéristiques de cette espèce.

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

Avec les notations de la déf.11, si A_ι est une partie stable de E_ι, $A = \prod_\iota A_\iota$ est une partie stable de E, et la structure induite sur A par celle de E est le produit de celles qui sont induites sur les A_ι par celles des E_ι. L'application pr_ι de E dans E_ι est une représentation de E sur E_ι ; de même la projection sur un produit partiel quelconque. Si f_ι est une représentation d'un ensemble F dans E_ι, (f_ι) est une représentation de F dans E.

Si E et F ont des structures de même espèce, et que les relations d'équivalence R entre éléments de E, S entre éléments de F, soient compatibles avec ces structures, l'application canonique de $(E/R) \times (F/S)$ sur $(E \times F)/(R \times S)$ est un isomorphisme.

S'il s'agit de structures déterminées sur chacun des E_ι par une seule loi interne associative, pour que $e=(e_\iota)$ soit élément neutre dans E, il faut et il suffit que e_ι soit élément neutre dans E_ι quel que soit ι ; pour que $x=(x_\iota)$ soit régulier, il faut et il suffit que chaque x_ι le soit ; pour que $x=(x_\iota)$ et $y=(y_\iota)$ soient inverses l'un de l'autre, il faut et il suffit que x_ι et y_ι le soient quel que soit ι.

Enfin, la structure étant d'espèce quelconque, considérons le cas où les E_ι sont identiques à un même ensemble F, E étant alors l'ensemble F^I des applications $f(\iota)$ de I dans F : pour chaque loi interne $\top$, le composé de $f(\iota)$ et $g(\iota)$ sera alors $f(\iota) \top g(\iota)$; et pour chaque loi interne $\perp$, le composé de l'opérateur α et de $f(\iota)$ sera $\alpha \perp f(\iota)$.

Pour I=F , il importe de distinguer soigneusement les lois de composition telles que $f(\iota)\top g(\iota)$ entre applications de I dans I , et la loi $(f,g) \longrightarrow f\circ g$.

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

I. Distributivité. Soit d'abord une loi externe $\perp$ entre opérateurs $\alpha \in \Omega$ et éléments de E : cette loi sera dite distributive par rapport à une loi interne $\top$ entre éléments de E , si, quel que soit $\alpha \in \Omega$, l'application $x \longrightarrow \alpha \perp x$ est une représentation de E dans E par rapport à la structure définie par $\top$, c'est-à-dire si $x'= \alpha \perp x$, $y'= \alpha \perp y$, $z=x\top y$ entraînent $\alpha \perp z=x'\top y'$. Pour le cas le plus ordinaire de lois définies partout, cette distributivité s'exprime par l'identité

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

Si la loi $\top$ est associative, on voit par récurrence qu'on aura pour une séquence quelconque $(x_\lambda)_{\lambda\in A}$: $\alpha \perp (\overset{\top}{\underset{\lambda\in A}{}} x_\lambda)=\overset{\top}{\underset{\lambda\in A}{}}(\alpha \perp x_\lambda)$.

Notations : Si la loi $\top$ est écrite multiplicativement, on emploiera fréquemment la notation exponentielle x^α pour la loi externe $\perp$, de sorte que la distributivité s'exprimera par l'identité $(xy)^\alpha=x^\alpha y^\alpha$. Si la loi $\top$ est écrite additivement, on emploiera fréquemment la notation multiplicative à gauche, $\alpha.x$, ou à droite $x.\alpha$, pour la loi $\perp$, la distributivité s'exprimant alors par $\alpha(x+y)=\alpha x+\alpha y$ ou resp. par $(x+y)\alpha = x\alpha + y\alpha$.

Supposons maintenant qu'en plus des lois $\top$ et $\perp$, on se soit donné une loi interne, également notée $\top$, dans l'ensemble Ω des opérateurs de la loi $\perp$. Celle-ci sera dite <u>distributive</u> par rapport aux lois internes données dans E et Ω si, quel que soit $x \in E$, l'application $\alpha \longrightarrow \alpha \perp x$ est une représentation de Ω dans E (par rapport aux lois $\top$) : pour des lois définies partout, cela s'exprime par $(\alpha \top \beta) \perp x = (\alpha \perp x) \top (\beta \perp x)$. Le plus souvent, il s'agira de lois internes notées <u>additivement</u> dans Ω et E (donc associatives et commutatives, cf. § 2, n° 6), et alors on emploiera pour la loi externe $\perp$ la notation multiplicative, soit à gauche, soit à droite, la distributivité s'exprimant par $(\alpha+\beta)x = \alpha x + \beta x$ ou resp. $x(\alpha+\beta)=x\alpha+x\beta$.

Avec la notation multiplicative à gauche $\alpha.x$, on dit en général que la loi externe $\cdot$ est <u>distributive à gauche</u> si l'on a l'identité $(\alpha+\beta)x = \alpha x + \beta x$, l'identité $\alpha(x+y)=\alpha x+\alpha y$ exprimant ce qu'on appelle la <u>distributivité à droite</u> (ces dénominations s'échangent pour une loi notée $x.\alpha$) ; avec les mêmes notations, la loi $\cdot$ est dite <u>doublement distributive</u> (par rapport aux lois +) si elle est distributive à gauche et à droite . Alors, si $(x_\lambda)_{\lambda \in A}$ est un système d'éléments de E , $(\alpha_\iota)_{\iota \in I}$ un système d'éléments de Ω , on aura

$$(\sum_\iota \alpha_\iota).(\sum_\lambda x_\lambda) = \sum_{(\iota,\lambda) \in I \times A} (\alpha_\iota . x_\lambda)$$

(et de même pour la notation à droite) comme on le voit par récurrence sur le nombre d'éléments de A et de I .

Un Une loi <u>interne</u> $\perp$ sera dite <u>doublement distributive</u> par rapport à une loi interne $\top$ si <u>les deux lois externes</u> déduites de $\perp$ par dédoublement, sont distributives par rapport à $\top$. Le plus souvent, il s'agira d'une loi $\top$ notée additivement ; on emploiera alors ordinairement la notation multiplicative pour $\perp$. Avec ces notations,

et en supposant de plus que les deux lois + et · sont <u>associatives et commutatives</u>, soit $(S_\alpha)_{\alpha\in A}$ un système de systèmes $S_\alpha=(x_{\alpha\lambda})_{\lambda\in L_\alpha}$ d'éléments de E ; on aura l'identité (qu'on vérifie par récurrence sur le nombre d'éléments de A) :

$$\prod_{\alpha\in A}\Big(\sum_{\lambda\in L_\alpha} x_{\alpha\lambda}\Big)=\sum_{\lambda(\alpha)\in\prod_{\alpha\in A}L_\alpha}\Big(\prod_{\alpha\in A} x_{\alpha,\lambda(\alpha)}\Big)$$

dite "formule générale de distributivité" .

<u>Exemples</u>. 1) Si la loi · est associative et commutative dans E , la loi x^n entre opérateurs $n\in\mathcal{N}^*$ et éléments x de E est distributive par rapport à la loi · dans E : <u>il n'en sera pas ainsi en général si celle-ci n'est pas commutative</u>. Si la loi °, associative et commutative, admet de plus un élément neutre, x^n sera distributif par rapport à · pour $n\in\mathcal{N}$; elle le sera pour $n\in\mathbb{Z}$ si de plus tout élément de E est inversible pour · . Si au lieu d'une loi notée °, on a affaire à une loi (associative et commutative) notée additivement, les mêmes résultats subsistent, la notation x^n étant alors à remplacer par nx .

2) La loi · étant associative, la loi x^n est distributive par rapport à la loi + dans $\mathcal{N}^*$ et à la loi · dans E , puisque $x^{m+n}=x^m x^n$. Si · est commutative, x^n est donc doublement distributive. De même pour la loi x^n , $n\in\mathbb{Z}$, quand de plus tout $x\in E$ est inversible.

3) Pour $X\subset E$, $K\subset E\times E$, la loi de composition externe $(K,X)\longrightarrow K(X)$ entre opérateurs K et éléments X de $\mathfrak{P}(E)$ est distributive par rapport a la loi interne $\cup$ dans $\mathfrak{P}(E)$, mais non par rapport à $\cap$ (<u>Ens</u>.R, § 3,n°7) ; elle est aussi distributive par rapport à $\cup$ dans $\mathfrak{P}(E\times E)$ et $\cup$ dans $\mathfrak{P}(E)$

c'est-à-dire que, si $K=K' \cup K''$, $K(X)=K'(X) \cup K''(X)$. De même pour la loi externe $A \circ B$ entre opérateurs $A \subset E \times E$ et éléments B de $\mathfrak{P}(F \times E)$.

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

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

6) Soit $\top$ une loi interne dans E ; la loi de composition interne $g \circ f$ entre applications de E dans E n'est pas en général doublement distributive par rapport à la loi interne $f \top g$ entre les mêmes applications, la loi externe à droite déduite de celle-là étant distributive par rapport à celle-ci, alors qu'il n'en est pas de même pour la loi externe à gauche.

II. Associativité. Une loi de composition interne associative $\top$ étant définie dans l'ensemble Ω des opérateurs d'une loi externe partout définie $\perp$ entre opérateurs $\alpha \in \Omega$ et éléments x de E , celle-ci est dite associative par rapport à celle-là si on a l'identité

$$(\alpha \top \beta) \perp x = \alpha \perp (\beta \perp x) .$$

Autrement dit, si l'on pose $f_\alpha(x)=\alpha \perp x$, $(f_\alpha)_{\alpha \in \Omega}$ étant donc la famille d'applications de E dans E qui correspond à la loi $\perp$, on doit avoir $f_{\alpha \top \beta} = f_\alpha \circ f_\beta$, c'est-à-dire que f_α est une représentation de Ω (avec la loi $\top$) dans l'ensemble des applications de E dans E de la loi $\circ$.

La loi $\top$ étant notée multiplicativement, on adoptera le plus souvent la notation multiplicative à gauche $\alpha.x$ pour une loi externe associative par rapport à celle-là, l'associativité s'exprimant par l'identité $\alpha(\beta x)=(\alpha\beta)x$; on adoptera, soit la notation multiplicative à droite $x.\alpha$, soit la notation exponentielle x^{α} , pour une loi externe associative par rapport à la loi opposée à la loi $\cdot$, les identités correspondantes étant $x(\beta\alpha)=(x\beta)\alpha$ et $x^{\beta\alpha}=(x^{\beta})^{\alpha}$.

Exemples. 1) La loi externe $A\circ B$ entre opérateurs $A \subset E\times E$ et parties $B\subset F\times E$ est associative par rapport à la loi $\circ$ entre opérateurs A . La loi externe $B\circ C$ entre opérateurs $C\subset F\times F$ et parties B de $E\times F$ est associative par rapport à la loi opposée à la loi $\circ$ entre opérateurs C .

2) La loi externe $(f,x)\longrightarrow f(x)$ entre applications f de E dans E (opérateurs) et éléments de E est associative par rapport à la loi interne $\circ$ entre les f ; de même pour la loi $(f,X)\longrightarrow f(X)$, le domaine d'opérateurs restant le même et muni de la même loi, et X étant une partie générique de E .

3) Si $\cdot$ est une loi associative entre éléments de E , x^n est une loi externe associative par rapport à la multiplication dans $\mathcal{N}^*$ puisque $(x^m)^n=x^{mn}$ (la multiplication dans $\mathcal{N}^*$ étant commutative, il n'y a pas de distinction à faire entre elle et la loi opposée). De même pour $n\in\mathcal{N}$ lorsqu'il y a un élément neutre dans E , et pour $n\in Z$ lorsque tous les $x\in E$ sont inversibles.

III. Double associativité. Soient deux lois externes partout définies, d'une part $\alpha \top x$ entre opérateurs $\alpha\in\Omega$ et éléments x de E , d'autre part $\beta \perp x$ entre opérateurs $\beta\in\textcircled{H}$ et éléments x de E .

On dit qu'il y a <u>double associativité entre</u> ces lois si l'on a l'identité $\alpha\top(\beta\perp x)=\beta\perp(\alpha\top x)$; autrement dit, $(f_\alpha)_{\alpha\in\Omega}$ et $(g_\beta)_{\beta\in\Theta}$ étant les familles d'applications de E dans E qui correspondent aux lois considérées, f_α doit être permutable avec g_β pour la loi $\circ$, quels que soient α et β . En général, on adoptera la notation multiplicative à gauche pour l'une des lois et multiplicative à droite pour l'autre, de sorte que la double associativité s'exprime par l'identité (qui justifie le nom donné à cette relation) : $\alpha(x\,\beta)=(\alpha\,x)\beta$.

<u>Exemple</u>. La condition ci-dessus est satisfaite pour les lois $A\circ B$, $B\circ C$ entre opérateurs $A\subset E\times E$ et parties B de $F\times E$ d'une part, opérateurs $C\subset F\times F$ et parties B de $F\times E$ de l'autre.

<u>Exercices</u>. 1) Toute relation d'équivalence dans $\mathbb{Z}$, compatible avec l'addition, est de la forme $x\equiv y\ (a)$, avec $a\in\mathbb{Z}$. En déduire qu'avec les notations de l'exerc.6 du § 2 , si C est fini à a éléments, il est isomorphe (avec la loi induite par .) à l'ensemble des entiers modulo a avec la loi + ; de même, avec les notations de l'exerc.7 du § 2, pour D si D est un ensemble à a éléments.

2) Soit $\perp$ une loi interne partout définie sur E , doublement distributive par rapport à une loi interne associative $\top$; montrer que si $x\perp x'$ et $y\perp y'$ sont réguliers pour la loi $\top$, $x\perp y'$ est permutable avec $y\perp x'$ pour la loi $\top$ (on calculera $(x\top y)\perp(x'\top y')$ de deux manières, en appliquant d'une part la distributivité d'abord à la première parenthèse puis à la seconde, et d'autre part à la seconde puis à la première).

En particulier, s'il y a un élément neutre u pour $\perp$, deux éléments réguliers pour la loi $\top$ sont permutables pour $\top$ (prendre $x'=y'=u$) ; si tous les éléments sont réguliers pour $\top$, cette loi est commutative.

3) Soient données, dans E, une addition pour laquelle tous les $x \in E$ soient inversibles, et une multiplication $\circ$ doublement distributive par rapport à + ; on pose $x \circ y = xy - yx$. Pour que x et y soient permutables pour $\circ$, il faut et il suffit que $x \circ y = 0$; et on a les identités

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

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

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

ce qui exprime la "déviation de l'associativité" de la loi $\circ$.

4) Soit E muni d'une loi associative . ; soit L(E) le système associatif libre déduit de E (exerc.6 du § 1) ; à tout élément u de L(E), on fait correspondre le composé f(u) de l'une quelconque des suites qui définissent u : montrer que f(u) est un homomorphis de L(E) sur E. Plus généralement, si $X \subset E$, et si A est la parti stable engendrée par X, montrer qu'on définit d'une manière analc gue un homomorphisme de L(X) sur A.

5) Soient deux lois internes sur E, $\top$ et $\perp$, possédant chacune un élément neutre ; si la loi externe à gauche déduite de chacune de ces lois est distributive par rapport à l'autre loi, tout élément de E est idempotent pour ces deux lois.

§ 4. Groupes ; groupes à opérateurs.

1. Groupes. Définition 1. On dit qu'une loi de composition interne, entre éléments d'un ensemble G , définit sur G une structure de groupe, et que G , muni de cette structure, est un groupe, si la loi est associative, s'il existe un élément neutre, et si tous les éléments de G sont inversibles pour cette loi.

Naturellement, l'existence d'un élément neutre est impliquée par celle d'éléments inversibles, et est donc conséquence des autres conditions pourvu que G soit non vide.

Exemples. 1) Si E est un ensemble muni d'une loi associative ayant un élément neutre, la structure induite par cette loi sur l'ensemble des éléments inversibles de E est une structure de groupe. Il en est donc ansi, en particulier, de la structure déterminée par la loi $\circ$ sur l'ensemble des applications biuni-voques d'un ensemble E sur lui-même (§ 2, n°3, ex.2), ou ensemble des permutations de E , qui muni de cette structure, s'appellera donc le groupe des permutations de E . Les groupes de permutations de deux ensembles équipotents sont évidemment isomorphes.

2) L'ensemble $\mathbf{Z}$, avec l'opération $+$, est un groupe qui s'appelle le groupe additif des entiers rationnels.

3) L'ensemble Q_+^* des nombres rationnels >0 (§ 2, n°5) est un groupe pour la multiplication. De même, plus généralement, pour l'ensemble des éléments réguliers de tout ensemble formé par application du th.1 du § 2.

Si une loi de composition sur G définit sur G une structure de groupe, il en est de même de la loi opposée : les deux groupes ainsi définis sur G sont dits opposés. Dans un groupe G , l'application de G sur lui-même qui, à tout $x \in G$, fait correspondre

l'élément inverse, est (d'après la prop.5 du § 2) un isomorphisme de G sur le groupe opposé, qu'on appelle la symétrie ou l'application symétrique de G sur lui-même : c'est une permutation involutive de G .

Dans ce § , sauf indication contraire, nous noterons toujours multiplicativement la loi de composition d'un groupe, et nous noterons e l'élément neutre d'une loi de groupe ainsi notée. La symétrie d'un groupe G sur lui-même s'écrit alors $x \to x^{-1}$. Suivant nos conventions générales (Ens.R, § 2,n°4), A^{-1} sera l'image, par la symétrie du groupe, d'une partie A de G . Mais il importe de noter que, malgré l'analogie des notations, A^{-1} n'est pas du tout élément inverse de A pour la loi de composition $(A,B) \to A.B$ entre parties de G (rappelons que A.B est l'ensemble des ab pour $a \in A$, $b \in B$) : en effet, l'élément neutre pour cette loi est $\{e\}$, et les seuls éléments de $\mathfrak{P}(G)$, inversibles pour cette loi, sont les ensembles $A=\{a\}$ à un seul élément (un tel A , d'ailleurs a bien pour inverse A^{-1}). On a l'identité $(AB)^{-1}=B^{-1}A^{-1}$ pour $A \subset G$, $B \subset G$. On dit que A est symétrique si $A=A^{-1}$. Quel que soit $A \subset E$, $A \cup A^{-1}$ et $A \cap A^{-1}$ sont symétriques.

L'application aux structures de groupe des définitions générales posées au § 3 conduit à examiner successivement les structures induites par une structure de groupe, et les structures quotients et produits de structures de groupes.

2. Sous-groupes. Soit H une partie d'un groupe G : pour que la loi induite sur H par la loi de composition de G soit partout définie, il faut et il suffit que H soit stable, c'est-à-dire (§ 1, n° 3) que $H.H \subset H$; pour qu'elle détermine sur H une structure de groupe, il faut d'abord

qu'elle possède un élément neutre u , qui satisfera à $u.u=u$, d'où (u étant inversible dans G), $u=u.u^{-1}=e$; autrement dit, H contient e qui est élément neutre pour la loi induite sur H ; il s'ensuit que, si $x\in H$ est inversible dans H , son inverse dans H n'est autre que x^{-1} : pour que H soit un groupe il faut donc que $H^{-1}\subset H$; la symétrie de G en G transforme cette inclusion en $H\subset H^{-1}$, on doit donc avoir $H=H^{-1}$ et aussi $H.H=H$ (car $e\in H$ entraîne $X\subset H.X$ quel que soit $X\subset G$, donc $H\subset H.H$), et par suite $H.H^{-1}=H^{-1}.H=H$. Réciproquement, si une partie non vide H de G satisfait à $H.H^{-1}\subset H$, on a, pour $x\in H$, $x.x^{-1}\in H$ ou $e\in H$, puis $e.x^{-1}\in H$ ou $x^{-1}\in H$, donc $H^{-1}\subset H$, d'où (comme plus haut) $H^{-1}=H$, d'où enfin $H.H\subset H$; la loi . est donc définie partout sur H , associative, elle a un élément neutre e , et tout $x\in H$ est inversible : H est bien un groupe.

Définition 2. Une partie H d'un groupe G , sur laquelle la loi de composition de G induise une structure de groupe, s'appellera un sous-groupe de G .

Proposition 1. Si H est un sous-groupe de G, on a $H=H^{-1}=H.H$; réciproquement, si H G et $H\neq\emptyset$, H sera sous-groupe de G si on a , soit $H.H^{-1}\subset H$, soit $H^{-1}.H\subset H$, soit $H.H\subset H$ et $H^{-1}\subset H$.

Si H est un sous-groupe de G et K un sous-groupe de H , il est clair que K est sous-groupe de G . L'ensemble $\{e\}$ est un sous-groupe de G ; c'est évidemment le plus petit (il est contenu dans tous les sous-groupes de G). L'intersection H d'une famille de sous-groupes H_ι est un sous-groupe, car elle est non vide (on a $e\in H_\iota$ quel que soit ι) et $x\in H$, $y\in H$ entraîne $xy^{-1}\in H_\iota$ quel que soit ι , donc $xy^{-1}\in H$. Il y a donc un plus petit sous-groupe de G contenant un $X\subset G$ donné ; on l'appelle le sous-groupe engendré par X .

Exemple. Soit H un sous-groupe du groupe additif $\mathbb{Z}$ des entiers rationnels : si H n'a pas pour seul élément l'élément neutre 0, soit $x \in H$, $x \neq 0$: ou bien $x > 0$, ou bien $x < 0$ et alors $x' = -x > 0$, $x' \in H$, donc l'ensemble des éléments > 0 de H est non vide : soit a le plus petit. Par récurrence sur $m \in \mathbb{N}^*$, on voit que $ma \in H$; donc aussi $-ma \in H$ pour $m \in \mathbb{N}^*$, et comme $0 \in H$, il suit que $na \in H$ quel que soit $n \in \mathbb{Z}$. Si $x \in H$, on a (§ 3, n°9) $x = qa + r$, $0 \leqslant r < a$; $qa \in H$, donc $x - qa \in H$: mais par définition de a , $0 < r < a$ entraîne $r \notin H$, donc $r = x - qa = 0$, $x = qa$: H est donc l'ensemble des na pour $n \in \mathbb{Z}$, c'est-à-dire $H = a.\mathbb{Z}$. Réciproquement, $a.\mathbb{Z}$ est évidemment un sous-groupe de $\mathbb{Z}$ pour $a \in \mathbb{N}^*$; si $a = 0$, $a.\mathbb{Z} = 0$ si $a < 0$ et $a' = -a$, on a $a' > 0$ et $a.\mathbb{Z} = a'.\mathbb{Z}$; il résulte d'ailleurs de la démonstration ci-dessus que $a.\mathbb{Z}$ est le sous-groupe engendré par $\{a\}$, et que la partie stable de $\mathbb{Z}$ engendrée par a est l'ensemble $a.\mathbb{N}^*$ des ma pour $m \in \mathbb{N}^*$.

Comme le montre cet exemple, il faut se garder de confondre la partie stable d'un groupe G engendrée par $X \subset G$ avec le sous-groupe engendré par X : celui-ci contient toujours celle-là, mais en est distinct en général. On a en tout cas la proposition suivante :

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

En effet, Y^∞ est l'ensemble des composés des séquences dont tous les termes sont des éléments de X ou des inverses d'éléments de X : l'inverse d'un tel composé est un composé de même forme (§ 2, prop. 5) ,

et si $x \in X$, Y^{∞} contient $x.x^{-1}=e$, donc Y^{∞} est un sous-groupe de G ; réciproquement, tout sous-groupe contenant X contient évidemment Y , donc Y^{∞}.

3. Groupes quotients. Passons aux structures quotients : il faut d'abord rechercher quelles sont les relations d'équivalence compatibles avec une structure de groupe. D'après la prop.1 du § 3, il y a lieu d'examiner séparément d'abord la compatibilité à gauche et à droite ; la question est résolue par le théorème suivant :

Théorème 1. Toute relation d'équivalence sur un groupe G , compatible à gauche avec la structure du groupe, est de la forme $x^{-1}y \in H$ (ou de la forme équivalente $y \in xH$), H étant un sous-groupe de G , et réciproquement ; toute relation compatible à droite avec la structure du groupe est de la forme $yx^{-1} \in H$ (ou $y \in Hx$) , H étant un sous-groupe, et réciproquement.

La seconde partie se déduit de la première par passage de G au groupe opposé. Soit donc R compatible à gauche avec la structure ; si $x \equiv e \pmod{R}$, on a $y.x \equiv y.e \pmod{R}$ quel que soit y , donc $yx \equiv y \pmod{R}$; en particulier, si $y=x^{-1}$, on a $e \equiv x^{-1} \pmod{R}$, donc $x \equiv e$ entraîne $x^{-1} \equiv e$; si $y \equiv e$, on a $yx \equiv y \equiv e$; donc, si H est la classe d'équivalence de e , on a $H^{-1} \subset H$ et $H.H \subset H$, H est un sous-groupe. Alors, si $x \equiv y \pmod{R}$, on a $x^{-1}x \equiv x^{-1}y \pmod{R}$ ou $x^{-1}y \in H$; et si $x^{-1}y \in H$, on a $x^{-1}y \equiv e$, $x(x^{-1}y) \equiv x$, donc $y \equiv x \pmod{R}$. Supposons, réciproquement, qu'on se soit donné un sous-groupe H de G ; les relations $x^{-1}y \in H$ et $y \in xH$ sont bien équivalentes, car la seconde se déduit de la première par la translation γ_x , qui est une application biunivoque de G sur G (§ 2, prop.3) ; si $x^{-1}y \in H$ on a $y^{-1}x=(x^{-1}y)^{-1} \in H^{-1}=H$,

donc cette relation est symétrique ; si $y \in xH$, $z \in yH$, on a $z \in x.HH=xH$, donc elle est transitive, et c'est bien une relation d'équivalence. Si $y \in xH$, on a $zy \in zxH$ quel que soit z , la relation est bien compatible à gauche avec la loi du groupe.

Tout sous-groupe H de G définit donc ainsi deux relations d'équivalence dans G , à savoir $y \in xH$ et $y \in Hx$: les classes d'équivalence pour ces relations sont respectivement les ensembles xH , qu'on appelle <u>classes à gauche suivant H</u> (ou <u>modulo H</u>), et Hx , qui s'appellent <u>classes à droite suivant H</u> (ou <u>modulo H</u>) . En saturant $A \subset G$ par rapport à ces relations, on obtient respectivement les ensembles AH et HA . Par passage au groupe opposé, tout sous-groupe H reste sous-groupe, les classes à gauche s'échangent avec les classes à droite ; par la symétrie de G en G , tout sous-groupe H est appliqué sur lui-même, les classes à gauche sont transformées en classes à droite et réciproquement.

Pour qu'une relation d'équivalence soit compatible avec la loi de groupe, il faut et il suffit qu'elle le soit à gauche et à droite ; si H est la classe d'équivalence de e , H sera donc un sous-groupe tel que les relations $y \in xH$ et $y \in Hx$ soient équivalentes, c'est-à-dire tel que $xH=Hx$ quel que soit x ; réciproquement, s'il en est ainsi, l'une ou l'autre des relations $y \in xH$, $y \in Hx$ est compatible avec la loi du groupe. Les classes à gauche coïncidant avec les classes à droite pour un tel sous-groupe, on aura $AH=HA$ quel que soit $A \subset G$. L'égalité $xH=Hx$ étant équivalente à $xHx^{-1}=H$ (celle-ci se déduisant de celle-là par la translation $\delta_{x^{-1}}$) on posera :

<u>Définition 3.</u> <u>Un sous-groupe H de G s'appellera sous-groupe distingué</u> (ou <u>invariant</u>) <u>de G si on a</u> $xHx^{-1}=H$ <u>quel que soit</u> $x \in G$.

Théorème 2. Toute relation d'équivalence compatible avec la loi d'un groupe G est de l'une des formes équivalentes $y \in xH$ ou $y \in Hx$, H étant un sous-groupe distingué de G ; et le quotient de G par cette relation est un groupe.

La première partie résulte de ce qui précède. Quant à la seconde elle résulte de la remarque déjà faite (§ 3, n°5) que la classe de l'élément neutre est élément neutre pour la loi quotient, et que les classes de deux éléments inverses l'un de l'autre sont inverses l'une de l'autre pour la loi quotient.

Définition 4. Le quotient d'un groupe G par la relation d'équivalence définie par un sous-groupe distingué H s'appelle le groupe quotient de G par H ; il se note G/H .

On notera parfois $x \equiv y \pmod{H}$ ou $x \equiv y \ (H)$ la relation d'équivalence définie par un sous-groupe distingué H .

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

G et $\{e\}$ sont des sous-groupes distingués de G (les quotients G/G et $G/\{e\}$ étant isomorphes respectivement à $\{e\}$ et à G) : si ce sont les seuls, G est dit simple. H étant sous-groupe distingué de G si $xyx^{-1} \in H$ quels que soient $x \in G$ et $y \in H$, il s'ensuit que l'intersection de toute famille de sous-groupes distingués de G est un sous-groupe distingué de G (on peut donc parler du plus petit sous-groupe distingué de G contenant $X \subset G$). Mais on notera que, si H est sous-groupe distingué de G et K sous-groupe distingué de H, K n'est pas toujours sous-groupe distingué de G (on en verra des exemples).

4. Représentations. Les définitions et résultats généraux du § 3, relatifs aux représentations, s'appliquent naturellement aux groupes. En particulier :

Définition 4. Une application f d'un groupe G dans un groupe G' s'appelle une représentation ou un homomorphisme de G dans G' si (G et G' étant notés multiplicativement) elle satisfait à $f(xy)=f(x)f(y)$ quels que soient $x \in G, y \in G$.

Si f est biunivoque, on dira que c'est un isomorphisme dans G'. L'application canonique de G sur G/H, H étant un sous-groupe distingué de G, s'appelle homomorphisme canonique de G sur G/H. Le th.1 du § 3 donne ici (en appliquant aussi le th.2 ci-dessus) :

Théorème 3. f étant une représentation d'un groupe G dans un groupe G', l'image réciproque $f^{-1}(e')$ de l'élément neutre e' de G' est un sous-groupe distingué H de G ; l'image $f(G)$ de G dans G' est un sous-groupe de G', isomorphe à G/H ; et f est composée d'un isomorphisme de G/H dans G' et de l'homomorphisme canonique de G sur G/H.

Autrement dit, la décomposition canonique de f (Ens.R, § 5, n°3) donne : 1° l'isomorphisme canonique de f(G) dans G' ; 2° un isomorphisme de G/H sur f(G) ; 3° l'homomorphisme canonique de G sur G/H .

Suivant toujours le § 3, une représentation de G dans G s'appellera un endomorphisme de G ; un isomorphisme de G sur G s'appellera un automorphisme de G . Le composé de deux endomorphismes par la loi ∘ sera encore un endomorphisme ; l'ensemble des automorphismes, avec cette même loi, forme un groupe (sous-groupe du groupe des permutations de l'ensemble G).

Proposition 3. Si $x \in G$, l'application α_x de G dans G , définie par $\alpha_x(y)=xyx^{-1}$, est un automorphisme de G ; et l'on a $\alpha_{xy}=\alpha_x \circ \alpha_y$.

α_x est une représentation, car $x.yz.x^{-1}=(xyx^{-1})(xzx^{-1})$. Si $u \in G$, $xyx^{-1}=u$ est équivalent à $y=x^{-1}ux$, donc il existe un y et un seul tel que $\alpha_x(y)=u$, et α_x est bien une application biunivoque de G sur G , c'est donc un automorphisme de G . Le second point se vérifie immédiatement.

$x \to \alpha_x$ est donc une représentation de G dans le groupe des permutations de l'ensemble G ; l'ensemble des automorphismes α_x est donc, d'après le th.3, un sous-groupe du groupe des automorphismes de G , qui s'appelle groupe des automorphismes intérieurs de G , les α_x s'appelant automorphismes intérieurs. Par le th.3, l'ensemble des $x \in G$ tels que α_x soit l'application identique de G sur G est un sous-groupe distingué Z de G : or c'est l'ensemble des x tels que $xyx^{-1}=y$ quel que soit y , c'est-à-dire tels que $xy=yx$ quel que soit y ; c'est donc le centre de G (§ 1, n°4). Il suit encore du th. 3 que le groupe des automorphismes intérieurs de G est isomorphe au quotient G/Z de G par son centre.

Un automorphisme de G , et en particulier un automorphisme intérieur, transforme évidemment un sous-groupe en un sous-groupe isomorphe ; la déf.3 signifie qu'un sous-groupe est distingué s'il est transformé en lui-même par tous les automorphismes intérieurs de G . Enfin (le groupe étant noté multiplicativement) on pose souvent

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

cette notation étant justifiée (d'après les conventions du § 3) par le fait que y^x , considéré comme loi <u>externe</u> de composition entre opérateurs $x \in G$ et éléments y de G , est distributive par rapport à la loi de groupe entre éléments y , et associative par rapport à la loi opposée entre opérateurs x , c'est-à-dire qu'on a les identités

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

5. <u>Produits de groupes</u>. Passons enfin au produit de structures de groupe : il est immédiat, d'après les remarques du § 3, n°10, qu'un tel produit est encore une structure de groupe, de sorte qu'on peut poser :

<u>Définition 5</u>. <u>Le produit de groupes</u> $(G_\iota)_{\iota \in I}$ <u>est l'ensemble</u> $G = \prod_{\iota \in I} G_\iota$ <u>avec la structure de groupe déterminée sur lui par la loi qui, à</u> $x=(x_\iota)$, $y=(y_\iota)$, <u>fait correspondre le produit</u> $xy=(x_\iota y_\iota)$.

Si $J \subset I$ et $K = \complement J$, la projection pr_J de G sur $G_J = \prod_{\iota \in J} G_\iota$ est évidemment un homomorphisme de G sur G_J , dans lequel l'image réciproque de l'élément neutre est l'ensemble des $x=(x_\iota)$ tels que $x_\iota = e_\iota$ quel que soit $\iota \in J$ (e_ι désignant l'élément neutre de G_ι) : cet ensemble est donc un sous-groupe distingué de G ; il est isomorphe à $G_K = \prod_{\iota \in K} G_\iota$, et on l'identifiera souvent avec G_K .

Soit en particulier un <u>produit fini</u> $G = \prod_{1 \leqslant i \leqslant n} G_i$: l'ensemble des $x=(x_i)$ tels que $x_j = e_j$ pour $j \neq i$ est un sous-groupe distingué H_i de G , isomorphe à G_i . Il est immédiat que tout élément de H_i est

permutable avec tout élément de H_j pour $j \neq i$. Si $x=(x_i) \in G$, et si $u_i=(u_{ij})$ est l'élément de H_i tel que $u_{ii}=x_i$, $u_{ij}=e_j$ pour $j \neq i$, on a $x=u_1u_2..u_n$; réciproquement, si $x=v_1v_2...v_n$, $v_i \in H_i$ $(1 \leqslant i \leqslant n)$, et si $pr_i(v_i)=y_i$, on a $x=(y_i)$, donc $y_i=x_i$, $v_i=u_i$: les u_i sont donc déterminés d'une manière unique par x ; d'ailleurs x est aussi le composé de toute suite qui se déduit de la suite $u_1,u_2,...,u_n$ par une permutation quelconque.

Réciproquement, on dit que le groupe G est <u>produit direct</u> (si G est noté additivement, on dit quelquefois <u>somme directe</u>) des sous-groupes H_i de G $(1 \leqslant i \leqslant n)$ si tout élément de H_i est permutable avec tout élément de H_j pour $j \neq i$, et si tout $x \in G$ peut se mettre d'<u>une manière et d'une seule</u> sous la forme $x=u_1u_2...u_n$ avec $u_i \in H_i$ $(1 \leqslant i \leqslant n)$. S'il en est ainsi, u_i étant bien déterminé par x au moyen de cette relation, soit $u_i=f_i(x)$. Soient $y \in G$, $v_i=f_i(y)$: on a $y=v_1v_2...v_n$; par la condition de permutabilité sur les H_i , on a $xy=(u_1v_1)(u_2v_2)...(u_nv_n)$: ce qu'on voit aisément en supposant que $u_i=v_i=e$ pour $i>p$, et en procédant par récurrence sur p (on observera que $u_pv_1v_2..v_{p-1}= v_1v_2...v_{p-1}u_p$ d'après la prop.2 du § 1). Il s'ensuit que $f_i(xy)=f_i(x)f_i(y)$: f_i est un homomorphisme de G dans H_i , et même <u>sur</u> H_i puisque $f(H_i)=H_i$. Si donc $x \in G$, $u=(u_i) \in \prod_{1 \leqslant i \leqslant n} H_i$, les relations $u_i=f_i(x)$, $x=u_1u_2...u_n$ établissent un isomorphisme entre G et $H=\prod_i H_i$, qui applique $H_i \subset G$ sur le sous-groupe de H formé des $u=(u_i)$ tels que $u_j=e$ pour $j \neq i$: d'où résulte en particulier que les H_i sont des sous-groupes distingués de G . Le produit direct étant ainsi isomorphe au produit proprement dit, il arrivera souvent qu'on ne fera pas de différence entre ces deux notions.

6. Groupes à opérateurs. Définition 6. On appelle groupe à opérateurs un ensemble G dont la structure est définie par une loi de groupe, et une ou plusieurs lois de composition externes distributives par rapport à la loi de groupe .

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

Dans une structure de groupe à opérateurs sur G , chaque opérateur définit un endomorphisme du groupe G ; la donnée de chacune des lois de composition externes qui déterminent la structure revient à la donnée d'une famille d'endomorphismes du groupe G , famille qui a Ω pour ensemble d'indices si Ω est le domaine des opérateurs de la loi ; la réunion des ensembles d'endomorphismes appartenant à ces diverses familles s'appellera l'ensemble des endomorphismes structuraux du groupe G . Dans ce qui va suivre, le groupe G étant noté multiplicativement, on notera exponentiellement les endomorphismes structuraux (suivant les conventions du § 3, n°11), c'est-à-dire que le composé d'un opérateur α de l'une des lois externes définies sur G , et de $x \in G$, s'écrira x^{α} .

Un groupe peut évidemment toujours être considéré comme groupe à opérateurs avec un seul ensemble d'opérateurs réduit à un seul élément α tel que $x^{\alpha}=x$ quel que soit x (opérateur neutre). Les résultats que nous allons énoncer sur les groupes à opérateurs s'appliquent donc d'eux-mêmes aux groupes. Nous examinerons successivement (en application du § 3) les structures induites, les structures quotients et les représentations, les structures produits.

7. Sous-groupes stables. Les structures induites ne prêtent à aucune remarque particulière ; il y a seulement intérêt à expliciter la définition suivante :

Définition 7. Par un sous-groupe stable d'un groupe à opérateurs G, on entend un sous-groupe H de G, stable par rapport aux lois externes définies sur G (c'est-à-dire appliqué dans lui-même par tous les endomorphismes structuraux de G), muni de la structure de groupe à opérateurs induite sur lui par celle de G.

G et $\{e\}$ sont toujours des sous-groupes stables de G ; l'intersection de toute famille de sous-groupes stables est un sous-groupe stable ; le plus petit sous-groupe stable contenant $X \subset G$ sera dit engendré par X : il n'est autre que la partie de G, stable à la fois par rapport à la loi interne et aux lois externes définies sur G, engendrée par $X \cup X^{-1}$. On notera qu'un sous-groupe distingué de G n'est pas autre chose qu'un sous-groupe stable pour la loi de composition $(s,x) \to x^s = s^{-1}xs$, dont G est le domaine d'opérateurs : cette loi, jointe à la structure de groupe, induisant donc sur tout sous-groupe distingué de G une structure de groupe à opérateurs dont le domaine d'opérateurs est encore G.

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

Théorème 4. Toute relation d'équivalence sur un groupe à opérateurs G, compatible à gauche avec la structure de G, est de la forme $x^{-1}y \in H$, où H est un sous-groupe stable de G : et réciproquement.

Par le th.1, la classe d'équivalence de e est un sous-groupe H ; pour tout endomorphisme structural α, si x est équivalent à e,

x^{α} doit l'être à $e^{\alpha}=e$, donc $H^{\alpha} \subset H$, H est stable ; par le th. 1 , la relation s'écrit $x^{-1}y \in H$. Réciproquement, si H est stable, $y \in xH$ entraîne $y^{\alpha} \in x^{\alpha}.H^{\alpha} \subset x^{\alpha}.H$, la relation est bien compatible avec la structure.

Le th.2 s'étend alors immédiatement. De même la déf.4 : le quotient d'un groupe à opérateurs G par la relation définie par un sous-groupe stable distingué H , muni de sa structure quotient, s'appellera le groupe à opérateurs quotient de G par H , et se notera G/H .

Conformément aux définitions générales, une application f d'un groupe à opérateurs G dans un groupe à opérateurs G' ayant une structure de même espèce (donc en particulier ayant mêmes domaines d'opérateurs) si l'on a identiquement, pour $x \in G$, $y \in G$, et pour tout opérateur α appartenant à la structure de G :

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

On notera qu'en particulier un endomorphisme du groupe à opérateurs G (représentation de G dans lui-même) n'est pas autre chose qu'un endomorphisme du <u>groupe</u> G , <u>permutable</u> avec tous les endomorphismes structuraux $x \longrightarrow x^{\alpha}$.

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

<u>Théorème 5</u>. <u>f étant une représentation d'un groupe à opérateurs G dans G' pourvu d'une structure de même espèce, l'image réciproque</u> $f^{-1}(e')$ <u>de l'élément neutre e' de G' est un sous-groupe stable distingué H de G ; f(G) est un sous-groupe stable de G' , isomorphe à G/H ; et f est composée d'un isomorphisme de G/H dans G' , et de l'homomorphisme canonique de G sur G/H .</u>

La prop.2 et les th.2 et 3 du § 3 s'appliquent naturellement aux groupes à opérateurs (donc à plus forte raison aux groupes) ; en combinant les th.2 et 3 du § 3 , et les complétant sur quelques points, on obtient le théorème :

Théorème 6. Soit f l'homomorphisme canonique du groupe à opérateurs G sur le quotient $G'=G/H$ de G par le sous-groupe stable distingué H . L'image réciproque $K=f^{-1}(K')$ d'un sous-groupe stable K' de G' est un sous-groupe stable de G , tel que $H \subset K$, et la relation $K=f^{-1}(K')$ établit une correspondance biunivoque entre les sous-groupes stables K' de G' et les sous-groupes stables K de G tels que $H \subset K$; si $K=f^{-1}(K')$, on a $K'=f(K)$, et K' est isomorphe à K/H . Si K' est sous-groupe distingué de G' , K est sous-groupe distingué de G , et G/K est isomorphe à G'/K' , donc à $(G/H)/(K/H)$. Si L est un sous-groupe stable quelconque de G , il en est de même de $L.H=H.L$; $H \cap L$ est sous-groupe stable distingué de L , et $L/(H \cap L)$ est isomorphe à HL/H .

En effet, il est immédiat que, si K' est sous-groupe stable de G' , $K=f^{-1}(K')$ l'est de G et contient H ; f appliquant G sur G' applique alors nécessairement K sur K', qui dans ces conditions est isomorphe à K/H par le th.5 . Si L est sous-groupe stable de G , la restriction de f à L est une représentation de L dans G' ; par le th.5, l'image réciproque $L \cap H$ de l'élément neutre par cette représentation est sous-groupe stable distingué de L , et $f(L)$ est isomorphe à $L/(L \cap H)$, et aussi, par le th.3 du § 3, au quotient HL/H , par H , de la partie $L.H=H.L$ de G obtenue en saturant L pour la relation $y \in xH$. Appliquant ces résultats à $L=K \supset H$, on aura $KH \subset KK=K$, donc $KH=K$, K est saturé, c'est-à-dire que, si $K'=f(K)$, on a $K=f^{-1}(K')$: la correspondance entre K et K' est

bien biunivoque. Enfin, le th.2 du § 3 signifie ici que si $K \supset H$ est sous-groupe stable distingué de G, K' l'est de G', et réciproquement, et que G/K est isomorphe à $(G/H)/(K/H)$.

9. Le théorème de Jordan-Hölder. Parmi toutes les conséquences importantes du th.6, nous donnerons le théorème connu sous le nom de Jordan-Hölder, qui se rapporte aux suites finies de sous-groupes d'un groupe G, dont chacun est distingué dans le précédent. Nous aurons besoin de quelques propositions préliminaires :

Proposition 4. Soient K, K' deux sous-groupes stables d'un groupe à opérateurs G, et H un sous-groupe stable distingué de K : alors la trace $H \cap K'$ de H sur K' est sous-groupe stable distingué de la trace $K \cap K'$ de K sur K'.

Evidemment, $K \cap K'$ est sous-groupe stable de G, et $H \cap K'$ de $K \cap K'$. Soit $x \in K \cap K'$: le transformé $(H \cap K')^x$ par l'automorphisme intérieur $y \to y^x$ de G n'est autre que $H^x \cap K'^x$; puisque $x \in K'$, on a $K'^x = K'$; puisque $x \in K$ et que H est distingué dans K, on a $H^x = H$; on a donc bien $(H \cap K')^x = H \cap K'$.

Proposition 5. Soient K sous-groupe stable de G ; H et L sous-groupes stables distingués de G et K respectivement. Alors $L.H$ est sous-groupe stable distingué de $K.H$, $L.(K \cap H)$ de K, et les quotients KH/LH et $K/L.(K \cap H)$ sont isomorphes.

Soient f l'homomorphisme canonique de G sur G/H, φ sa restriction à K, qui est un homomorphisme de K dans G/H ; soient $f(K) = K'$ $f(L) = L'$; φ est un homomorphisme de K sur K', donc l'image L', par φ, du sous-groupe distingué L de K est sous-groupe distingué de K' ; si e' est l'élément neutre de G/H, donc de K', on a

$\varphi^{-1}(e')=K\cap H$, donc (par le th.6), $\varphi^{-1}(L')=L.(K\cap H)$; par le th.6, $K/L.(K\cap H)$ est isomorphe à K'/L' (K, $L.(K\cap H)$, K' et L' prenant respectivement la place des quatre groupes notés G,K,G' et K' dans l'énoncé du th.6). D'autre part, par le th.6, $f^{-1}(K')=K.H$, $f^{-1}(L')=L.H$: la restriction de f à K.H est un homomorphisme, donc par le même raisonnement L.H est distingué dans K.H , et KH/LH est isomorphe à K'/L' .

Proposition 6. Soient K,K' sous-groupes stables de G , H et H' sous-groupes stables distingués de K et K' respectivement : alors les quotients $((K\cap K').H')/((H\cap K').H')$ et $((K\cap K').H)/((H'\cap K).H)$ sont isomorphes.

(Cet énoncé implique que $(H\cap K').H'$ est distingué dans $(K\cap K').H'$ et de même pour l'autre quotient).

En effet, $K\cap H'$ est distingué dans $K\cap K'$ (prop.4) ; dans la prop.5, remplaçons alors G,H,K,L par $K,H,K\cap K',K\cap H'$ respectivement : on trouve que $(K\cap K').H/(K\cap H').H$ est isomorphe à $(K\cap K')/(K\cap H').(K\cap K'\cap H)$, c'est-à-dire à $(K\cap K')/(K\cap H').(H\cap K')$; dans ce dernier quotient, K et H d'une part, K' et H' de l'autre figurent symétriquement, et en les permutant on obtient le résultat annoncé.

Définition 8. Par une suite de composition d'un groupe à opérateurs G , on entend une suite finie $(G_i)_{0\leqslant i\leqslant n}$ de sous-groupes stables de G , ayant pour premier terme $G_o=G$, pour dernier terme $G_n=\{e\}$, et telle que G_{i+1} soit sous-groupe distingué de G_i quel que soit $i<n$. Les quotients G_i/G_{i+1} s'appellent les quotients de la suite. Une suite de composition Σ' est dite plus fine qu'une suite de composition Σ mx si Σ est une suite extraite de Σ' .

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

Proposition 7. (Lemme de Zassenhaus). Etant données deux suites de composition Σ_1, Σ_2 du groupe à opérateurs G , il y a des suites de composition Σ'_1, Σ'_2 de G , plus fines respectivement que Σ_1 et Σ_2, et telles que le système des quotients de Σ'_1 soit identique à celui de Σ .

Soient $(G_i)_{0 \leqslant i \leqslant n}$, $(H_j)_{0 \leqslant j \leqslant p}$ les suites données. Construisons comme suit deux suites de sous-groupes de G . Posons $G'_{ij}=(G_i \cap H_j).G_{i+1}$, pour $0 \leqslant i \leqslant n-1$, $0 \leqslant j \leqslant p$, et $H'_{ji}=(G_i \cap H_j).H_{j+1}$ pour $0 \leqslant i \leqslant n$, $0 \leqslant j \leqslant p-1$. Il résulte de la prop.6 que $G'_{i,j+1}$ est sous-groupe distingué de G'_{ij} , $H'_{j,i+1}$ de H'_{ji} et que $G'_{ij}/G'_{i,j+1}$ est isomorphe à $H'_{ji}/H'_{j,i+1}$. D'autre part, on a $G'_{ip}=G'_{i+1,0}=G_{i+1}$, $H'_{jn}=H'_{j+1,0}=H_{j+1}$. Avec les G'_{ij} , on formera alors de la manière suivante la suite de composition Σ'_1 : on donnera à l'indice (ij) toutes les valeurs satisfaisant à $j < p$ ou à $i=n-1$, l'ensemble de ces np+1 valeurs étant ordonné lexicographiquement, c'est-à-dire par $(ij)<(i'j')$ pour $i<i'$ ou $i=i'$ et $j<j'$: dans ces conditions, l'élément qui suit (ij) est (i,j+1) si $j<p-1$ ou si $i=n-1, j=p-1$; l'élément qui suit (i,p-1) pour $i<n-1$ est (i+1,0) : dans l'un et l'autre cas, il apparait bien que, dans la suite des groupes G'_{ij} formée au moyen de cet ensemble d'indices ainsi ordonné, chaque groupe est sous-groupe stable distingué du précédent ; et le système des quotients de cette suite est l'ensemble des $G'_{ij}/G'_{i,j+1}$ pour $0 \leqslant i \leqslant n-1$, $0 \leqslant j \leqslant p-1$. De même pour les H'_{ji} en échangeant les indices i et j et les nombres n et p. La proposition est démontrée.

On dit qu'une suite de composition est sans répétition si tous les termes en sont distincts deux à deux.

Définition 9. Un groupe à opérateurs G est dit simple s'il n'y a aucun sous-groupe stable distingué de G autre que G et $\{e\}$.

Définition 10. On appelle suite de Jordan-Hölder d'un groupe à opérateurs G une suite de composition sans répétition, telle qu'il n'existe aucune suite de composition sans répétition strictement plus fine.

Proposition 8. Pour qu'une suite de composition sans répétition de G soit suite de Jordan-Hôlder de G , il faut et il suffit que tous les quotients de la suite soient simples.

Si la suite donnée n'est pas suite de Jordan-Hölder, c'est qu'il y a une suite de composition sans répétition strictement plus fine. Les deux suites n'étant pas identiques, il y aura deux termes consécutifs G_i, G_{i+1} de la première qui ne seront pas consécutifs dans la seconde : soit H le premier terme qui suit G_i dans celle-ci, c'est un groupe stable distingué de G_i qui contient G_{i+1} ; la seconde suite étant sans répétition, $H \neq G_{i+1}$. Dans l'homomorphisme canonique de G_i sur G_i/G_{i+1} , l'image de H est donc un sous-groupe stable distingué du quotient G_i/G_{i+1} , distinct de celui-ci et de l'élément neutre, ce quotient n'est donc pas simple. Réciproquement, si l'un des quotients G_i/G_{i+1} de la suite donnée n'est pas simple, il contient un sous-groupe stable distingué autre que lui-même et l'élément neutre, dont l'image réciproque dans G_i sera donc un sous-groupe stable distingué H de G_i , contenant G_{i+1} , distinct de G_i et G_{i+1} : on obtient donc une suite de composition sans répétition, distincte de la suite donnée et plus fine qu'elle, en insérant le terme H entre G_i et G_{i+1} .

Théorème 7 (Théorème de Jordan-Hölder). Si Σ_1, Σ_2 sont deux suites de Jordan-Hölder d'un groupe à opérateurs G , elles ont même nombre de termes, et les systèmes des quotients des deux suites sont identiques.

Appliquons la prop.7 : on obtient deux suites Σ_1', Σ_2' plus fines respectivement que Σ_1 et Σ_2 ; celles-ci étant des suites de Jordan-Hölder , Σ_1' est identique à Σ_1 ou s'en déduit en répétant certains termes ; le système des quotients de Σ_1' se déduit de celui de Σ_1 en lui ajoutant un certain nombre de termes isomorphes au groupe $\{e\}$; Σ_1 étant sans répétition, le système des quotients de Σ_1 se déduit de celui de Σ_1' en retranchant tous les termes isomorphes à $\{e\}$. De même pour Σ_2 et Σ_2'. Les systèmes des quotients de Σ_1' et Σ_2' étant identiques, il en est donc de même de ceux de Σ_1 et Σ_2 ; en particulier, ils ont même nombre de termes. Le théorème est démontré.

10. Groupes abéliens. Définition 11. Un groupe, ou un groupe à opérateurs, est dit abélien, si sa loi de composition interne est commutative.

Un groupe abélien sera souvent noté additivement ; alors son élément neutre se notera d'ordinaire 0 ; et les opérateurs (s'il y en a) sur un groupe ainsi noté se noterons d'ordinaire multiplicativement, à gauche ou à droite (cf. § 3).

Dans un groupe G quelconque, le sous-groupe X engendré par un élément $x \in G$ est l'ensemble des x^n pour $n \in \mathbb{Z}$, et est toujours abélien ; d'après l'identité $x^{m+n}=x^m x^n$, l'application $n \longrightarrow x^n$ est un homomorphisme du groupe additif $\mathbb{Z}$ sur X ; X est donc isomorphe, soit à $\mathbb{Z}$, soit à un groupe quotient de $\mathbb{Z}$, c'est-à-dire (§ 4,n°3) au groupe

additif des entiers modulo a , si a est le nombre d'éléments distincts de X qui est alors fini.

Soit G un groupe (ou groupe à opérateurs) abélien, noté multiplicativement. Par récurrence sur n , on vérifie que, si $x \in G$, $y \in G$, on a $(xy)^n = x^n y^n$ pour $n \in \mathcal{N}^*$; de même évidemment pour $n=0$; de même pour $n=-m$, $m \in \mathcal{N}^*$, comme on le voit en remplaçant x,y par x^{-1}, y^{-1} . Si G est un groupe à opérateurs, et α un opérateur de la structure de G , $x \longrightarrow x^\alpha$ est un endomorphisme du groupe G , qui applique donc x^n sur $(x^\alpha)^n$: quel que soit $n \in \mathbb{Z}$, $x \longrightarrow x^n$ est donc une représentation du groupe à opérateurs dans lui-même.

En particulier, si G est un groupe abélien quelconque, noté multiplicativement, on pourra le considérer comme groupe à opérateurs, ayant $\mathbb{Z}$ pour domaine d'opérateurs, avec la loi de composition externe $(n,x) \longrightarrow x^n$. De même bien entendu quelle que soit la notation : pour un groupe noté additivement, en particulier, la loi se notera $(n,x) \longrightarrow nx$. Plus généralement, si G est un groupe à opérateurs, on pourra toujours, le cas échéant, adjoindre la loi externe $(n,x) \longrightarrow x^n$ (ou, avec la notation additive, $(n,x) \longrightarrow n.x$) aux lois déjà impliquées dans la structure de G .

Evidemment, le groupe des automorphismes intérieurs d'un groupe abélien se réduit à l'automorphisme identique ; donc tout sous-groupe d'un groupe abélien est sous-groupe distingué. Tout groupe quotient d'un groupe abélien est abélien ; tout produit de groupes abéliens est abélien. Le centre d'un groupe quelconque, ou plus généralement le sous-groupe d'un groupe quelconque engendré par un ensemble d'éléments deux à deux permutables, est abélien.

11. Groupes de transformations. On va examiner plus particulièrement le groupe des applications biunivoques d'un ensemble E sur lui-même, groupe qui dans ce § sera noté $\mathfrak{S}(E)$, de sorte que si $s \in \mathfrak{S}(E)$, $x \to s(x)$ sera une permutation. On a déjà vu (Ens.R, § 8, n°5) qu'une telle application en induit une de chacun des ensembles de l'échelle des types construite à partir de E (et éventuellement d'ensembles auxiliaires) sur lui-même. Ce résultat peut se préciser comme suit :

Théorème 8. Si F est un ensemble de l'échelle des types construite à partir de E et d'ensembles auxiliaires quelconques, et si S est l'application biunivoque de F sur lui-même induite par l'application biunivoque s de E sur lui-même, la correspondance $s \to S$ est une représentation de $\mathfrak{S}(E)$ dans $\mathfrak{S}(F)$.

Rappelons d'abord la définition de S . Par définition de l'échelle des types, F est un ensemble construit à partir des ensembles de base (à savoir E et les ensembles auxiliaires), suivant un schéma explicitement donné, au moyen des opérations "produit de deux ensembles déjà construits" et "formation de l'ensemble des parties d'un ensemble déjà construit" , ou de la répétition de ces opéra-tions de la manière prescrite par le schéma. Une définition ou démonstration relative à F pourra procéder par récurrence suivant le nombre des opérations impliquées par le schéma de F : on n'aura pour cela qu'à la donner pour les ensembles de base, et donner le moyen de l'étendre de proche en proche, soit de deux ensembles déjà construit à l'ensemble de ses parties.

Cela étant, soit $s \in \mathfrak{S}(E)$; posons $S_E = s$, et désignons par S_F l'application identique de F sur lui-même chaque fois que F est l'un des ensembles auxiliaires dont il est question dans l'énoncé du th.8.

Soit maintenant F appartenant à l'échelle des types dont il s'agit : supposons d'abord que ce soit le produit de deux ensembles L et M de cette échelle, c'est-à-dire l'ensemble des couples (u,v) avec $u \in L, v \in M$; $s \in \mathfrak{S}(E)$ étant donné, supposons définies les applications S_L , S_M de L et M respectivement sur eux-mêmes ; si S_L est l'application $u \longrightarrow \sigma(u)$, S_M l'application $v \longrightarrow \tau(v)$, l'application $(u,v) \longrightarrow (\sigma(u), \tau(v))$ de $F=L\times M$ dans F est une application biunivoque de F sur F qui sera notée S_F . Si d'autre part F est l'ensemble des parties d'un ensemble L de l'échelle étudiée, et si S_L est l'application $u \longrightarrow \sigma(u)$ de L sur lui-même, l'application $U \longrightarrow \sigma(U)$ de F dans lui-même, où U désigne une partie générique de L , est une application biunivoque de F sur F qui sera notée S_F . Ce qui précède constitue une définition par récurrence de S_F pour chacun des ensembles F de l'échelle des types construite sur E et sur les ensembles auxiliaires donnés : S_F s'appelle l'application de F sur lui-même qui est induite par l'application s de E sur lui-même .
Le th.8 se vérifie alors aisément par récurrence : la correspondance $s \quad S_E$ est l'application identique de $\mathfrak{S}(E)$ sur lui-même, c'est donc une représentation de $\mathfrak{S}(E)$ dans $\mathfrak{S}(E)$; si F est un ensemble auxiliaire de l'échelle, la correspondance $s \longrightarrow S_F$ fait correspondre à tout $s \in \mathfrak{S}(E)$ l'élément neutre de $\mathfrak{S}(F)$, c'est encore une représentation.

LIVRE II (Etat 3)

CHAPITRE I (suite)

§4. Groupes et groupes à opérateurs (suite)

Exercices. 1) Déterminer toutes les structures de groupe sur un ensemble de n éléments, pour $2 \leqslant n \leqslant 6$. Déterminer les sous-groupes et les groupes quotients de ces groupes.

2) Une loi de composition associative $(x,y) \longrightarrow xy$ dans un ensemble E définit une structure de groupe sur E si elle satisfait aux conditions suivantes : a) il existe $e \in E$ tel que , quel que soit $x \in E$, $ex=x$; b) quel que soit $x \in E$, il existe $y \in E$ tel que $yx=e$.

3) Dans un groupe G , toute partie finie non vide H stable (pour la loi du groupe) est un sous-groupe de G (pour voir que $x \in H$ entraîne $x^{-1} \in H$, considérer le sous-groupe de G engendré par x).

4) Si A est une partie non vide d'un groupe G ne contenant pas l'élément neutre, l'ensemble des sous-groupes (resp. sous-groupes distingués) de G qui ne rencontrent pas A , admet un élément maximal.

5) Soient H,H',K,K' quatre sous-groupes d'un groupe G , tels que $H' \subset H$, $K' \subset K$. Montrer que

$$(H \cap K) \cap (H'K') = (H' \cap K)(H \cap K')$$

6) Soient H et K deux sous-groupes d'un groupe G . Pour que HK soit un sous-groupe de G , il faut et il suffit que $HK = KH$.

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

8) Soit H un sous-groupe fini d'un groupe G , tel qu'il existe un groupe quotient G/H de G isomorphe à H (c'est-à-dire qu'il existe un homomorphisme de G sur H) ; montrer que $H \cap K = \{e\}$.

9) Si H et K sont deux sous-groupes distingués d'un groupe G tels que $H \cap K = \{e\}$, tout élément de H est permutable avec tout élément de K.

10) Soit $(H_i)_{1 \leqslant i \leqslant n}$ une suite finie de sous-groupes distingués d'un groupe G. Pour que G soit produit direct des H_i il faut et il suffit que $G = H_1 H_2 .. H_n$, et que, pour tout indice k tel que $1 \leqslant k \leqslant n-1$, $(H_1 H_2 .. H_k) \cap H_{k+1} = \{e\}$.

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

12) Soit (G_α) une famille de sous-groupes distingués d'un groupe G, telle que $\bigcap_\alpha G_\alpha = \{e\}$; montrer que G est isomorphe à un sous-groupe du groupe produit $\prod_\alpha (G/G_\alpha)$.

13) Soit H un sous-groupe distingué d'un groupe G. Pour que G soit isomorphe au produit $H \times (G/H)$, il faut et il suffit qu'il existe une représentation f de G sur H telle que $f(x)=x$ pour tout $x \in H$.

14) Soit G un groupe abélien, H un sous-groupe de G tel que G/H soit un groupe monogène infini. Montrer que G est isomorphe au groupe produit $H \times (G/H)$.

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

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

17) Soit A une partie non vide quelconque d'un groupe G ; on appelle <u>normalisateur</u> de A l'ensemble N des $x \in G$ tels que $xAx^{-1} = A$;

on appelle centralisateur de A l'ensemble K des $x \in G$ tels que $xax^{-1}=a$ quel que soit $a \in A$. Montrer que N est un sous-groupe de G , et K un sous-groupe distingué de N . Si A est un sous-groupe de G , le normalisateur N de A est le plus grand des sous-groupes H de G tels que A soit sous-groupe distingué de H .

18) On appelle groupe des commutateurs, ou groupe dérivé d'un groupe G, le sous-groupe C de G engendré par les commutateurs $x \circ y$ de tous les couples d'éléments de G (§ 2, exerc.8). Montrer que C est un sous-groupe distingué, stable pour tous les endomorphismes de G ; le groupe quotient G/C est abélien, et C est le plus petit des sous-groupes distingués K de G tels que G/K soit abélien.

On pose $C=D(G)$, et on définit par récurrence le $k^{ème}$ groupe dérivé $D^k(G)$ comme égal à $D(D^{k-1}(G))$; montrer que $D^k(G)$ est un sous-groupe distingué de G , stable pour tous les endomorphismes de G . Si H est un sous-groupe de G , $D^k(H) \subset D^k(G)$; si H est distingué, on a $D^k(G/H)=(D^k(G)).H/H$.

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

20) On dit que les sous-groupes stables appartenant à un ensemble $\mathscr{E}$ de sous-groupes stables d'un groupe à opérateurs G satisfont à la condition minimale (resp. condition maximale) si tout ensemble de sous-groupes stables de G contenu dans $\mathscr{E}$, ordonné par inclusion, possède un élément minimal (resp. maximal).

a) On suppose que les sous-groupes stables de G satisfont à la condition minimale, et on appelle sous-groupes distingués minimaux de G les éléments minimaux de l'ensemble des sous-groupes stables distingués de G non réduits à e . Soit S le plus petit sous-groupe de G contenant un ensemble $\mathcal{F}$ de sous-groupes distingués minimaux de G ; montrer que S est le produit direct d'un nombre fini de sous-groupes minimaux distingués de G (soit (M_n) une suite de sous-groupes distingués minimaux de G appartenant à $\mathcal{F}$, et telle que M_{n+1} ne soit pas contenu dans le sous-groupe stable engendré par $M_1, M_2, \ldots, M_n$; soit S_k le sous-groupe stable engendré par les M_n d'indice $n \geqslant k$; montrer qu'on a $S_{k+1}=S_k$ à partir d'un certain rang, et par suite que (M_n) est une suite finie ; utiliser enfin l'exerc. 10).

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

c) Montrer (dans les mêmes hypothèses) qu'il n'existe aucun sous-groupe stable de G isomorphe à G et distinct de G (raisonner par l'absurde en prouvant que l'hypothèse entraînerait l'existence d'une suite infinie strictement décroissante de sous-groupes stables de G).

21) Si les sous-groupes stables d'un groupe à opérateurs G satisfont aux conditions maximale et minimale, G possède une suite de Jordan-Hölder (remarquer que, si H est un sous-groupe stable de G , l'ensemble des sous-groupes stables distingués de H , distincts de H , possède un élément maximal).

22) Soit G un groupe à opérateurs ; on dit qu'une suite de composition (G_i) de G est <u>distinguée</u> si tous les G_i sont des sous-groupes stables distingués <u>de</u> G ; une suite distinguée est dite <u>principale</u> si elle est strictement décroissante et s'il n'existe aucune suite distinguée strictement plus fine.

a) Si <u>X</u> (G_i) et (H_j) sont deux suites distinguées de G , montrer qu'il existe une suite distinguée plus fine que (G_i) et (H_j) (appliquer convenablement le th. de Schreier-Zassenhaus). Donner une seconde démonstration de cette proposition, en considérant les sous-groupes $G_{ij} = G_i \cap (G_{i+1}.H_j)$ et $H_{ji} = H_j \cap (H_{j+1}.G_i)$.

b) Si les sous-groupes stables distingués de G satisfont aux conditions maximale et minimale, pour tout sous-groupe stable distingué H de G , il existe une suite principale (G_i) de G telle que $H = G_i$ pour un indice i ; deux suites principales <u>X</u> (G_i) et (H_j) de G sont isomorphes à l'ordre près. Réciproquement, si G possède une suite principale, les sous-groupes stables distingués de G satisfont aux conditions maximale et minimale (utiliser a)).

c) Si G possède une suite principale (G_i) et si les sous-groupes stables de G satisfont à la condition minimale, tout groupe quotient G_i/G_{i+1} est produit direct d'un nombre fini de sous-groupes stables simples et isomorphes entre eux (utiliser l'exerc. 20).

23) Soit (H_ι) une famille quelconque de sous-groupes d'un groupe G ; on dit que G est <u>produit direct</u> de cette famille de sous-groupes si : 1° pour $\iota \neq \varkappa$, tout élément de H_ι est permutable avec tout élément de $H_\varkappa$; 2° pour tout $x \in G$, il existe, pour chaque ι , un élément $x_\iota \in H_\iota$ et un seul, tel que $x_\iota \neq e$ pour un nombre fini d'indices seulement, et que, si $\iota_1, \iota_2, \ldots, \iota_n$ sont les indices ι tels que $x_\iota \neq e$,

on ait $x=x_{\iota_1}x_{\iota_2}\dots x_{\iota_n}$. On dit que G est <u>complètement réductible</u> s'il est produit direct d'une famille de sous-groupes <u>simples</u>.

a) Montrer que, si G est produit direct de la famille de sous-groupes (H_ι), il est isomorphe à un sous-groupe du groupe produit $H = \prod_\iota H_\iota$, distinct de H si la famille (H_ι) est infinie ; en déduire que les H_ι sont des sous-groupes distingués de G .

b) Etendre aux produits directs infinis et aux groupes complétement réductibles les propositions.

c) Soit G un groupe tel qu'il soit engendré par la réunion d'une famille $(H_\iota)_{\iota\in I}$ de sous-groupes distingués simples de G . Montrer qu'il existe une sous-famille $(H_\iota)_{\iota\in J}$ telle que G soit produit direct de cette famille (montrer à l'aide du th. de Zorn, qu'il existe une partie maximale J de I telle que le sous-groupe engendré par la réunion de la famille $(H_\iota)_{\iota\in J}$ soit le produit direct de cette famille ; prouver ensuite, à l'aide de l'exerc.9, que ce sous-groupe est identique à G).

24) Soit L le système associatif libre (§ 1) engendré par deux familles (x_ι), (y_ι) ayant le même ensemble d'indices ; le système quotient de L obtenu en assujettissant les éléments x_ι, y_ι aux relations $x_\iota y_\iota = y_\iota x_\iota = e$ quel que soit ι (§ , exerc.), est un groupe, dit <u>groupe libre</u> engendré par la famille (x_ι) ; si $(u_\varkappa)$ est une autre famille d'éléments de L et qu'on assujettisse en outre les x_ι et y_ι à satisfaire aux relations $u_\varkappa = e$ pour tout $\varkappa$, le système quotient de L correspondant est encore un groupe, isomorphe à un groupe quotient du groupe libre engendré par les x_ι , et qu'on dit <u>défini par les relations</u> $u_\varkappa = e$ <u>entre les générateurs</u> x_ι . Tout élément x du groupe libre engendré par une famille (x_ι) peut se mettre d'une mnière

et d'une seule sous la forme $x_{\iota_1}^{\varepsilon_1} x_{\iota_2}^{\varepsilon_2} \ldots x_{\iota_n}^{\varepsilon_n}$, où les ε_i sont égaux à ± 1 , et où $\varepsilon_i = \varepsilon_{i+1}$ si $\iota_i = \iota_{i+1}$.

Si un groupe G est engendré par une famille (x_ι) d'éléments distincts de G , il est isomorphe à un groupe quotient du groupe libre engendré par cette famille ; on dit que G est un groupe libre s'il existe une famille (x_ι) d'éléments distincts engendrant G et telle que G soit isomorphe au groupe libre engendré par cette famille.

25) a) Soit (x_ι) une famille d'éléments engendrant un groupe G ; soient L le groupe libre engendré par (x_ι) , et φ l'application canonique de L sur G . S'il existe une représentation f de G dans L , telle que $x = \varphi(f(x))$ quel que soit $x \in G$, montrer que G est défini par les relations $x_\iota = \varphi(f(x_\iota))$ entre les générateurs x_ι (montrer que toute relation entre les x_ι est une conséquence de ces dernières).

b) Soit G le groupe libre, engendré par la famille (x_ι), et soit H un sous-groupe de G . S'il existe une application g de G dans G , telle que $g(g(x))=g(x)$, $g(e)=e$, et que les relations $g(x)=g(y)$ et $xy^{-1} \in H$ soient équivalentes, l'ensemble des $g(x)$ est dit un système de représentants des classes à droite suivant H . Montrer qu'il existe un tel système de représentants R tel que, si $x_{\iota_1}^{\varepsilon_1} x_{\iota_2}^{\varepsilon_2} \ldots x_{\iota_n}^{\varepsilon_n}$ appartient à R , chacun des éléments $x_{\iota_1}^{\varepsilon_1} x_{\iota_2}^{\varepsilon_2} \ldots x_{\iota_m}^{\varepsilon_m}$ appartient à R pour $1 \leqslant m \leqslant n$ (considérer un système maximal R_o de représentants de classes à droite suivant H , ayant la propriété précédente, et prouver que tout élément de G appartient à une classe à droite dont un représentant appartient à R_o).

c) Si R est un système de représentants des classes à droite suivant H , défini par l'application g , montrer que l'ensemble des éléments $zx_\iota(g(zx_\iota))^{-1}$, où z parcourt R , engendre le sous-groupe H

(si $x_{\iota_1}^{\varepsilon_1}x_{\iota_2}^{\varepsilon_2}\dots x_{\iota_n}^{\varepsilon_n}\in H$, montrer qu'on peut le mettre sous la forme d'un composé d'éléments de la forme $zx_\iota(g(zx_\iota))^{-1}$ en prenant pour les z les images par g des éléments $x_{\iota_1}^{\varepsilon_1}x_{\iota_2}^{\varepsilon_2}\dots x_{\iota_m}^{\varepsilon_m}$, où $1\leqslant m\leqslant n$).

d) Déduire de ce qui précède que H est un groupe libre (l'application de H sur le groupe libre engendré par les éléments $u_{z,\iota}=zx_\iota(g(zx_\iota))^{-1}$, définie dans c) est une représentation f satisfaisant aux conditions de a) ; en prenant pour R un système de représentants satisfaisant à la condition énoncée dans b), montrer que f est un isomorphisme).

26) Soit Q le groupe engendré par trois éléments a,b,c satisfaisant aux relations $a^2=b^2=(ab)^2=c$, $c^2=e$. Montrer que Q est un groupe non commutatif d'ordre 8 ("groupe quaternionique"), que tout sous-groupe de Q est distingué, et que tout sous-groupe de Q distinct de $\{e\}$ contient c .

27) Soit E un ensemble, et f une application de E^m dans E ; on écrira $f(x_1,x_2,\dots,x_m)=x_1x_2\dots x_m$; on suppose que f satisfait aux conditions suivantes :

1° on a identiquement

$$(x_1x_2\dots x_m)x_{m+1}\dots x_{2m-1}=x_1(x_2x_3\dots x_{m+1})x_{m+2}\dots x_{2m-1}\ ;$$

2° quels que soient $a_1,a_2,\dots,a_{m-1}$, les applications

$$x\longrightarrow xa_1a_2\dots a_{m-1}$$

$$x\longrightarrow a_1a_2\dots a_ixa_{i+1}\dots a_{m-1}\qquad(1\leqslant i\leqslant m-2)$$

$$x\longrightarrow a_1a_2\dots a_{m-1}x$$

sont des applications biunivoques de E sur E .

a) Montrer qu'on a identiquement

$$(x_1x_2\dots x_m)x_{m+1}\dots x_{2m-1}=x_1x_2\dots x_i(x_{i+1}\dots x_{i+m})x_{i+m+1}\dots x_{2m-1}$$

pour tout indice i tel que $1\leqslant i\leqslant m-1$ (raisonner par récurrence sur i , en considérant l'élément

$$((x_1x_2\dots x_m)x_{m+1}\dots x_{2m-1})a_1a_2\dots a_{m-1}\ .)$$

b) Quels que soient $a_1, a_2, \ldots, a_{m-2}$, il existe $u \in E$ tel que l'on ait identiquement en x

$$x = xa_1a_2..a_{m-2}u = ua_1a_2...a_{m-2}x$$

(raisonner comme dans la prop. du § 2).

c) Dans l'ensemble E^k des suites $(u_1, u_2, \ldots, u_k)$ de k éléments de E $(1 < k < m)$ on considère la relation R_k : quels que soient $x_1, x_2, .., x_{m-k}$, $u_1u_2..u_kx_1x_2..x_{m-k} = v_1v_2..v_kx_1..x_{m-k}$; on désigne par E_k l'ensemble quotient E^k/R_k, par G l'ensemble somme de $E_1=E, E_2, E_3, .., E_{m-1}$. Soient $\alpha_i \in E_i$, $\beta_j \in E_j$; si $(u_1, u_2, ..u_i)$ est une suite de la classe α_i, $(v_1, \ldots, v_j)$ une suite de la classe β_j, on considère la suite $(u_1, u_2, .., u_i, v_1, v_2, .., v_j)$ si $i+j \leqslant m$, la suite $(u_1, u_2, .., u_{i+j-m}, (u_{i+j-m+1}..u_iv_1v_2..v_j))$ si $i+j > m$; montrer que la classe de cette suite dans E_{i+j} (resp. $E_{i+j-m+1}$) ne dépend que de α_i et β_j ; on la désigne par $\alpha_i.\beta_j$. Montrer qu'on définit ainsi dans G une loi de composition interne pour laquelle G est un groupe. Montrer que $H=E_{m-1}$ est un sous-groupe distingué de G, que le groupe quotient G/H est cyclique d'ordre m-1, et que E est identique à une classe (mod.H) engendrant le groupe G/H.

§ 5. Groupes de transformations

1. Groupes de transformations d'un ensemble E. Comme nous l'avons déjà signalé (§ 4, n°1), l'ensemble des applications biunivoques d'un ensemble E sur lui-même forme un groupe pour la loi de composition $f \circ g$; on désigne ce groupe par la notation $\mathfrak{S}_E$ et on l'appelle groupe symétrique de E. Si E et E' sont deux ensembles équipotents, et φ une application biunivoque de E sur E', Ψ l'application réciproque de φ, il est immédiat que l'application $f \to \varphi \circ f \circ \Psi$ est un isomorphisme du groupe symétrique $\mathfrak{S}_E$ sur le groupe symétrique $\mathfrak{S}_{E'}$.

Lorsque E est l'intervalle $[1,n]$ de l'ensemble $\mathcal{N}$ des entiers naturels, le groupe symétrique $\mathfrak{S}_E$ se note $\mathfrak{S}_n$; c'est un groupe fini d'ordre n! ; le groupe symétrique d'un ensemble quelconque de n éléments est isomorphe à $\mathfrak{S}_n$.

<u>Définition 1</u>. <u>Tout sous-groupe du groupe symétrique $\mathfrak{S}_E$ est appelé groupe de permutations, ou groupe de transformations, de l'ensemble E</u> .

On réserve le plus souvent le nom de groupe de permutations au cas où E est <u>fini</u> : tout groupe de permutations de E est alors un groupe <u>fini</u>. On dit qu'un sous-groupe de $\mathfrak{S}_n$ est un groupe de permutations de <u>degré</u> n .

<u>Exemples</u>. 1) <u>Groupe alterné</u>. Etant donnée une permutation $\pi \in \mathfrak{S}_n$, considérons le produit d'entiers naturels $V_n = \prod_{1 \leqslant i < j \leqslant n} (j-i)$, et formons le produit $\pi(V_n) = \prod_{1 \leqslant i < j \leqslant n} (\pi(j)-\pi(i))$; on a $\pi(V_n) = \varepsilon_\pi . V_n$, où ε_π est égal à $+1$ ou -1 . En effet, soit (h,k) un couple d'entiers naturels tels que $1 \leqslant h < k \leqslant n$; si $\pi^{-1}(h) < \pi^{-1}(k)$, on a $k-h = \pi(j)-\pi(i)$, en posant $i = \pi^{-1}(h)$, $j = \pi^{-1}(k)$; si au contraire $\pi^{-1}(h) > \pi^{-1}(k)$, on a $k-h = -(\pi(j)-\pi(i))$ en posant $i = \pi^{-1}(k)$, $j = \pi^{-1}(h)$; on a donc $\varepsilon_\pi = (-1)^\nu$, où ν est le nombre de couples (i,j) tels que $1 \leqslant i < j \leqslant n$ et $\pi(i) > \pi(j)$ (nombre qu'on appelle <u>nombre d'inversions</u> de π).

Le nombre ε_π est appelé la <u>signature</u> de la permutation π ; π est dite <u>paire</u> (resp. <u>impaire</u>) si $\varepsilon_\pi = +1$ (resp. $\varepsilon_\pi = -1$). La permutation identique ω (élément neutre de $\mathfrak{S}_n$) est paire. On appelle <u>transposition</u> de deux nombres i,j tels que $1 \leqslant i < j \leqslant n$, la permutation $\tau \in \mathfrak{S}_n$ telle que $\tau(i)=j$, $\tau(j)=i$, $\tau(h)=h$ pour h distinct de i et j . Une transposition est <u>impaire</u> ;

en effet, pour $1 \leqslant h < k \leqslant n$, on ne peut avoir $\tau(k) - \tau(h) = -(k-h)$ que pour les valeurs suivantes de h et k : 1° h=i, k=j ; 2° h=i , i<k<j ; 3° i<h<j , k=j ; le nombre d'inversions de τ est donc le nombre impair $2(j-i-1)+1$.

Si π, ρ sont deux permutations de $\mathfrak{S}_n$, et $\sigma = \pi\rho$, on a $\sigma(V_n) = \varepsilon_\rho . \pi(V_n) = \varepsilon_\pi . \varepsilon_\rho . V_n$, d'où la relation

(1) $$\varepsilon_{\pi\rho} = \varepsilon_\pi \varepsilon_\rho$$

qui prouve que l'application $\pi \longrightarrow \varepsilon_\pi$ est une <u>représentation</u> de $\mathfrak{S}_n$ <u>sur</u> le groupe multiplicatif formé des deux nombres +1 , -1 . L'ensemble des permutations <u>paires</u> de $\mathfrak{S}_n$ est l'image réciproque de +1 par cette représentation ; c'est donc un sous-groupe distingué d'indice 2 (et par suite d'ordre $\frac{n!}{2}$) de $\mathfrak{S}_n$, qu'on appelle <u>groupe alterné</u> de degré n , et qu'on désigne par la notation $\mathfrak{A}_n$.

2) <u>Groupes des translations d'un groupe</u>. Si G est un groupe les <u>translations à gauche</u> γ_x (§ 2, n°) sont des permutations de G § 2, prop.3) ; l'ensemble Γ de ces translations est un <u>sous-groupe</u> de $\mathfrak{S}_G$, isomorphe à G . En effet, l'application $x \longrightarrow \gamma_x$ de G sur Γ est biunivoque, car la relation $\gamma_x = \gamma_y$ entraîne $xe = ye$, donc $x=y$; en outre, cette application est une <u>représentation</u>, d'après la prop.1 du § 2.

On montre de même que l'ensemble Δ des translations à droite de G est un sous-groupe de $\mathfrak{S}_G$, isomorphe au groupe opposé à G , donc isomorphe à G .

Soit φ un isomorphisme d'un groupe G dans le groupe symétrique $\mathfrak{S}_E$ d'un ensemble E ; on dit que l'image $\varphi(G)$ est une <u>réalisation du groupe G comme groupe de transformations</u>.

Le groupe Γ des translations à gauche et le groupe Δ des translations à droite d'un groupe quelconque G sont donc des réalisations de G comme groupe de transformations.

2. Extensions d'un groupe de transformations. Soit M un ensemble d'une échelle d'ensembles (Ens.R, § 8) ayant pour base, par exemple, trois ensembles E,F,G . Si f,g,h sont trois permutations de E,F,G respectivement, on sait définir de proche en proche dans l'échelle, une permutation de M appelée extension de f,g,h à M , et que nous désignerons par $\varphi_M(f,g,h)$. Rappelons brièvement comment on procède ; deux cas sont à distinguer :

1° on a $M = \mathfrak{P}(L)$, où L est un ensemble de l'échelle pour lequel $\varphi_L(f,g,h)$ a été déjà définie ; alors $\varphi_M(f,g,h)$ n'est autre que l'extension de $\varphi_L(f,g,h)$ aux ensembles des parties (Ens.R, § 2, n°9) ;

2° on a $M = P \times Q$, où P et Q sont des ensembles de l'échelle pour lesquels $\varphi_P(f,g,h)$ et $\varphi_Q(f,g,h)$ ont été définis ; alors $\varphi_M(f,g,h)$ est l'extension $(\varphi_P(f,g,h), \varphi_Q(f,g,h)$ de $\varphi_P(f,g,h)$ et $\varphi_Q(f,g,h)$ aux ensembles produits (Ens.R, § 3, n°14).

Si f',g',h' sont trois autres permutations de E,F,G respectivement, il résulte aussitôt de la définition précédente, qu'on a $\varphi_M(f\circ f', g\circ g', h\circ h') = \varphi_M(f,g,h)\circ\varphi_M(f',g',h')$; autrement dit, φ_M est une représentation du groupe produit $\mathfrak{S}_E \times \mathfrak{S}_F \times \mathfrak{S}_G$ dans le groupe $\mathfrak{S}_M$.

Considérons maintenant F et G comme des ensembles auxiliaires, et prenons pour g (resp. h) la permutation identique u (resp. v) de F (resp.G). Alors, si l'ensemble M n'appartient pas à l'échelle ayant pour base les seuls ensembles F et G , l'application $f \to \varphi_M(f,u,v)$ est un isomorphisme du groupe symétrique $\mathfrak{S}_E$ dans le groupe symétrique $\mathfrak{S}_M$. En effet, si $M = \mathfrak{P}(L)$, L n'appartient pas à

l'échelle ayant pour base F et G ; si $M=P\times Q$, l'un au moins des ensembles P,Q n'appartient pas à cette échelle ; de proche en proche, on est donc ramené à vérifier la proposition pour les cas où M est un des ensembles $\mathfrak{P}(E)$, $E\times E$, $E\times F$, $E\times G$; or, si on a $M=\mathfrak{P}(E)$, $\varphi_M(f)$ est l'application $X\to f(X)$, et la relation "quel que soit $X\subset E$, $f(X)=f'(X)$ " entraîne $f=f'$; la vérification du fait que φ_M est biunivoque se fait aussi aisément dans les autres cas.

Nous dirons que l'isomorphisme ainsi défini est l'isomorphisme canonique du groupe symétrique $\mathfrak{S}_E$ dans le groupe symétrique $\mathfrak{S}_M$.

Définition 2. Soit M un ensemble de l'échelle construite à partir d'un ensemble E et de deux ensembles auxiliaires F et G ,(M n'appartenant pas à l'échelle d'ensembles ayant pour base F et G) ; si Γ est un groupe de transformations de E , on appelle extension de Γ à l'ensemble M , l'image de Γ par l'isomorphisme canonique du groupe symétrique $\mathfrak{S}_E$ dans le groupe symétrique $\mathfrak{S}_M$.

3. Invariants d'un groupe de transformations. Groupes d'automorphismes. Soit Γ un groupe de transformations d'un ensemble E , et soit M un ensemble de l'échelle ayant pour base E et (par exemple) deux ensembles auxiliaires F,G ; comme ci-dessus, on suppose que M n'appartient pas à l'échelle ayant pour base F et G seuls.

Définition 3. On dit qu'un élément $s\in M$ est un invariant du groupe Γ (ou que Γ laisse invariant s) si s est invariant par toutes les applications appartenant à l'extension Γ_M du groupe Γ à l'ensemble M .

On notera que, grâce à cette définition, on peut ramener la considération de plusieurs invariants d'un groupe (appartenant à un même ensemble de l'échelle ou à des ensembles différents),

à celle d'<u>un seul</u> invariant du groupe appartenant à un autre ensemble (convenablement formé) de l'échelle ; de même, la considération d'une <u>famille</u> $(s_\iota)_{\iota \in I}$ d'invariants de Γ , appartenant à un ensemble M de l'échelle, se ramène à envisager l'invariant formé de l'ensemble représentatif de l'application $\iota \longrightarrow s_\iota$, qui est un élément de $\mathfrak{P}(I \times M)$ (on considère alors I comme un ensemble auxiliaire).

Il faut se garder, par contre, de confondre un <u>ensemble d'invariants</u> appartenant à un même ensemble M , et une <u>partie de M invariante par</u> Γ (qui est un élément de $\mathfrak{P}(M)$ invariant par Γ).

Etant donné un groupe de transformations Γ d'un ensemble E , la détermination de tous les invariants de Γ appartenant à un ensemble donné M de l'échelle des ensembles ayant pour base E (et éventuellement un certain nombre d'ensembles auxiliaires) constitue le problème fondamental de la <u>théorie des invariants</u> du groupe Γ . Mais inversement, un groupe de transformations Γ de E est <u>bien déterminé</u> par la condition d'avoir des invariants donnés dans un ensemble M de l'échelle ; de façon précise :

<u>Proposition 1</u>. <u>Soit A une partie d'un ensemble M de l'échelle des ensembles ayant pour base un ensemble donné E (ainsi qu'un certain nombre d'ensembles auxiliaires)</u>. <u>L'ensemble des permutations</u> $f \in \mathfrak{S}_E$ <u>telles que tout élément</u> $s \in A$ <u>soit invariant par l'extension</u> $\varphi_M(f)$ <u>de f à</u> M , <u>est un sous-groupe de</u> $\mathfrak{S}_E$.

En effet, si s est invariant par $\varphi_M(f)$ et $\varphi_M(g)$, il est aussi invariant par $\varphi_M(f \circ g) = \varphi_M(f) \circ \varphi_M(g)$; et, si h est l'application réciproque de f , s est invariant par $\varphi_M(h)$, application réciproque de $\varphi_M(f)$.

On dit que le sous-groupe de $\mathfrak{S}_E$ ainsi défini est déterminé par la condition de laisser invariants les éléments de A .

L'ensemble des invariants de ce sous-groupe appartenant à M contient évidemment l'ensemble A , mais peut aussi contenir des éléments de M n'appartenant pas à A .

Considérons en particulier une structure σ donnée sur un ensemble E (Ens.R, §8) : c'est un élément d'un ensemble M de l'échelle des ensembles ayant pour base E et les ensembles auxiliaires qui interviennent dans la structure. Les permutations f de E telles que σ soit invariant par l'extension $\varphi_M(f)$ sont, par définition (Ens. R, §8, n°5) les automorphismes de la structure σ ; donc :

Proposition 2. Les automorphismes d'une structure donnée σ sur un ensemble E forment un groupe de transformations de E (qu'on appelle groupe d'automorphismes de la structure σ).

Soit σ' une structure isomorphe à σ , définie sur un ensemble E' , φ un isomorphisme de σ sur σ' , ψ l'isomorphisme réciproque ; il est immédiat que l'application $f \to \varphi \circ f \circ \psi$ est un isomorphisme du groupe d'automorphismes de σ sur le groupe d'automorphismes de σ' .

Exemple. Groupe d'automorphismes d'un groupe. Etant donné un groupe G , les automorphismes de G forment, d'après la prop.2, un sous-groupe Γ du groupe symétrique $\mathfrak{S}_G$. Les automorphismes intérieurs a_x définis au §4 (n°) forment un sous-groupe Δ de Γ ; en effet, on vérifie immédiatement l'identité $a_x \circ a_y = a_{xy}$. Cette relation montre en outre que l'application $x \to a_x$ est une représentation de G sur Δ ; pour que a_x soit l'application identique de G sur lui-même, il faut et il suffit que $xyx^{-1}=y$ quel que soit $y \in G$, c'est-à-dire $xy=yx$; autrement dit, x doit être permutable avec tous les éléments de G , donc appartenir au centre Z de G ; ceci montre à nouveau, d'après le th.3 du §4 ,

que Z est un sous-groupe distingué de G , et on voit de plus que le groupe Δ des automorphismes intérieurs de G est isomorphe au au groupe quotient G/Z .

On notera que le groupe Δ peut être identique à Γ ; il peut aussi se réduire à l'application identique : il faut et il suffit pour cela que Z=G , donc que G soit abélien. Les automorphismes de G qui ne sont pas des automorphismes intérieurs sont parfois appelés automorphismes extérieurs de G .

Lorsque G est muni d'une structure de groupe à opérateurs les automorphismes de cette structure forment un groupe Γ' qui est évidemment un sous-groupe du groupe Γ des automorphismes de la structure de groupe de G ; on notera qu'en général le groupe Δ des automorphismes intérieurs n'est pas un sous-groupe de Γ'.

4. Groupes transitifs. Soit Γ un groupe de transformations d'un ensemble E . La relation "il existe $f \in \Gamma$ tel que $y=f(x)$" est une relation d'équivalence dans E ; en effet, elle est réfléxive, car la permutation identique u appartient à Γ , et on a $x=u(x)$; elle est symétrique, car si $f \in \Gamma$ est telle que $y=f(x)$ son application réciproque g appartient à Γ , et $x=g(y)$; enfin, elle est transitive, car de $y=f(x)$, $z=g(y)$, on tire $z=g(f(x))$, et si f et g appartiennent à Γ , il en est de même de $g \circ f$.

Les classes suivant la relation d'équivalence précédente sont appelées classes d'intransitivité du groupe Γ ; s'il n'existe qu'une seule classe d'intransitivité (identique à E), on dit que Γ est un groupe transitif ; dans le cas contraire, Γ est dit intransitif. La condition pour que Γ soit transitif peut encore s'exprimer de la façon suivante : étant donné un élément $a \in E$, pour tout $x \in E$, il existe $f \in \Gamma$ telle que $x=f(a)$.

Exemples. 1) Le groupe des translations à gauche d'un groupe G est transitif, car si e est l'élément neutre de G , on a $\gamma_x(e)=x$; de même, le groupe des translations à droite est transitif.

2) Le groupe Δ des automorphismes intérieurs d'un groupe G (ayant plus d'un élément) est intransitif, car $\alpha_x(e)=e$ quel que soit $x \in G$; les éléments d'une même classe d'intransitivité de Δ sont appelés éléments conjugués dans G ; chacun des éléments du centre de G forme à lui seul une classe d'intransitivité de Δ .

3) Si Γ est un groupe de transformations intransitif dans un ensemble E , et A une classe d'intransitivité de E , les restrictions à A des permutations de Γ constituent un groupe transitif de transformations de A .

5. Espaces homogènes. La donnée d'un groupe de transformations Γ d'un ensemble E définit sur E une loi de composition externe $(\sigma,x) \longrightarrow \sigma(x)$ entre opérateurs $\sigma \in \Gamma$, et éléments $x \in E$ (§ 3, n°). Il est immédiat que cette loi est associative (§ 3, n°) par rapport à la loi de composition (interne) du groupe Γ .

Réciproquement, supposons donnée, sur un ensemble E , une loi de composition externe, notée multiplicativement à gauche, dont le domaine d'opérateurs G soit un groupe pour une loi interne (notée aussi multiplicativement) ; supposons que la loi externe soit associative par rapport à la loi interne de G (c'est-à-dire qu'on a identiquement $(\alpha\,\beta)x = \alpha(\beta x)$ pour $\alpha \in G$, $\beta \in G$, $x \in E$); enfin, supposons que l'application $x \longrightarrow \alpha x$ de E dans lui-même, que nous désignerons par f_α , soit une permutation de E pour tout $\alpha \in G$.

Alors l'application $\alpha \to f_\alpha$ est une <u>représentation</u> du groupe G dans le groupe symétrique $\mathfrak{S}_E$; si Γ est l'image de G par cette représentation, Γ est un groupe de transformations de E , isomorphe au groupe quotient G/K , où K est le sous-groupe distingué de G formé des α tels que f_α soit la permutation identique de E (autrement dit, tels que $\alpha x = x$ pour tout $x \in E$).

<u>Définition 4</u>. <u>On appelle espace homogène un ensemble E muni d'une loi de composition externe</u> $(\alpha,x) \to \alpha x$ <u>dont le domaine d'opérateurs est un groupe</u> G , <u>et qui satisfait aux conditionss suivantes</u> :

a) <u>quels que soient</u> α , β <u>dans</u> G , <u>et</u> $x \in E$, $(\alpha\beta)x = \alpha(\beta x)$ (<u>associativité</u> de la loi externe par rapport à la loi du groupe G) ;

b) <u>pour tout</u> $\alpha \in G$, <u>l'application</u> $x \to \alpha x$ <u>est une permutation de</u> E

c) <u>quels que soient x et y dans</u> E , <u>il existe</u> $\alpha \in G$ <u>tel que</u> $y = \alpha x$.

Avec les notations précédentes, la condition c) de la définition 1 exprime que le groupe de transformations Γ formé des f_α est <u>transitif</u>.

Soit a un élément de l'espace homogène E , et considérons l'ensemble H_x des $\alpha \in G$ tels que $x=\alpha a$; cet ensemble n'est pas vide par hypothèse, et si α et β en sont deux éléments, on a $\beta^{-1}(\alpha a)=a$, c'est-à-dire $\beta^{-1}\alpha \in H_a$, et réciproquement, si $\alpha \in H_x$, $\gamma \in H_a$, on a $\alpha\gamma \in H_x$. Si on prend en particulier $x=a$, on en déduit que $H=H_a$ est un <u>sous-groupe</u> de G ; et pour un x quelconque dans E , H_x est une <u>classe à gauche</u> $\alpha.H$ suivant le sous-groupe H . A tout élément $x \in E$ correspond donc une telle classe à gauche H_x ; réciproquement, si $\alpha.H$ est une classe à gauche suivant H , il existe un x et un seul tel que $H_x = \alpha.H$, à savoir l'élément $x = \alpha a$.

Nous avons donc défini une application biunivoque $x \to H_x$ de E <u>sur</u> l'ensemble des classes à gauche de G suivant le sous-groupe H ,

c'est-à-dire l'ensemble quotient de G par la relation d'équivalence $\beta^{-1}\alpha \in H$. Nous désignerons cet ensemble quotient par G/H ; on peut y transporter par l'application biunivoque $x \longrightarrow H_x$ la structure d'espace homogène de E : la loi de composition externe dans l'espace homogène G/H fait correspondre à l'opérateur $\alpha \in G$, et à l'élément $u=\beta.H \in G/H$, l'élément $\alpha.u=(\alpha\beta).H$ de G/H .

Inversement, étant donné un groupe G et un sous-groupe quelconque H de G , la loi de composition externe précédente définit sur G/H une structure d'espace homogène ayant G pour domaine d'opérateurs ; en effet, la condition a) de la déf.4 est trivialement vérifiée ; l'application $u \longrightarrow \alpha.u$ est une permutation de G/H , car si $v=\beta.H$, l'élément $u=(\alpha^{-1}\beta).H$ est l'unique élément de G/H tel que $v=\alpha.u$; enfin, si $w=\beta.H$ et $v=\gamma.H$ sont deux éléments de G/H , on a $w=(\gamma\beta^{-1}).v$, ce qui démontre que la condition c) est vérifiée. L'ensemble G/H , muni de la structure d'espace homogène ainsi définie, est appelé l'espace homogène défini par le sous-groupe H du groupe G ; et on peut énoncer la proposition suivante :

Proposition 3. Soit E un espace homogène, G le groupe d'opérateurs de E ; si $H=H_a$ est le sous-groupe de G formé des opérateurs α tels que $\alpha a=a$ (a élément quelconque de E), l'espace homogène E est isomorphe à l'espace homogène G/H , défini par le sous-groupe H de G .

Si b est un autre élément de E , E est aussi isomorphe à l'espace homogène G/H_b ; d'ailleurs, si β est un élément de G tel que $b=\beta a$, les relations $\alpha b=b$ et $\beta^{-1}\alpha\beta a = a$ sont équivalentes, donc $H_b=\beta H_a \beta^{-1}$. L'intersection K de tous les sous-groupes H_b , lorsque b parcourt E , est le sous-groupe distingué K de G formé des α tels que $\alpha x=x$ pour tout $x \in E$; on a vu plus haut que le sous-groupe

de $\mathfrak{S}_E$ formé des permutations f_a est isomorphe au groupe quotient G/K . En particulier, ce sous-groupe sera isomorphe à G lui-même si H est un sous-groupe ne contenant aucun sous-groupe distingué de G autre que $\{e\}$.

Groupes primitifs. Soit G/H un espace homogène défini par un sous-groupe H d'un groupe G ; cherchons les relations d'équivalence compatibles avec la loi externe de cet espace. Soit R une telle relation ; considérons d'abord l'ensemble des éléments $u=a.H$ de G/H tels que $u \equiv H \pmod{R}$; il est immédiat que l'ensemble des $a \in G$ tels que $u=aH$ ait cette propriété est un sous-groupe K de G : en effet, si $aH \equiv H$, on a $a^{-1}(aH) \equiv a^{-1}H$, donc $a^{-1}H \equiv H \pmod{R}$; et si $aH \equiv H$, $\beta H \equiv H$, on a $a(\beta H) \equiv aH \equiv H \pmod{R}$. Le sous-groupe K contient évidemment H ; montrons que les classes d'équivalence suivant R dans G/H sont les images canoniques des classes à gauche (mod.K) dans G ; en effet, l'ensemble des classes $v=\beta H$ telles que $v \equiv u = aH \pmod{R}$ s'obtient en prenant pour β tous les éléments de G tels que $a^{-1}\beta H \equiv H \pmod{R}$, c'est-à-dire les éléments de la classe $a.K$. L'ensemble quotient de G/H par la relation R est donc en correspondance biunivoque avec l'espace homogène G/K ; en outre, à un opérateur $\gamma \in G$ et à la classe (mod.R) de $u=aH$ correspond, par la loi quotient de la loi externe sur G/H , la classe (mod.R) de $\gamma.u = \gamma aH$; on en conclut que :

Proposition 4. Toute structure quotient d'un espace homogène G/H défini par un sous-groupe H d'un groupe G , est isomorphe à celle d'un espace homogène G/K , où K est un sous-groupe de G contenant H .

Réciproquement, il est immédiat que si K est un sous-groupe de G contenant H , et si on désigne par R (resp.S) la relation d'équivalence

$\alpha^{-1}\beta \in H$ (resp. $\alpha^{-1}\beta \in K$), la relation quotient (Ens.R, §5) S/R dans l'espace homogène G/H , est compatible avec la loi externe dans cet espace, et la structure quotient correspondante est isomorphe à celle de G/K .

Considérons en particulier un groupe transitif de transformations Γ d'un ensemble E , et la structure d'espace homogène définie sur E par ce groupe ; on dit que Γ est un groupe <u>primitif</u> s'il n'existe aucune structure quotient de cette structure d'espace homogène, autre qu'elle-même et la structure quotient correspondant à la relation d'équivalence R dans E pour laquelle E est la seule classe (mod.R) (structure définie sur un ensemble à <u>un seul</u> élément) ; dans le cas contraire, Γ est dit <u>imprimitif</u>.

Si Δ est le sous-groupe de Γ laissant invariant un élément $a \in E$ on voit d'après ce qui précède que, <u>pour que Γ soit primitif, il faut et il suffit qu'il n'existe aucun groupe Θ distinct de Γ et Δ et tel que</u> $\Delta \subset \Theta \subset \Gamma$.

<u>Exercices</u>. 1) Montrer que le nombre des conjugués d'un élément a d'un groupe fini G est égal à l'indice du <u>normalisateur</u> (§ 4, exerc. 17) de a et par suite est un diviseur de l'ordre de G .

2) Si G est un groupe fini d'ordre n , le nombre des automorphismes de G est $\leqslant n^{\log_2 n}$ (soit $\{a_1, a_2, \ldots, a_m\}$ un système de générateurs de G tels que a_i n'appartienne pas au sous-groupe engendré par $a_1, a_2, \ldots, a_{i-1}$; montrer que $2^m \leqslant n$, et que le nombre d'automorphismes de G est $\leqslant n^m$).

3) Soit Γ le groupe des automorphismes d'un groupe G , Δ le groupe des automorphismes intérieurs de G ; montrer que Δ est sous-groupe distingué de Γ . Pour qu'un automorphisme σ de G soit

permutable avec tous les automorphismes intérieurs de G, il faut et il suffit que $a^{-1}\sigma(a)$ appartienne au centre de G, pour tout $a \in G$; en déduire que si le centre de G est réduit à l'élément neutre, il en est de même du centralisateur (§ 4, exerc. 17) de Δ dans Γ.

4) a) Soit G un groupe simple non abélien, Γ le groupe des automorphismes de G, Δ le sous-groupe des automorphismes intérieurs de G, Δ le sous-groupe des automorphismes intérieurs de G (isomorphe à G). Si s est un automorphisme du groupe Γ, montrer que $s(\Delta) = \Delta$ (remarquer en vertu de l'exerc. 3, et de l'exerc. 9 du § 4, que l'intersection $\Delta \cap s(\Delta)$ ne peut se réduire à l'élément neutre de Γ).

b) Si φ est l'isomorphisme $x \to a_x$ de G sur Δ, soit ρ l'automorphisme $\varphi^{-1} \circ s \circ \varphi$ de G ; montrer que l'automorphisme $\xi \to \rho^{-1} s(\xi) \rho$ de Γ est l'automorphisme identique (remarquer, à l'aide de l'exerc. 3 que, si un automorphisme t de Γ laisse invariant tout élément $a \in \Delta$, t est l'automorphisme identique, en considérant $t(\sigma a \sigma^{-1})$ pour $a \in \Delta$ et $\sigma \in \Gamma$).

c) Déduire de b) que tout automorphisme du groupe Γ est un automorphisme intérieur.

5) a) Soit G un groupe, Σ le groupe de ses automorphismes, Γ le groupe des translations à gauche de G (isomorphe à G). Montrer que, dans le groupe symétrique $\mathfrak{S}_G$, l'intersection $\Sigma \cap \Gamma$ se réduit à l'élément neutre et que $\Gamma\Sigma = \Sigma\Gamma$; en déduire que $\Sigma\Gamma = \Omega$ est un sous-groupe de $\mathfrak{S}_G$, qu'on appelle l'<u>holomorphie</u> du groupe G (§ 4, exerc. 6).

b) Montrer que Γ est un sous-groupe distingué de Ω, et que tout automorphisme de Γ est de la forme $\gamma \longrightarrow \sigma\gamma\sigma^{-1}$, où $\sigma \in \Sigma$.

c) Le groupe Δ des translations à droite de G est un sous-groupe distingué de Ω, et l'intersection $\Gamma \cap \Delta$ est le centre de chacun de ces deux groupes.

d) Montrer que Ω est le normalisateur (§ 4, exerc. 17) du sous-groupe Γ dans $\mathfrak{S}_G$ (soit τ un élément du normalisateur de Γ ; si on pose $\tau \gamma_x \tau^{-1} = \gamma_{\sigma(x)}$, montrer qu'on a $\sigma(x) = \tau(xu)$ où $u = \tau^{-1}(e)$; montrer que σ est un automorphisme de G, puis utiliser c)).

e) Montrer que Δ est le centralisateur (§ 4, exerc. 17) de Γ dans $\mathfrak{S}_G$.

6) Soit H un sous-groupe distingué d'un groupe G, tel que tous les automorphismes de H soient intérieurs. Montrer que dans chaque classe (mod. H) de G, il existe un élément permutable avec tout élément de H (si $u \in G$, considérer l'automorphisme $x \longrightarrow uxu^{-1}$ de H). En déduire que, si le centre de H est réduit à e, G est produit direct de H et d'un sous-groupe isomorphe à G/H (considérer le centralisateur de H dans G).

7) On appelle sous-groupe <u>caractéristique</u> d'un groupe à opérateurs G tout sous-groupe stable H de G tel que $\sigma(H) \subset H$ pour tout automorphisme σ de G. On dit qu'une suite de composition (G_i) d'un groupe G est une <u>suite caractéristique</u> si tous les termes de cette suite sont des sous-groupes caractéristiques de G et s'il n'existe aucune suite de composition strictement plus fine ayant la même propriété.

a) Si on identifie G avec le groupe Γ de ses translations à gauche, tout sous-groupe caractéristique de G est un sous-groupe distingué de l'holomorphie Ω du groupe G (exerc. 5) et réciproquement, tout sous-groupe distingué de Ω contenu dans G est sous-groupe caractéristique de G.

b) Si les sous-groupes stables de G satisfont à la condition minimale (§ 4, exerc. 20), et s'il existe une suite caractéristique (G_i) du groupe G, montrer que chacun des groupes G_i/G_{i+1} est un produit direct d'un nombre fini de groupes simples isomorphes entre eux (utiliser a) et l'exerc. 20 b) du § 4).

c) Si (G_i) et (H_j) sont deux suites de composition de G dont tous les termes sont caractéristiques, il existe une suite de composition plus fine que (G_i) et (H_j) et dont tous les termes sont caractéristiques (appliquer convenablement le th. de Schreier-Zassenhaus)

d) Si les sous-groupes caractéristiques de G satisfont aux conditions maximale et minimale (§ 4, exerc. 20), pour tout sous-groupe caractéristique H de G, il existe une suite caractéristique (G_i) de G telle que $H = G_i$ pour un indice i ; deux suites caractéristiques (G_i) et (H_j) de G sont isomorphes à l'ordre près. Réciproquement, si G possède une suite caractéristique, les sous-groupes caractéristique, les sous-groupes caractéristiques de G satisfont aux conditions maximale et minimale (utiliser c)).

8) a) Soit (E_ι) une partition d'un ensemble E. L'ensemble des permutations σ de E telles que $\sigma(E_\iota)=E_\iota$ pour tout ι est un sous-groupe du groupe symétrique $\mathfrak{S}_E$ isomorphe au produit $\prod_\iota \mathfrak{S}_{E_\iota}$ (considérer les sous-groupes Γ_ι où Γ_ι est formé des permutations σ telles que $\sigma(E_\iota)=E_\iota$, et $\sigma(x)=x$ pour tout $x \notin E_\iota$).

b) Soit σ une permutation de E, (E_ι) la partition de E formée des classes d'intransitivité du sous-groupe cyclique de $\mathfrak{S}_E$ engendré par σ. La composante de σ dans le groupe $\mathfrak{S}_{E_\iota}$ engendre dans ce groupe un groupe cyclique transitif ; on dit que c'est une permutation <u>circulaire</u> de E_ι, et la permutation correspondante

dans Γ_ν est appelée un <u>cycle</u> de σ ; lorsque le nombre des cycles non réduits à la permutation identique est fini, σ est égal au produit de ses cycles. Lorsqu'un des E_ν a un nombre fini d'éléments, on peut ranger ces éléments en une suite finie $(a_i)_{1 \leqslant i \leqslant n}$ telle que $a_{i+1}=\sigma(a_i)$ $(1 \leqslant i \leqslant n-1)$, et $a_1=\sigma(a_n)$; le cycle correspondant de σ se note alors $(a_1 a_2 \ldots a_n)$.

Si τ est une permutation quelconque de $\mathfrak{S}_E$, on a

(1) $\quad \tau.(a_1 a_2 .. a_n).\tau^{-1}=(\tau(a_1)\tau(a_2)..\tau(a_n))$.

d) Pour que deux permutations de $\mathfrak{S}_n$ soient conjuguées, il faut et il suffit qu'elles se décomposent en le même nombre de cycles, et qu'on puisse faire correspondre les cycles de l'une à ceux de l'autre de sorte que les cycles correspondants permutent le même nombre d'éléments (aient même "longueur"). En déduire que, si σ est une permutation de $\mathfrak{S}_n$ décomposée en p_1 cycles de longueur 1 , p_2 cycles de longueur 2 ,..., p_n cycles de longueur n , le nombre d'éléments de $\mathfrak{S}_n$ conjugués de σ est égal à

$$n!/(p_1!1^{p_1}p_2!2^{p_2}\ldots p_n!n^{p_n}).$$

9) a) Montrer que toute permutation de $\mathfrak{S}_n$ est un produit de transpositions.

b) En déduire que $\mathfrak{S}_n$ est engendré par les n-1 transpositions (12),(13),...,(1n), et aussi par les n-1 transpositions (12),(13),...,(n-1 n) (utiliser la formule (1) de l'exerc. 8c)).

c) En déduire que $\mathfrak{S}_n$ est engendré par les <u>deux</u> permutations (12) et (123...n) (même méthode).

10) a) Montrer que toute permutation de $\mathfrak{A}_n$ est un produit de cycles de longueur 3 (le démontrer pour un produit de deux transpositions).

b) En déduire que $\mathfrak{A}_n$ est engendré par les n-2 permutations (1 2 3), (1 2 4),...,(1 2 n) (utiliser la formule (1)).

c) En déduire que, si n est impair, $\mathfrak{A}_n$ est engendré par les deux permutations (1 2 3) et (1 2 .. n) , et si n est pair, par les deux permutations (1 2 3) et (2 3 .. n) .

11) a) Si un sous-groupe distingué de $\mathfrak{A}_n$ contient un cycle (abc) de longueur 3 , il est identique à $\mathfrak{A}_n$ (utiliser 10b)).

b) Soit Γ un sous-groupe distingué de $\mathfrak{A}_n$ ($n>4$), σ une permutation de Γ qui laisse invariants moins de n-3 éléments de $(1,n)$; montrer qu'il existe un cycle (abc)=ρ tel que $\rho\sigma\rho^{-1}\sigma^{-1}$ laisse invariant un élément de plus que σ et est distincte de la permutation identique.

c) En déduire que $\mathfrak{A}_n$ est un groupe <u>simple</u> si $n>4$.

d) Montrer que, si $n\neq 4$, $\mathfrak{A}_n$ est le seul sous-groupe distingué de $\mathfrak{S}_n$ distinct de $\mathfrak{S}_n$ et de $\{e\}$ (même méthode que dans b)).

e) Montrer que les groupes $\mathfrak{S}_3$ et $\mathfrak{S}_4$ sont résolubles (§ 4,ex.19).

12) Soit Γ un groupe transitif de permutations d'un ensemble E . Pour que Γ soit imprimitif, il faut et il suffit qu'il existe une partie A de E , contenant plus d'un élément et distincte de E , et telle que, pour toute permutation $\sigma\in\Gamma$, on ait $A\cap\sigma(A)=\emptyset$ ou $\sigma(A)\subset A$.

13) Soit Γ un groupe primitif de permutations d'un ensemble E . Montrer que tout sous-groupe distingué de Γ , non réduit à la permutation identique, est transitif (si Δ est un tel sous-groupe, appliquer l'exerc.12 à une classe d'intransitivité de Δ).

14) Un groupe de permutations Γ d'un ensemble E est dit r fois transitif si, quels que soient les deux ensembles $\{a_1,a_2,\ldots,a_r\}$, $\{b_1,b_2,\ldots,b_r\}$ d'éléments de E, il existe une permutation $\sigma \in \Gamma$ telle que $\sigma(a_i)=b_i$ pour $1 \leqslant i \leqslant r$, cette propriété n'ayant plus lieu pour un couple au moins de sous-ensembles de r+1 éléments de E.

a) Montrer qu'un groupe r fois transitif est primitif si $r>1$ (appliquer l'exerc. 12).

b) L'ordre d'un groupe de permutations r fois transitif d'un ensemble de n éléments est de la forme $n(n-1)..(n-r+1)d$, où d est un diviseur de $(n-r)!$ (considérer le sous-groupe des permutations laissant invariants r éléments).

§ 6. Anneaux et anneaux à opérateurs.

1. Anneaux. Définition 1. On dit qu'une structure algèbrique sur un ensemble E est une structure d'anneau (et que E, muni de cette structure, est un anneau), si elle est définie par la donnée de deux lois de composition internes partout définies, dont la première est une loi de groupe abélien sur E, et dont la seconde est associative et doublement distributive par rapport à la première.

Exemples. I. Anneau des entiers rationnels. Nous avons défini, sur l'ensemble Z des entiers rationnels, l'addition (§ 2, n°5) et la multiplication (§ 3, n°9) ; l'addition est une loi de groupe abélien, et la multiplication est associative et doublement distributive par rapport à l'addition ; donc Z, muni de ces deux lois, est un anneau qu'on appelle l'anneau des entiers rationnels.

II . Anneau des endomorphismes d'un groupe abélien. Soit G un groupe abélien noté additivement. L'ensemble G^G des applications de G dans G est muni de deux lois de composition associatives : d'une part la loi $(f,g) \to f \circ g$, que nous noterons ici fg ; d'autre part, la loi $(f,g) \to f+g$ (rappelons que $h=f+g$ est l'application de G dans G telle que $h(x)=f(x)+g(x)$ pour tout $x \in G$) , qui définit une structure de groupe abélien sur G^G. L'ensemble E des endomorphismes de G est un sous-groupe de ce groupe abélien ; en effet, si f et g sont des endomorphismes, et $h=f-g$, on a $h(x+y)=f(x+y)-g(x+y) = f(x)+f(y)-(g(x)+g(y)) = (f(x)-g(x))+(f(y)-g(y)) = h(x)+h(y)$, donc h est un endomorphisme. En outre, E est évidemment stable pour la loi $(f,g) \to fg$; enfin, cette dernière loi est doublement distributive dans E par rapport à la loi $(f,g) \to f+g$: en effet, si $\varphi=f(g+h)$, où f,g et h sont des endomorphismes, on a $\varphi(x)=f(g(x)+h(x)) = f(g(x))+f(h(x))$; et d'autre part, si $\psi=(g+h)f$, on a $\psi(x)=g(f(x))+h(f(x))$. La structure induite sur E par les deux lois précédentes est donc bien une structure d'anneau ; E , muni de cette structure, est appelé l'anneau des endomorphismes du groupe G . Les anneaux définis de cette manière jouent un rôle considérable en Algèbre (voir chap.II et VII) ; on notera que l'anneau des endomorphismes du groupe abélien Z est isomorphe à l'anneau Z des entiers rationnels.

III. Sur tout groupe abélien G (noté additivement), on peut définir une structure d'anneau en prenant comme seconde loi de composition la loi $(x,y) \to 0$, qui est associative, commutative et doublement distributive par rapport à la loi du groupe.

Comme dans les exemples précédents, on note d'ordinaire additivement la loi de groupe abélien d'un anneau A , multiplicativement sa seconde loi de composition.

L'addition, et les deux lois externes déduites par dédoublement (§ 3, n°2) de la multiplication, définissent sur A une structure de groupe abélien à opérateurs, A lui-même étant le domaine d'opérateurs pour chacune des deux lois externes ; pour tout $a \in A$, on appelle homothétie à gauche (resp. homothétie à droite) de l'anneau A, l'endomorphisme $x \to ax$ (resp. $x \to xa$) du groupe additif de A.

Si la multiplication d'un anneau possède un élément neutre, cet élément est dit élément unité de l'anneau, et se note souvent 1 (si aucune confusion n'est à craindre).

Exemples. 1) L'anneau des endomorphismes d'un groupe abélien G possède toujours un élément unité, l'application identique de G sur lui-même.

2) L'anneau G considéré dans l'exemple III ci-dessus n'a pas d'élément unité, si G n'est pas réduit à 0.

3) L'ensemble des entiers rationnels pairs est un anneau sans élément unité.

Il est clair que la structure opposée d'une structure d'anneau est encore une structure d'anneau ; deux anneaux, dont les structures sont opposées, sont dits opposés.

Un anneau est dit commutatif si sa multiplication est commutative ; il est identique à son opposé.

Les anneaux des exemples I et III sont commutatifs ; par contre, l'anneau des endomorphismes d'un groupe abélien quelconque n'est pas commutatif en général (voir exerc. 2).

2. Anneaux à opérateurs. Définition 2. On appelle anneau à opérateurs un ensemble A muni d'une structure d'anneau, et d'une ou plusieurs lois de composition externes distributives par rapport à l'addition dans A, et telles que, si on note $(\alpha,x) \longrightarrow \alpha x$ une quelconque de ces lois, on ait identiquement

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

On voit que les lois de composition externes d'un anneau à opérateurs A , et les deux lois externes déduites par dédoublement de la multiplication dans A , définissent (avec l'addition comme loi interne) une structure de groupe abélien à opérateurs sur A ; en outre, la condition (1) exprime que les lois externes de l'anneau A sont permutables (§ 3, n° 11) avec chacune des deux lois externes déduites par dédoublement de la multiplication.

Les endomorphismes $x \longrightarrow \alpha x$ de la structure de groupe additif de A , produits par les opérateurs de l'anneau A , sont souvent appelés homothéties externes de l'anneau A ; ils sont donc permutables (dans l'anneau des endomorphismes du groupe additif A) avec les homothéties à droite et à gauche de A ; ce qu'on peut encore exprimer en disant que ce sont des endomorphismes de la structure de groupe à opérateurs de A , définie par l'addition et les deux lois externes déduites par dédoublement de la multiplication.

Un anneau A peut toujours être considéré comme anneau à opérateurs avec un seul ensemble d'opérateurs, réduit à un seul élément α tel que $\alpha x = x$ pour tout x (opérateur neutre). Il peut aussi être considéré comme anneau à opérateurs avec pour ensemble d'opérateurs, l'anneau des entiers $\mathbb{Z}$, la loi externe étant $(n,x) \longrightarrow \overset{n}{+} x$

(qu'on notera d'ordinaire n.x ou simplement nx si aucune confusion n'en résulte) ; les identités (1) résultent en effet dans ce cas de la double distributivité de la multiplication par rapport à l'addition.

Aussi, dans toute la suite de ce paragraphe, ne parlerons-nous en principe que d'anneaux à opérateurs ; les résultats que nous énoncerons s'appliqueront aux anneaux comme cas particuliers.

3. Diviseurs de 0. Anneaux d'intégrité. Généralisant la terminologie utilisée pour les entiers naturels (Ens., chap.III), on dira que, dans un anneau à opérateurs A , un élément a est multiple à gauche (resp. multiple à droite) d'un élément b s'il existe $c \in A$ tel que $a=cb$ (resp. $a=bc$) ; on dit aussi alors que b est diviseur à droite (resp. diviseur à gauche) de a .

2 On observera que, si A n'a pas d'élément unité, un élément $a \in A$ n'est pas nécessairement diviseur (à droite ou à gauche) de lui-même ; c'est ce que montre l'exemple III ci-dessus. De même, n.x ne sera pas en général un multiple de x si A n'a pas d'élément unité. Au contraire, si A possède un élément unité e , on peut écrire $n.x = n.ex = (n.e)x = x(n.e)$.

Pour tout élément x d'un anneau à opérateurs A , on a $x^2=x(x+0)=x^2+x0$, d'où $x0=0$, et de même $0x=0$: tout multiple (à gauche ou à droite) de 0 est égal à 0 . Par suite, quels que soient x et y , on a $(-x)y = x(-y) = -xy$, car $(-x)y+xy = (-x+x)y = 0y = 0$; on en conclut que $(-x)(-y) = xy$ (règles des signes).

Par récurrence sur n , on voit donc que $(-x)^n=x^n$ si n est pair, et $(-x)^n=-x^n$ si n est impair.

La relation $x0=0$ montre aussi que si un anneau A n'est pas réduit à 0 et possède un élément unité e , on a $e \neq 0$.

Conformément à la terminologie introduite ci-dessus, tout élément $x \in A$ devrait être considéré comme un diviseur (à droite et à gauche) de 0 ; mais par abus de langage (lorsque A n'est pas réduit au seul élément 0) on réserve le nom de <u>diviseur à gauche</u> (resp. <u>diviseur à droite</u>) <u>de</u> 0 à tout élément a tel qu'il existe $b \neq 0$ satisfaisant à la relation $ab=0$ (resp. $ba=0$). Les diviseurs à gauche et les diviseurs à droite de 0 peuvent encore être caractérisés comme les éléments <u>non réguliers</u> (§ 2, n° 2) pour la multiplication dans A ; en effet si un élément a n'est pas régulier, il existe deux éléments distincts x, y tels que $ax=ay$ ou $xa=ya$, c'est-à-dire $a(x-y)=0$ ou $(x-y)a=0$, avec $x-y \neq 0$; la réciproque est évidente.

Dans un anneau à opérateurs A non réduit à 0, 0 est toujours diviseur (à droite et à gauche) de 0 ; lorsqu'il n'existe pas d'autre diviseur de 0, on dit (par abus de langage) que A est un anneau <u>sans diviseur de</u> 0 ; dans un tel anneau, la relation $ab=0$ est donc équivalente à "$a=0$ ou $b=0$" ; on en déduit, par récurrence sur n, que $a^n=0$ est équivalente à $a=0$.

<u>Définition 3</u>. <u>On appelle anneau d'intégrité un anneau à opérateurs commutatif sans diviseur de</u> 0.

<u>Exemples</u>. 1) L'anneau $\mathbb{Z}$ des entiers rationnels est un anneau d'intégrité ; par contre, l'anneau des endomorphismes d'un groupe abélien quelconque aura en général des diviseurs de 0 (voir ex. 2).

2) Dans l'exemple III donné ci-dessus, tout élément est diviseur de 0 si G n'est pas réduit au seul élément 0.

4. <u>Sous-anneaux</u>. Soit A un anneau à opérateurs, B une partie <u>stable</u> (§ 3, n° 4) de A ; pour que B, muni de la structure induite par celle de A, soit un anneau à opérateurs, il faut et il suffit que B soit un <u>sous-groupe</u> du groupe additif de A. On dit alors que B, muni de la structure induite par la structure d'anneau à opérateurs de A, est un <u>sous-anneau de A</u>.

Exemples. 1) Tout sous-groupe du groupe additif $\mathbb{Z}$, étant de la forme $n.\mathbb{Z}$, avec $n \in \mathbb{N}$, est un sous-anneau de $\mathbb{Z}$; il y a donc identité entre les sous-anneaux de l'anneau $\mathbb{Z}$ et les sous-groupes du groupe additif $\mathbb{Z}$.

2) Dans un anneau à opérateurs A , possédant un élément unité e , les éléments $n.e$ ($n \in \mathbb{Z}$) forment un ensemble B , qui est un sous-groupe du groupe additif de A , et est stable pour la multiplication ; mais il ne sera pas stable en général pour toutes les lois externes sur A , et ne sera donc pas un sous-anneau de A au sens défini ci-dessus.

Remarques. 1) Les conditions pour qu'une partie B d'un anneau à opérateurs A soit un sous-anneau s'écrivent encore : $B+B \subset B$, $-B \subset B$, $B.B \subset B$ et $aB \subset B$ pour tout opérateur a de A .

2) L'exemple 2 ci-dessus prouve que la notion de sous-anneau d'un anneau à opérateurs A , dépend essentiellement des lois externes sur A , et non seulement de la structure d'anneau de A : un sous-anneau de A reste sous-anneau relativement à la structure moins riche obtenue en restreignant les lois externes de A à des parties des domaines d'opérateurs donnés ; mais la réciproque est inexacte. Toutefois, un sous-anneau dans un anneau sans opérateurs A reste encore un sous-anneau quand on considère sur A la loi externe $(n,x) \longrightarrow n.x \quad (= \overset{n}{+} x)$, car tout sous-groupe du groupe additif de A est stable pour cette loi.

Toute intersection de sous-anneaux de A est encore un sous-anneau ; on peut donc définir le sous-anneau engendré par une partie C de A comme le plus petit sous-anneau contenant C .

Proposition 1. Le centre (relatif à la multiplication) d'un anneau à opérateurs A est un sous-anneau de A .

En effet, le centre C de A est stable pour la multiplication (§ 1, n°4); il est stable pour chacune des lois externes de A , car si x est permutable avec z , on a , pour tout opérateur a de A , $(ax)z=a(xz)=a(zx)=z(ax)$ d'après (1). Enfin, C est un sous-groupe du groupe additif de A , car si x et y sont permutables avec z , on a $(x-y)z=xz-yz=zx-zy=z(x-y)$, donc $x-y$ est permutable avec z .

Ce raisonnement montre plus généralement que l'ensemble B des éléments de A permutables avec tous les éléments d'une partie quelconque M de A , est un sous-anneau de A . Par exemple, soit G un groupe abélien à opérateurs ; dans l'anneau E des endomorphismes de la structure de groupe de G , les endomorphismes de la structure de groupe à opérateurs de G sont ceux qui sont permutables avec les homothéties (§ 4, n°) de G ; ils forment donc un sous-anneau de E , qu'on appelle l'anneau des endomorphismes du groupe à opérateurs G .

5. Relations d'équivalence dans un anneau à opérateurs. Idéaux. Anneaux quotients

Cherchons les relations d'équivalence compatibles avec la structure d'un anneau à opérateurs A . D'après le th.4 du § 4, une relation R compatible avec l'addition et avec les lois externes de A , est de la forme $x-y \in H$, où H est un sous-groupe du groupe additif de A , stable pour les opérateurs de A . D'après la prop.1 du § 3, pour exprimer que cette relation est compatible avec la multiplication, il y a lieu d'exprimer séparément qu'elle est compatible à gauche et compatible à droite. Or, la compatibilité à gauche signifie que $x \equiv y \pmod{R}$

entraîne $zx \equiv zy \pmod{R}$, c'est-à-dire que $x-y \in H$ entraîne $zx-zy=z(x-y) \in H$ quel que soit $z \in A$. On est donc conduit à poser la définition suivante :

Définition 4. On appelle idéal à gauche (resp. idéal à droite) d'un anneau à opérateurs A, tout sous-groupe H du groupe additif de A, stable pour les opérateurs de A, et tel que $zH \subset H$ (resp. $Hz \subset H$) pour tout $z \in A$. Une partie de A qui est à la fois idéal à gauche et idéal à droite de A est appelée idéal bilatère de A.

Tout idéal à gauche dans un anneau A est idéal à droite dans l'opposé de A, et réciproquement. Lorsque A est commutatif, les trois espèces d'idéaux se confondent, et on parle alors simplement d'idéaux de A (sans qu'il soit nécessaire de préciser).

Remarques. 1) Pour montrer qu'une partie H d'un anneau à opérateurs A est un idéal à gauche (resp. à droite) de A, il faut donc vérifier les relations $H+H \subset H$, $-H \subset H$, $A.H \subset H$ (resp. $H.A \subset H$) et $\alpha H \subset H$ pour tout opérateur α. Tout idéal est évidemment un sous-anneau de A, la réciproque étant inexacte. Les idéaux d'un anneau sont d'ordinaire désignés par des minuscules gothiques.

2) On peut encore dire qu'un idéal à gauche dans un anneau à opérateurs A, est un sous-groupe du groupe additif de A, stable pour les opérateurs de A, et pour la loi externe à gauche déduite de la multiplication (§ 3, n° 2).

3) Comme celle de sous-anneau, la notion d'idéal, dans un anneau à opérateurs A, est essentiellement relative aux domaines d'opérateurs considérés ; les remarques faites ci-dessus pour les sous-anneaux s'appliquent également aux idéaux.

Théorème 1. Toute relation d'équivalence compatible avec la structure d'un anneau à opérateurs A , est de la forme $x-y \in \mathfrak{a}$, où $\mathfrak{a}$ est un idéal bilatère de A ; et le quotient de A par cette relation est un anneau à opérateurs.

La première partie résulte de ce qui précède. D'autre part, le quotient de l'addition dans A par la relation d'équivalence considérée R est une loi de groupe abélien sur A/R , et les quotients des lois externes de A sont distributives par rapport à cette loi de groupe (§ 3, n°) ; enfin, le quotient par R de la multiplication dans A est une loi associative dans A/R (§ 3, n°), doublement distributive par rapport à la loi quotient de l'addition (§ 3, n°) et satisfaisant aux identités (1) pour tous les opérateurs α de A (§ 3, n°).

Définition 5. Le quotient d'un anneau à opérateurs A par la relation d'équivalence définie par un idéal bilatère $\mathfrak{a}$ s'appelle l'anneau quotient de A par $\mathfrak{a}$; il se note $A/\mathfrak{a}$.

Exemples d'idéaux et d'anneaux quotients. 1) Un anneau à opérateurs A est toujours un idéal bilatère dans A ; de même, l'ensemble réduit au seul élément 0 est un idéal bilatère dans A , qu'on appelle l'idéal nul, et qu'on note souvent (0). L'anneau quotient A/(0) est isomorphe à A ; l'anneau quotient A/A est réduit à 0 .

2) Pour tout élément a d'un anneau à opérateurs A , l'ensemble A.a (resp. a.A) est un idéal à gauche (resp. à droite) de A ; on notera que, si A n'a pas d'élément unité, cet idéal ne contient pas nécessairement a .

3) Si M est une partie quelconque de A , l'ensemble des éléments $x \in A$ tels que $xy=0$ (resp. $yx=0$) pour tout $y \in M$,

est un idéal à gauche (resp. à droite) qu'on appelle l'annihilateur à gauche (resp. à droite) de M . Si A n'a pas de diviseurs de 0 , et si M contient un élément $\neq 0$, les annihilateurs de M se réduisent à l'idéal nul.

4) Les idéaux dans l'anneau $\mathbb{Z}$ des entiers rationnels sont des sous-groupes additifs de $\mathbb{Z}$, donc de la forme $n.\mathbb{Z}$, où $n \in \mathbb{N}$; mais réciproquement, il est évident que tout sous-groupe de cette forme est un idéal de $\mathbb{Z}$; en d'autres termes il y a identité entre les idéaux de l'anneau $\mathbb{Z}$ et les sous-groupes du groupe additif $\mathbb{Z}$; l'idéal $n.\mathbb{Z}$ se note encore (n). L'anneau quotient $\mathbb{Z}/(n)$, pour $n>0$, est un anneau commutatif fini à n éléments (§ 3, n°9) ; on remarquera qu'il possède en général des diviseurs de 0 : par exemple, on a $2 \not\equiv 0 \pmod 4$, mais $2.2 \equiv 0 \pmod 4$, donc la classe (mod.4) de 2 est diviseur de 0 dans l'anneau $\mathbb{Z}/(4)$.

La relation d'équivalence $x-y \in \mathfrak{a}$ définie par un idéal bilatère $\mathfrak{a}$ dans un anneau à opérateurs A , se note le plus souvent $x \equiv y \pmod{\mathfrak{a}}$ ou $x \equiv y \ (\mathfrak{a})$, et s'appelle <u>congruence modulo</u> $\mathfrak{a}$. Les relations $x \equiv y \ (\mathfrak{a})$, $x' \equiv y' \ (\mathfrak{a})$ entraînent donc $x+x' \equiv y+y' \ (\mathfrak{a})$, $-x \equiv -y \ (\mathfrak{a})$, $xx' \equiv yy' \ (\mathfrak{a})$ et $ax \equiv ay \ (\mathfrak{a})$ pour tout opérateur a (<u>règles du calcul des congruences</u>).

On notera par contre que la relation $xy \equiv xz \ (\mathfrak{a})$ <u>n'entraîne pas en général</u> $y \equiv z \ (\mathfrak{a})$, car la classe (mod. $\mathfrak{a}$) de x n'est pas nécessairement élément régulier de $A/\mathfrak{a}$, même si x est régulier dans A (voir exemple 4 ci-dessus).

6. Propriétés des idéaux. Soit A un anneau à opérateurs, $\mathfrak{a}$ un idéal à gauche A , B un sous-anneau de A ; l'intersection $B \cap \mathfrak{a}$ est un idéal à gauche dans l'anneau B . En particulier, si $\mathfrak{a} \subset B$, $\mathfrak{a}$ est un idéal à gauche dans B ; mais inversement, un idéal à gauche dans B n'est pas nécessairement idéal à gauche dans A .

Un idéal à gauche dans A pouvant être considéré comme sous-groupe relatif à une structure de groupe à opérateurs définie sur A , toutes les propriétés des sous-groupes d'un groupe à opérateurs (§ 4, n°) sont applicables aux idéaux à gauche dans A . C'est ainsi que l'intersection d'une famille $(\mathfrak{a}_\iota)$ d'idéaux à gauche est un idéal à gauche ; parmi les idéaux à gauche qui contiennent une partie donnée M de A , il en existe un plus petit, qu'on appelle l'idéal à gauche engendré par M .

En particulier, dans un anneau sans opérateurs A , l'idéal à gauche engendré par l'ensemble réduit à un seul élément a est identique à l'ensemble des éléments de la forme $n.a+xa$ ($n \in \mathbb{Z}$, $x \in A$) car ces éléments appartiennent évidemment à tout idéal à gauche contenant a , et on vérifie aussitôt que leur ensemble est un idéal à gauche. Lorsque A possède un élément unité e , l'idéal à gauche engendré par a est identique à Aa , puisque $n.a=(n.e)a$; en particulier, si un idéal à gauche contient e , il est identique à A . Lorsque A est commutatif, l'idéal engendré par a se note (a) ; tout idéal ainsi engendré par un seul élément est alors dit idéal principal.

Nous avons vu ci-dessus que, dans l'anneau $\mathbb{Z}$, tout idéal est principal.

Soit $(\mathfrak{a}_\iota)$ une famille d'idéaux à gauche dans un anneau à opérateurs A . L'idéal engendré par la réunion des $\mathfrak{a}_\iota$ est identique au sous-groupe du groupe additif de A engendré par cette réunion, c'est-à-dire à l'ensemble des sommes $\sum_{\iota\in H} x_\iota$, où $x_\iota \in \mathfrak{a}_\iota$, et où H est une partie finie quelconque de l'ensemble d'indices ; en effet, pour tout $z \in A$, on a $z(\sum_{\iota\in H} x_\iota) = \sum_{\iota\in H} zx_\iota$, et $zx_\iota \in \mathfrak{a}_\iota$; de même, pour tout opérateur a de A , $a(\sum_{\iota\in H} x_\iota) = \sum_{\iota\in H} ax_\iota$, et $ax_\iota \in \mathfrak{a}_\iota$. En particulier :

Proposition 2. Le plus petit idéal à gauche contenant un nombre fini d'idéaux à gauche $\mathfrak{a}_i$ $(1 \leqslant i \leqslant n)$ est leur somme $\sum_{i=1}^{n} \mathfrak{a}_i$.

En particulier, le plus petit idéal contenant deux idéaux (m) et (n) dans l'anneau $\mathbb{Z}$ est leur somme (m)+(n) ; cet idéal est un idéal principal (d) $(d \in \mathcal{N})$. Or, pour qu'un idéal principal (a) contienne (m), il faut et il suffit évidemment que $m \in (a)$, c'est-à-dire que a soit un diviseur de m . On voit donc que tous les diviseurs communs de m et n sont diviseurs d'un même élément $d \in \mathcal{N}$, qui est lui-même diviseur commun de m et n , et est par suite le plus grand des diviseurs communs de m et n qui sont $\geqslant 0$; aussi appelle-t-on d le plus grand commun diviseur (en abrégé p.g.c.d.) de m et n ; et on voit qu'il existe deux entiers (positifs ou négatifs) p,q, tels que $d=pm+qn$.

De même, le plus grand idéal contenu dans (m) et (n), c'est-à-dire leur intersection $(m)\cap(n)$, est un idéal principal (r) $(r \in \mathcal{N})$; un raisonnement analogue prouve que tout multiple commun de m et n est un multiple de r , et que r est le plus petit des multiples communs $\geqslant 0$ de m et n ; on l'appelle le plus petit commun multiple (p.p.c.m.) de m et n .

On généralise aisément ces considérations à un nombre fini quelconque d'entiers rationnels (cf. chap.V).

Si on revient à l'idéal à gauche engendré par une partie quelconque M d'un anneau à opérateurs A , il est clair que cet idéal contient, pour tout $x \in A$ l'idéal à gauche $\mathfrak{a}_x$ engendré par le seul élément x ; il est donc identique au sous-groupe engendré par la réunion des $\mathfrak{a}_x$.

En particulier, dans un anneau sans opérateurs A , l'idéal à gauche engendré par M est identique à l'ensemble des sommes $\sum_i (n_i \cdot a_i + x_i a_i)$, où (a_i) est une famille finie quelconque d'éléments de M , (n_i) une famille finie quelconque d'entiers rationnels, (x_i) une famille finie quelconque d'éléments de A .

On n'a parlé ci-dessus que d'idéaux à gauche ; nous laissons au lecteur le soin d'énoncer les propositions correspondantes pour les idéaux à droite et les idéaux bilatères.

7. Idéaux maximaux. Définition 6. Dans un anneau à opérateurs A , on appelle idéal à gauche maximal un élément maximal de l'ensemble des idéaux à gauche $\neq A$ (ordonné par inclusion).

Théorème 2 (Krull). Dans un anneau à opérateurs possédant un élément unité, tout idéal à gauche $\neq A$ est contenu dans un idéal à gauche maximal.

D'après le théorème de Zorn (Ens. R, §6), il suffit de prouver que l'ensemble $\mathfrak{E}$ des idéaux à gauche $\neq A$, ordonné par inclusion, est inductif, c'est-à-dire que, si $\mathfrak{F}$ est une partie totalement ordonnée de $\mathfrak{E}$, la réunion $\mathfrak{m}$ des idéaux appartenant à $\mathfrak{F}$ est un idéal à gauche $\neq A$. Or, aucun des idéaux de $\mathfrak{F}$ ne contient l'élément unité e de A , et par suite $e \notin \mathfrak{m}$; d'autre part tout $x \in \mathfrak{m}$ appartient à un idéal $\mathfrak{a} \in \mathfrak{F}$, donc $zx \in \mathfrak{a} \subset \mathfrak{m}$, et $ax \in \mathfrak{a} \subset \mathfrak{m}$ pour tout $z \in A$

et tout opérateur a de A ; enfin, si x et y sont deux éléments quelconques de $\mathfrak{m}$, il existe deux idéaux $\mathfrak{a}$, $\mathfrak{b}$ appartenant à $\mathfrak{F}$ et tels que $x \in \mathfrak{a}$, $y \in \mathfrak{b}$; comme l'un des deux idéaux $\mathfrak{a}$, $\mathfrak{b}$, contient l'autre, x-y appartient à l'un d'eux, et par suite à $\mathfrak{m}$.

C.Q.F.D.

Définitions et résultats analogues pour les idéaux à droite et les idéaux bilatères.

Remarque. Le théorème 2 n'est plus toujours vrai lorsqu'on ne suppose pas que A possède un élément unité (voir exerc. 16).

Exemple. Un idéal maximal dans l'anneau $\mathbb{Z}$ est d'après la déf.6, un idéal principal (p), où $p > 1$ est un nombre entier caractérisé par la propriété de ne posséder aucun diviseur q tel que $1 < q < p$; un tel nombre est appelé nombre premier ; on vérifie immédiatement, par exemple, que 2,3,5,7 sont premiers.

Le th.2 montre que tout entier $n > 1$ possède un diviseur premier ; on peut d'ailleurs le prouver ici sans faire usage du théorème de Zorn : en effet, si n est premier, la proposition est établie ; sinon, il existe un diviseur a_1 de n tel que $1 < a_1 < n$; par récurrence, on établit l'existence d'une suite strictement décroissante (a_k) de diviseurs > 1 de n, et une telle suite est nécessairement finie, donc son dernier terme est premier (cf.ch.V).

8. Homomorphismes d'un anneau. L'application aux anneaux à opérateurs des définitions générales du § 3 donne la définition suivante :

Définition 7. Soient A et A' deux anneaux à opérateurs de même espèce. Une application f de A dans A' s'appelle une représentation (ou un homomorphisme) de A dans A' si elle satisfait aux identités suivantes :

$f(x+y)=f(x)+f(y)$, $f(xy)=f(x)f(y)$, $f(\alpha x)=\alpha f(x)$ quels que soient $x \in A$, $y \in A$, et quel que soit l'opérateur α de A .

L'application canonique d'un anneau à opérateurs A sur un anneau quotient de A est un homomorphisme, dit homomorphisme canonique.

Théorème 5. Si f est une représentation d'un anneau à opérateurs A dans un anneau à opérateurs A' de même espèce, l'image réciproque $f(0)$ est un idéal bilatère de A ; l'image $f(A)$ est un sous-anneau de A' , isomorphe à $A/\mathfrak{a}$; et f est composée d'un isomorphisme de $A/\mathfrak{a}$ dans A' et de l'homomorphisme canonique de A sur $A/\mathfrak{a}$.

Cela résulte du th.1 ci-dessus et du th.1 du § 3, car, la relation $f(x) = f(y)$ s'écrit $f(x-y)=0$.

Exemple. Soit A un anneau sans opérateurs, non réduit à 0 et possédant un élément unité e ; l'application $n \longrightarrow n.e$ est une représentation de l'anneau $\mathbb{Z}$ dans A ; le sous-anneau de A formé par les éléments $n.e$ est donc isomorphe à un anneau quotient $\mathbb{Z}/(q)$, où $q \geqslant 0$; le nombre q est appelé la caractéristique de l'anneau A (cf. chap. II, § 1) ; si $q > 0$, on peut définir ce nombre en disant que c'est le plus petit des entiers $m > 0$ tels que, pour tout $x \in A$, $m.x = 0$.

Proposition 3. Dans un anneau à opérateurs A , si a est un élément inversible, l'application $x \longrightarrow axa^{-1}$ est un automorphisme de A .

On a en effet $a(x+y)a^{-1} = axa^{-1} + aya^{-1}$, $a(xy)a^{-1} = (axa^{-1})(aya^{-1})$, et, pour tout opérateur α de A , $a(\alpha x)a^{-1} = \alpha(axa^{-1})$ en vertu de (1).

9. Idéaux et sous-anneaux dans un anneau quotient. Théorème 4. Soit f l'homomorphisme canonique d'un anneau à opérateurs A sur le quotient $A'=A/\mathfrak{a}$ de A par un idéal bilatère $\mathfrak{a}$.

a) L'image réciproque $B=f^{-1}(B')$ d'un sous-anneau B' (resp. idéal à gauche, idéal à droite) de A', est un sous-anneau (resp. idéal à gauche, idéal à droite) de A , contenant $\mathfrak{a}$; on a $B'=f(B)$, et B' est un anneau isomorphe à l'anneau quotient $B/\mathfrak{a}$.

b) La relation $B=f^{-1}(B')$ établit une correspondance biunivoque entre les sous-anneaux (resp. idéaux à gauche, idéaux à droite) de A' et les sous-anneaux (resp. idéaux à gauche, idéaux à droite) de A , contenant $\mathfrak{a}$. Si $\mathfrak{b}'$ et $\mathfrak{c}'$ sont deux idéaux à gauche (resp. à droite) de A' , on a $f^{-1}(\mathfrak{b}'+\mathfrak{c}')=f^{-1}(\mathfrak{b}')+f^{-1}(\mathfrak{c}')$,
$f^{-1}(\mathfrak{b}'\cap\mathfrak{c}')=f^{-1}(\mathfrak{b}')\cap f^{-1}(\mathfrak{c}')$.

c) Si $\mathfrak{b}'$ est un idéal bilatère de A' , $\mathfrak{b}=f^{-1}(\mathfrak{b}')$ est un idéal bilatère de A , contenant $\mathfrak{a}$, et $A/\mathfrak{b}$ est isomorphe à $A'/\mathfrak{b}'$.

d) Si B est un sous-anneau quelconque de A , $B+\mathfrak{a}$ est un sous-anneau de A , et f(B) est un sous-anneau de A' isomorphe à $B/(B\cap\mathfrak{a})$ et à $(B+\mathfrak{a})/\mathfrak{a}$.

On vérifie immédiatement que si B' est un sous-anneau (resp. idéal à gauche, idéal à droite) de A' , $B=f^{-1}(B')$ est sous-anneau (resp. idéal à gauche, idéal à droite) de A , et contient $\mathfrak{a}$; comme f applique A sur A' , il applique B sur B' , donc B' est isomorphe à $B/\mathfrak{a}$ d'après le th.3 .

Si B est un sous-anneau quelconque de A , la restriction de f à B est une représentation de B dans A' , et l'image réciproque de 0 par cette représentation est $B\cap\mathfrak{a}$; d'après le th. 3 ,

$f(B)$ est donc isomorphe à $B/(B \cap \mathfrak{a})$. L'ensemble $B+\mathfrak{a}$ s'obtient en saturant B pour la relation $x-y \in \mathfrak{a}$; d'après le th.3 du § 3, il est stable pour la multiplication et les lois externes de A, et comme c'est un groupe additif, c'est un sous-anneau de A ; le même théorème prouve que $(B+\mathfrak{a})/\mathfrak{a}$ est isomorphe à $B/(B \cap \mathfrak{a})$. Si on applique ces résultats au cas où $B \supset \mathfrak{a}$, on a $B+\mathfrak{a}=B$, B est saturé, donc si $B'=f(B)$, on a $B=f^{-1}(B')$, la correspondance entre B et B' est bien biunivoque ; d'ailleurs si B est un idéal à gauche (resp. à droite), il en est de même de B', puisque f est une application de A sur A'.

On a ainsi démontré a),d) et la première partie de b) ; les relations $f^{-1}(\mathfrak{b}'+\mathfrak{c}')=f^{-1}(\mathfrak{b}')+f^{-1}(\mathfrak{c}')$, $f^{-1}(\mathfrak{b}' \cap \mathfrak{c}')=f^{-1}(\mathfrak{b}') \cap f^{-1}(\mathfrak{c}')$ sont valables pour des sous-groupes quelconques de A' (§ 4, th.6). Enfin, c) résulte du th.2 du § 3.

Pour tout sous-anneau $B \supset \mathfrak{a}$ de A, on <u>identifiera</u> en général $f(B)$ avec l'anneau quotient $B/\mathfrak{a}$; la partie c) du th.4 s'exprime alors en disant que l'anneau quotient $(A/\mathfrak{a})/(\mathfrak{b}/\mathfrak{a})$ est isomorphe à $A/\mathfrak{b}$.

10. <u>Produits d'anneaux</u>. Il est immédiat (§ 3, n°10) que le produit des structures d'une famille (A_ι) d'anneaux à opérateurs de même espèce, est encore un anneau à opérateurs de même espèce ; on pose donc la définition suivante :

<u>Définition 8</u>. <u>Le produit de la famille d'anneaux à opérateurs</u> $(A_\iota)_{\iota \in I}$ <u>est l'ensemble</u> $A=\prod_{\iota \in I} A_\iota$, <u>avec la structure d'anneau à opérateurs déterminée par les lois</u> $((x_\iota),(y_\iota)) \to (x_\iota+y_\iota)$, $((x_\iota),(y_\iota)) \to (x_\iota y_\iota)$, $(a,(x_\iota)) \to (a\,x_\iota)$ (a opérateur quelconque des A_ι).

Si B_ι est un sous-anneau (resp. idéal à gauche, idéal à droite) de A_ι, $B=\prod_{\iota \in I} B_\iota$ est un sous-anneau (resp. idéal à gauche, idéal à droite) de A. En particulier, si J est une partie non vide de I, $K=\complement J$,

et si $B_\iota = A_\iota$ pour $\iota \in J$, $B_\iota = (0)$ pour $\iota \in K$, le sous-anneau $A'_J = \prod_{\iota \in I} B_\iota$ est un idéal bilatère de A , <u>isomorphe</u> à l'anneau produit $A_J = \prod_{\iota \in J} A_\iota$, avec lequel on l'identifiera souvent. La projection pr_J de A sur A_J est un homomorphisme ; l'image réciproque de 0 par cet isomorphisme n'est autre que A'_K , donc A_J est isomorphe à A/A'_K . On a en outre $A'_J . A'_K = \{0\}$, d'après la définition de la multiplication dans A : on dit que les sous-anneaux A'_J et A'_K <u>s'annulent mutuellement</u>. Il en résulte que tout idéal <u>dans</u> A'_J est aussi un idéal <u>dans</u> A .

On voit aussi que tout produit d'anneaux non réduits à 0 contient des <u>diviseurs de</u> 0 (autres que 0).

Lorsque J est un ensemble $\{\iota\}$ a un seul élément, on désigne encore le sous-anneau A'_J , isomorphe à A_ι , par la notation A'_ι . Si $\mathfrak{a}$ est un idéal à gauche (resp. à droite) dans A , sa projection sur A_ι est un idéal à gauche (resp. droite) dans A_ι (th.4) ; en outre :

<u>Proposition 4</u>. <u>Si l'anneau produit A a un élément unité, l'idéal</u> $\mathfrak{a} \cap A'_\iota$ <u>est isomorphe à la projection de</u> $\mathfrak{a}$ <u>sur</u> A_ι , <u>et</u> $\mathfrak{a}$ <u>est isomorphe au produit de ses projections sur les</u> A_ι .

En effet, soit $x=(x_\iota)$ un élément de $\mathfrak{a}$, e_ι l'élément unité de A_ι , e'_ι l'élément unité de A'_ι ; $\mathfrak{a}$ contient $e'_\iota x$, qui n'est autre que l'élément dont toutes les coordonnées sont nulles, à l'exception de celle d'indice ι , égale à x_ι ; d'où aussitôt la proposition.

Cette proposition est inexacte si on ne suppose plus que A ait un élément unité (voir exerc.).

11. <u>Composés directs de sous-anneaux</u>. Considérons un produit $A = \prod_{1 \leqslant i \leqslant n} A_i$ d'un nombre <u>fini</u> d'anneaux à opérateurs A_i ; avec les notations précédentes, le groupe additif de A est <u>somme directe</u> (§ 4, n°) des groupes additifs des A'_i (on dit aussi, par abus de langage,

que l'anneau A est somme directe des sous-anneaux A_i) ; mais il y a plus, car si $x = \sum_{i=1}^{n} x_i$, $y = \sum_{i=1}^{n} y_i$ sont les décompositions (uniques) de deux éléments quelconques x,y de A ($x_i \in A_i, y_i \in A_i$) , on a $xy = \sum_{i=1}^{n} x_i y_i$.

Définition 9. On dit qu'un anneau à opérateurs A est composé direct d'une famille finie (B_i) de sous-anneaux de A s'il est somme directe des B_i , et si on a identiquement $(\sum_{i=1}^{n} x_i)(\sum_{i=1}^{n} y_i) = \sum_{i=1}^{n} x_i y_i$ ($x_i \in B_i, y_i \in B_i \quad 1 \leqslant i \leqslant n$).

Si A est composé direct des sous-anneaux B_i , il est donc isomorphe à leur produit.

2 On aura soin de ne pas confondre, pour les anneaux, les notions de somme directe et de composé direct de sous-anneaux : un anneau peut fort bien être somme directe de sous-anneaux (et même d'idéaux à gauche ou d'idéaux à droite) sans être leur composé direct ; on en verra des exemples au chap.VII .

Proposition 5. Si un anneau A est somme directe d'une famille finie $(B_i)_{1 \leqslant i \leqslant n}$ de sous-anneaux, les propositions suivantes sont équivalentes :

a) A est composé direct des B_i ;

b) les sous-anneaux B_i sont des idéaux bilatères dans A ;

c) les sous-anneaux B_i s'annulent mutuellement.

En effet, a) entraîne b) puisque A est isomorphe à $\prod_{1 \leqslant i \leqslant n} B_i$; b) entraîne c), car si les B_i sont des idéaux bilatères, on a $B_i . B_j \subset B_i \cap B_j = \{0\}$ pour $i \neq j$; enfin c) entraîne a) d'après la distributivité de la multiplication, et la définition 9 .

Exemple. *Considérons, dans l'anneau quotient $Z/(6)$, le sous-anneau A formé des classes (mod.6) de 0 et 3, et le sous-anneau B formé des classes de 0,2 et 4 ; A est isomorphe à $Z/(2)$, et B isomorphe à $Z/(3)$; $Z/(6)$ est somme directe de A et B, car on a $1=3-2$, et on ne peut avoir $u \equiv v$ (6) $u \equiv 0$ (2), $v \equiv 0$ (3) que si $u \equiv v \equiv 0$ (6) ; enfin, il est immédiat que A et B s'annulent mutuellement, donc $Z/(6)$ est composé direct de A et B, et par suite isomorphe au produit $(Z/(2)) \times (Z/(3))$ (cf. chap.V). *

Si A est composé direct des sous-anneaux B_i $(1 \leqslant i \leqslant n)$, le centre C de A est composé direct des centres C_i des B_i, et on a $C_i = C \cap B_i$. En outre :

Proposition 6. Soit A un anneau à opérateurs ayant un élément unité ; si le centre C de A est composé direct de sous-anneaux C_i $(1 \leqslant i \leqslant n)$, et si $\mathfrak{a}_i$ est l'idéal bilatère de A engendré par C_i, A est composé direct des $\mathfrak{a}_i$.

Soit e l'élément unité de A ; on a $e = \sum_{i=1}^{n} e_i$, où e_i est l'élément unité de C_i ; pour tout $x \in A$, $x = xe = \sum_{i=1}^{n} xe_i$ et $xe_i \in \mathfrak{a}_i$, donc A est somme des $\mathfrak{a}_i$. Reste à prouver que cette somme est directe ; or, l'ensemble des sommes de la forme $\sum_{k=1}^{m} u_k z_k$ où $u_k \in A$, $z_k \in C_i$, m arbitraire, est un idéal bilatère dans A, puisque chacun des z_k est permutable avec tout élément de A ; cet idéal est contenu dans $\mathfrak{a}_i$ et contient C_i, donc il est identique à $\mathfrak{a}_i$. Il en résulte que, pour tout $z \in \mathfrak{a}_i$, $ze_i = z$ et $ze_j = 0$ pour $j \neq i$, car ces propriétés sont vraies pour tout $z \in C_i$. Par suite, si on a $0 = \sum_{i=1}^{n} x_i$, avec $x_i \in \mathfrak{a}_i$, on en tire $0 = 0.e_i = x_i$, ce qui achève la démonstration.

Il y a donc correspondance <u>biunivoque</u> entre les décompositions de A et de son centre C en somme directe d'idéaux bilatères, lorsque A possède un élément unité.

<u>Proposition 7</u>. <u>Soit A un anneau à opérateurs, composé direct de sous-anneaux</u> B_i $(1 \leqslant i \leqslant n)$; <u>si</u> $\mathfrak{a}_i$ <u>est un idéal bilatère dans</u> B_i , <u>l'anneau quotient</u> $A/(\sum_{i=1}^{n} \mathfrak{a}_i)$ <u>est isomorphe au produit des anneaux quotients</u> $B_i/\mathfrak{a}_i$.

C'est une conséquence de la prop. du §3 .

<u>Exercices</u>. 1) Déterminer toutes les structures d'anneau sur un ensemble de n éléments, pour $2 \leqslant n \leqslant 5$, ainsi que les idéaux dans ces anneaux.

2) Montrer que l'anneau des endomorphismes du groupe abélien $\mathbb{Z}/(2) \times \mathbb{Z}/(2)$ est non commutatif et admet des diviseurs de 0.

3) Dans l'ensemble $\mathfrak{P}(E)$ des parties d'un ensemble E , montrer qu'on définit une structure d'anneau commutatif ayant un élément unité (anneau <u>booléien</u>) en posant $AB = A \cap B$ et $A+B = (A \cap \complement B) \cup (B \cap \complement A)$. Cet anneau est isomorphe à l'anneau K^E des applications de E dans l'anneau $K = \mathbb{Z}/(2)$ à deux éléments.

4) Soit A un anneau (sans opérateurs) ; sur l'ensemble $\mathbb{Z} \times A$ on définit l'addition et la multiplication de la manière suivante:

$$(m,x)+(n,y) = (m+n, x+y)$$

$$(m,x)(n,y) = (mn, m.y+n.x+xy)$$

Montrer que ces deux lois définissent sur $\mathbb{Z} \times A$ une structure d'anneau ayant un élément unité, et que A est isomorphe à un idéal bilatère de cet anneau.

5) Soit A un anneau admettant un élément unité e . Si, pour un élément $a \in A$, il existe un $x \in A$ et <u>un seul</u> tel que $ax=e$, a est inversible et x est l'inverse de a (voir § 3, exerc.).

6) Soit A un anneau sans diviseur de 0, admettant un élément unité e, et de caractéristique $\neq 2$. Si $\top$ est une loi de composition interne dans A , distributive à gauche par rapport à l'addition, et doublement distributive par rapport à la multiplication, on a $x \top y = 0$ quels que soient x et y dans A (voir § 3, exerc.).

7) Soit A un anneau à opérateurs, B une partie quelconque de A . Soit B' la partie de A stable pour les lois externes de A , engendrée par B ; soit $B''=B'^{\infty}$ la partie de A , stable pour la multiplication, engendrée par B' ; montrer que le sous-anneau engendré par B est identique au sous-groupe du groupe additif de A engendré par B''. De même, l'idéal à gauche engendré par B est identique au sous-groupe du groupe additif engendré par $B'+A.B'$; l'idéal bilatère engendré par B est identique au sous-groupe additif engendré par $B'+A.B'.A$.

8) Soit A un anneau non réduit à 0 sans diviseur de 0 , et tel que tout sous-groupe additif de A soit un idéal à gauche dans A . Montrer que A est isomorphe à un sous-anneau de $\mathbb{Z}$, ou à un anneau quotient de la forme $\mathbb{Z}/(p)$, où p est premier (considérer le groupe additif engendré par un élément $a \neq 0$; en exprimant que ce groupe est un idéal à gauche, montrer qu'il existe $b \in A$ tel que tout $x \in A$ soit de la forme $n.b$; on a donc $b^2=q.b$; en déduire que l'application $q.n \to n.b$ est une représentation de l'anneau $q.\mathbb{Z}$ des multiples de q , sur l'anneau A).

9) Dans un anneau à opérateurs, l'idéal à droite engendré par un idéal à gauche est un idéal bilatère.

10) Dans un anneau à opérateurs, l'annihilateur à droite d'un idéal à droite est un idéal bilatère.

11) Dans un anneau à opérateurs A , l'idéal bilatère $\mathfrak{a}$ engendré par les éléments xy-yx , où x et y parcourent A , est le plus petit des idéaux bilatères $\mathfrak{b}$ tels que $A/\mathfrak{b}$ soit commutatif.

12) Soit $(\mathfrak{a}_\alpha)$ une famille d'idéaux bilatères dans un anneau à opérateurs A , telle que $\bigcap_\alpha \mathfrak{a}_\alpha = (0)$. Montrer que A est isomorphe à un sous-anneau de l'anneau produit $\prod_\alpha E/\mathfrak{a}_\alpha$.

13) Dans un anneau à opérateurs A , on dit qu'un idéal bilatère $\mathfrak{a}$ est <u>irréductible</u> s'il n'existe pas de couple d'idéaux bilatères $\mathfrak{b}$, $\mathfrak{c}$, distincts de $\mathfrak{a}$ et tels que $\mathfrak{a} = \mathfrak{b} \cap \mathfrak{c}$. Montrer que l'intersection de tous les idéaux irréductibles de A se réduit à 0 (remarquer que l'ensemble des idéaux bilatères ne contenant pas un élément $a \neq 0$ est inductif).

14) Dans un anneau à opérateurs A , on dit qu'un idéal bilatère est <u>indécomposable</u> s'il n'existe aucun couple d'idéaux bilatères $\mathfrak{b}$, $\mathfrak{c}$, distincts de $\mathfrak{a}$ et tels que $\mathfrak{b} \cap \mathfrak{c} = \mathfrak{a}$ et $\mathfrak{b} + \mathfrak{c} = A$. Montrer que tout idéal bilatère est l'intersection des idéaux indécomposables qui le contiennent (raisonner comme dans l'exerc.13, dans l'anneau quotient $A/\mathfrak{a}$).

15) Dans un anneau à opérateurs commutatif A , on dit qu'un idéal $\mathfrak{P} \neq A$ est <u>premier</u> si l'anneau quotient $A/\mathfrak{P}$ est un anneau d'intégrité (autrement dit, si les relations $x \notin \mathfrak{P}$, $y \notin \mathfrak{P}$ entraînent $xy \notin \mathfrak{P}$) .

a) Montrer que, si A possède un élément unité, tout idéal maximal de A est premier.

b) Tout idéal premier est irréductible.

c) L'ensemble des idéaux premiers contenant un idéal donné, s'il n'est pas vide, est inductif pour la relation $\supset$. Si A contient un élément unité, l'ensemble des idéaux premiers contenant un idéal donné $\neq A$ est non vide et inductif pour la relation $\subset$.

d) Soit $\mathfrak{a}$ un idéal $\neq A$ quelconque, $\mathfrak{b}$ l'ensemble des $x \in A$ tels qu'il existe une puissance $x^n \in \mathfrak{a}$ (pour un n dépendant de x). Montrer que $\mathfrak{b}$ est un idéal, et que, si $\mathfrak{b} \neq A$, l'intersection des idéaux premiers contenant $\mathfrak{a}$ est identique à $\mathfrak{b}$ (remarquer que si $a \notin \mathfrak{b}$, l'ensemble des idéaux contenant $\mathfrak{a}$ et ne contenant aucune puissance a^n est inductif, et prouver que, si $\mathfrak{p}$ est un élément maximal de cet ensemble, $\mathfrak{p}$ est premier).

16) Dans le groupe additif Q/Z des nombres rationnels (mod.1) on considère le sous-groupe G formé des classes (mod.1) des nombres rationnels de la forme k/p^n (k et n entiers $\geqslant 0$ arbitraires, p nombre premier fixe). Montrer que tout sous-groupe de G est de la forme G_n , où G_n est le sous-groupe des classes (mod.1) des nombres de la forme k/p^n (k entier $\geqslant 0$ arbitraire). En déduire que, si on considère sur G la structure d'anneau obtenue en prenant $xy=0$ quels que soient x et y dans G , il n'existe pas d'idéal maximal ni d'idéal premier dans G .

17) Soit A un anneau à opérateurs possédant un élément unité. Si A est somme directe d'un nombre fini d'idéaux à gauche $\mathfrak{l}_i$ $(1 \leqslant i \leqslant n)$, et si $e = \sum_{i=1}^{n} e_i$ $(e_i \in \mathfrak{l}_i)$, on a $e_i^2 = e_i$, $e_i e_j = 0$ pour $i \neq j$, et $\mathfrak{l}_i = Ae_i$ (écrire que $x=xe$ pour tout $x \in A$). Réciproquement si n indempotents e_i sont tels que $e_i e_j = 0$ pour $i \neq j$, et $e = \sum_{i=1}^{n} e_i$, A est somme directe dans n idéaux à gauche Ae_i . Pour que les idéaux Ae_i soient bilatères, il faut et il suffit que les e_i appartiennent au centre de A .

18) Soit A un anneau à opérateurs, e un idempotent de A .

a) Montrer que A est somme directe de l'idéal à gauche $\mathfrak{a} = Ae$ et de l'annihilateur à gauche $\mathfrak{b}$ de e (remarquer que pour tout $x \in A$, $x - xe \in \mathfrak{b}$).

b) Tout idéal à droite $\mathfrak{d}$ de A est somme directe de $\mathfrak{d} \cap \mathfrak{a}$ (idéal à droite dans le sous-anneau $\mathfrak{a}$) et $\mathfrak{d} \cap \mathfrak{b}$ (idéal à droite dans le sous-anneau $\mathfrak{b}$).

c) Si $Ae = eA$, e est élément unité de $\mathfrak{a}$, $\mathfrak{b}$ est un idéal bilatère de A , et A est composé direct de $\mathfrak{a}$ et $\mathfrak{b}$; tout idéal à gauche (resp. à droite) $\mathfrak{L}$ de A est somme directe des idéaux à gauche (resp. à droite) $\mathfrak{L} \cap \mathfrak{a}$ et $\mathfrak{L} \cap \mathfrak{b}$ de A .

19) On appelle <u>annéloïde</u> un ensemble E muni de deux lois de composition

a) une multiplication $(x,y) \longrightarrow xy$ partout définie, et associative ;

b) une loi notée additivement $(x,y) \longrightarrow x+y$, <u>non partout définie</u>, et satisfaisant aux conditions suivantes :

1° si $x+y$ est défini, il en est de même de $y+x$, et $x+y = y+x$; on dit alors que x et y sont <u>addibles</u> ;

2° x et y étant addibles, pour que $x+y$ et z soient addibles, il faut et il suffit que x et z , d'une part, y et z d'autre part, soient addibles ; on a alors $(x+y)+z = x+(y+z)$;

3° il existe un élément neutre 0 ;

4° si x et z , d'une part, y et z d'autre part, sont addibles, et si $x+z = y+z$, $x = y$;

5° la multiplication est doublement distributive par rapport à l'addition.

Tout anneau est un annéloïde ; pour qu'un annéloïde admettant un élément unité e soit un anneau, il faut et il suffit qu'il existe un élément x addible avec e et tel que $e+x=0$.

Examiner comment peuvent s'étendre aux annéloïdes les définitions et résultats du § 6 et les exercices ci-dessus (on appellera idéal à gauche d'un annéloïde E une partie $\mathfrak{a}$ de E telle que $E.\mathfrak{a} \subset \mathfrak{a}$, et que la somme de deux éléments addibles de $\mathfrak{a}$ appartienne à $\mathfrak{a}$).

20) Soit G un groupe à opérateurs, f et g deux endomorphismes de G . Pour que l'application $x \to f(x)g(x)$ soit un endomorphisme de G , il faut et il suffit que tout élément du sous-groupe $f(G)$ soit permutable avec tout élément du sous-groupe $g(G)$; si on note alors $f+g$ cet endomorphisme, et fg l'endomorphisme composé $x \to f(g(x))$, montrer que l'ensemble E des endomorphismes de G , muni de ces deux lois de composition, est un <u>annéloïde</u> ayant un élément unité (exerc.19) ; pour que E soit un anneau, il faut et il suffit que G soit <u>abélien</u>.

Pour qu'un élément f de E soit addible avec tous les éléments de E , il faut et il suffit que $f(G)$ soit contenu dans le centre de G ; l'ensemble N de ces endomorphismes est un <u>anneau</u> qu'on appelle le <u>noyau</u> de l'annéloïde E .

Un endomorphisme f de G est dit <u>distingué</u> s'il est permutable avec tous les automorphismes intérieurs de G ; pour tout sous-groupe distingué H de G , $f(H)$ est alors un sous-groupe distingué de G . Montrer que l'ensemble D des endomorphismes distingués de G forme un sous-annéloïde de E , et que le noyau N est un idéal bilatère dans D .

§ 7. Corps .

1. Corps et corps à opérateurs. Définition 1. On dit qu'un anneau K est un corps, si l'ensemble des éléments $\neq 0$ de K est un groupe pour la loi induite par la multiplication de K .

L'ensemble des éléments $\neq 0$ d'un corps K se note d'ordinaire K^* ; muni de la structure de groupe qu'y définit la multiplication de K , on l'appelle le groupe multiplicatif du corps K .

Exemples. * 1) Les corps les plus importants en Mathématique sont le corps des nombres rationnels, qui sera défini au n° , le corps des nombres réels et le corps des nombres complexes, que nous définirons en Topologie générale (chap.IV et V). *

2) D'après la définition 1 , l'ensemble K^* des éléments $\neq 0$ d'un corps K n'est pas vide, puisqu'il forme un groupe ; l'élément neutre e de ce groupe est par définition (§ 6, n°) l'élément unité du corps K ; il est donc $\neq 0$. Un corps possède donc au moins deux éléments ; inversement, sur un ensemble E de deux éléments, on peut définir une structure de corps et (à une permutation près) une seule. En effet, un des éléments de E est l'élément neutre 0 du groupe additif, l'autre est l'élément neutre e du groupe multiplicatif. Le groupe additif est complètement défini par la donnée de e+e , qui ne peut être que 0 ; le groupe multiplicatif est réduit à e ; enfin, on doit avoir $0.e=e.0=0$. On vérifie aussitôt que la multiplication ainsi définie est bien distributive par rapport à l'addition, et on a bien défini ainsi sur E une structure de corps.

On dit qu'un corps est commutatif si la multiplication y est commutative.

Tous les exemples de corps donnés ci-dessus sont commutatifs ; aux chap.III et VII, nous rencontrerons des exemples de corps non commutatifs. Un corps non commutatif est parfois appelé corps gauche.

Il est clair que l'opposé d'un corps est encore un corps.

Si la structure d'anneau d'un anneau à opérateurs K est une structure de corps, on dit que K est un corps à opérateurs ; comme on l'a vu au § 6 , tout corps peut être considéré comme un corps à opérateurs ; aussi ne parlerons-nous en principe que de ces derniers dans ce qui suit.

2. Sous-corps. Soit B une partie non réduite à 0 d'un anneau à opérateurs A ; pour que la structure induite sur B par la structure de A soit une structure de corps à opérateurs, il faut d'abord que B soit un sous-anneau de A ; en outre, il faut que ce sous-anneau possède un élément unité e , et que tout élément $x \neq 0$ de B soit inversible dans B . Inversement, si ces conditions sont remplies, B est un corps ; en effet, tout élément $\neq 0$ de B est alors régulier dans B pour la multiplication, donc l'ensemble B^* de éléments $\neq 0$ de B est stable pour la multiplication, et par suite est un groupe (§ 4, n°).

Si A est un corps à opérateurs, les conditions pour que B soit un corps se simplifient de la façon suivante : il faut et il suffit que B soit un sous-anneau de A , contenant les inverses de tous ses éléments $\neq 0$. Ces conditions sont en effet suffisantes d'après ce qui précède ; elles sont aussi nécessaires, car l'ensemble B^* étant un sous-groupe du groupe multiplicatif de A , doit contenir l'élément unité de A .

Si un sous-anneau B d'un corps à opérateurs K est un corps, on dit que c'est un sous-corps de K ; K est souvent appelé un sur-corps ou une extension du corps B .

Toute intersection de sous-corps d'un corps à opérateurs K est encore un sous-corps de K ; on peut donc définir le sous-corps engendré par une partie quelconque A de K comme le plus petit sous-corps contenant A .

Proposition 1. Le centre d'un corps à opérateurs K est un sous-corps de K .

On sait en effet (§ 6, prop. 1) que c'est un sous-anneau de K . D'autre part, si $x \neq 0$ est permutable avec z , il en est de même de x^{-1} (§ 2, n°), d'où la proposition.

Cela montre plus généralement que l'ensemble B des éléments de K permutables avec tous les éléments d'une partie quelconque A de K , est un sous-corps de K .

3. Idéaux dans un corps. Proposition 2. Dans un corps à opérateurs K , les seuls idéaux à gauche (resp. à droite) sont (0) et K .

En effet, si $x \neq 0$ appartient à un idéal à gauche $\mathfrak{a}$, $x^{-1}x = e \in \mathfrak{a}$, donc $\mathfrak{a} = K$.

Proposition 3. Si f est une représentation d'un corps à opérateurs K dans un anneau à opérateurs A , ou bien f(K) est réduit à 0 , ou bien f(K) est un corps, et f un isomorphisme de K sur f(K).

En effet, $f^{-1}(0)$ est un idéal bilatère dans K , donc identique à K ou à (0), et la proposition résulte du th. 3 du § 6 .

La proposition 2 admet la réciproque suivante :

Proposition 4. Si, dans un anneau à opérateurs A admettant un élément unité et non réduit à 0 , il n'existe aucun idéal à gauche distinct de (0) et de A , A est un corps.

En effet, soit x un élément quelconque $\neq 0$ de A ; comme A possède un élément unité e , l'idéal à gauche engendré par x est l'ensemble Ax;

comme il contient $x \neq 0$, il est identique à A , donc il existe $x' \in A$ tel que $x'x=e$. On a $x' \neq 0$, donc le même raisonnement prouve qu'il existe $x'' \in A$ tel que $x''x'=e$; par suite $xx'=exx'=x''x'xx'=x''x'=e$, autre-ment dit, x' est élément inverse de x , ce qui prouve la proposition.

Corollaire. Soit A un anneau à opérateurs commutatif ayant un élément unité. Pour qu'un anneau quotient $A/\mathfrak{a}$ de A soit un corps, il faut et il suffit que $\mathfrak{a}$ soit un idéal maximal de A .

En effet, $A/\mathfrak{a}$ possède un élément unité, et la condition de l'énoncé exprime que les seuls idéaux de $A/\mathfrak{a}$ sont (0) et $A/\mathfrak{a}$, d'après le th.4 du § 6 .

On voit en particulier que, pour que l'anneau quotient $\mathbb{Z}/(p)$ soit un corps, il faut et il suffit que p soit premier ; par exemple, $\mathbb{Z}/(2)$ est un corps à deux éléments, et on vérifie aisément que sa structure est isomorphe à celle du corps à deux éléments défini ci-dessus.

4. Corps des fractions d'un anneau d'intégrité. Comme tout élément $\neq 0$ d'un corps K est inversible, donc régulier pour la multiplication, un sous-anneau quelconque de K est un anneau sans diviseur de 0 ; en particulier, tout sous-anneau d'un corps commutatif est un anneau d'intégrité. Nous allons montrer qu'inversement, tout anneau d'intégrité peut être "plongé" dans un corps commutatif.

Plus généralement :

Proposition 5. Soit A un anneau à opérateurs commutatif, $\bar{A}$ le symétrisé de A pour la multiplication (§ 2, th.1) .

1) On peut définir sur $\bar{A}$ une structure d'anneau à opérateurs et une seule induisant sur A la structure d'anneau à opérateurs donnée.

2) Soit f une représentation de A dans un anneau à opérateurs A' , telle que l'image par f de tout élément non diviseur de 0 dans A soit inversible dans A' ; on peut prolonger f d'une manière et d'une seule en une représentation $\bar{f}$ de $\bar{A}$ dans A' .

1) Considérons comme d'ordinaire A comme plongé dans $\bar{A}$; tout élément régulier de A est alors inversible dans $\bar{A}$, et tout élément de $\bar{A}$ est de la forme $\frac{x}{y}$, où $x \in A$, $y \in A$ et y est régulier. Cherchons à définir la somme de deux éléments $z = \frac{x}{y}$, $z' = \frac{x'}{y'}$ de $\bar{A}$, de façon que l'addition ainsi définie induise sur A la loi additive donnée, et que la multiplication dans $\bar{A}$ soit distributive par rapport à cette addition ; comme on a $z = \frac{xy'}{yy'}$, $z' = \frac{x'y}{yy'}$, ces conditions entraînent nécessairement que $z + z' = \frac{xy'+x'y}{yy'}$.

Inversement, montrons d'abord que l'élément de $\bar{A}$ ainsi défini ne dépend que de z et z', et non de leur représentation sous forme de fractions ; en effet, si $z = \frac{x_1}{y_1}$, on a $x_1 y = x y_1$, donc $(x_1 y' + x' y_1)y = (xy'+x'y)y_1$, d'où $\frac{x_1 y' + x' y_1}{y_1 y'} = \frac{xy' + x'y}{yy'}$.
On vérifie aussitôt que l'addition ainsi définie dans $\bar{A}$ est associative et commutative, que tout élément $z = \frac{x}{y}$ admet un symétrique $z' = \frac{(-x)}{y}$, et enfin que la multiplication est distributive par rapport à cette addition, donc que ces deux lois définissent sur $\bar{A}$ une structure d'anneau commutatif prolongeant celle de A .

Reste à prolonger à $\bar{A}$ les lois externes de l'anneau A , de façon que les identités (1) du § 6 restent vérifiées ; ici encore, cela n'est possible que d'une seule manière, car si α est un opérateur de A , et $z = \frac{x}{y}$, on doit avoir $\alpha z = \frac{(\alpha x)}{y}$ en vertu de la condition précédente. L'élément αz ainsi défini ne dépend bien que de α et z , et non de la représentation de z sous forme de fraction, car si $\frac{x}{y} = \frac{x_1}{y_1}$, on a

on a $a(x_1 y) = a(x y_1)$, donc $(ax_1)y = (ax)y_1$; on vérifie immédiatement que la loi externe ainsi définie est bien distributive par rapport à l'addition dans $\overline{A}$ et satisfait aux identités (1) du § 6 ; la première partie de la proposition est ainsi complètement démontrée.

2) Si on considère sur A la structure définie par la seule multiplication, on sait (§ 3, th.) que f se prolonge d'une seule manière en une représentation $\overline{f}$ de $\overline{A}$ (muni de la multiplication seule) dans A' , en posant $\overline{f}(\frac{x}{y}) = f(x)(f(y))^{-1}$. En vertu des hypothèses sur f , et de la définition de la structure d'anneau à opérateurs de $\overline{A}$, on vérifie immédiatement que $\overline{f}$ est une représentation de cet anneau à opérateurs dans A' .

Définition 2. On appelle anneau des fractions (ou anneau des quotients) d'un anneau à opérateurs commutatif A , l'anneau à opérateurs commutatif obtenu en munissant le symétrisé $\overline{A}$ de A (pour la multiplication) de la structure définie dans la proposition 5 .

Proposition 6. L'anneau des fractions $\overline{A}$ d'un anneau d'intégrité A est un corps commutatif, appelé corps des fractions (ou corps des quotients) de A .

En effet, tout élément $\neq 0$ de A est régulier dans A , donc inversible dans $\overline{A}$; tout élément $\neq 0$ de $\overline{A}$, étant de la forme $\frac{x}{y}$, où x et y appartiennent à A et sont $\neq 0$, est donc inversible dans $\overline{A}$, d'où la proposition.

Proposition 7. Si un anneau d'intégrité A est contenu dans un corps K , l'ensemble des éléments xy^{-1} de K , où x parcourt A , et y l'ensemble des éléments $\neq 0$ de A , est un sous-corps de K , isomorphe au corps des fractions de A .

C'est une conséquence immédiate de la seconde partie de la prop.5, appliquée à l'application identique de A sur lui-même ; la représentation de $\overline{A}$ dans K , obtenue par prolongement, est nécessairement un isomorphisme d'après la prop.3 .

5. Le corps des nombres rationnels. Définition 3. On appelle corps des nombres rationnels, et on désigne par Q , le corps des fractions de l'anneau Z des entiers rationnels ; les éléments de Q sont appelés nombres rationnels.

On a défini sur Z une relation d'ordre $x \leqslant y$ (§ 2, n°) qui satisfait aux trois conditions suivantes :

a) $x \leqslant y$ entraîne $x+y \leqslant y+z$ quel que soit z ;

b) $x \geqslant 0$ et $y \geqslant 0$ entraînent $xy \geqslant 0$;

c) la structure d'ordre définie par $x \leqslant y$ est une structure d'ensemble totalement ordonné.

Montrons qu'on peut définir sur Q une relation d'ordre et une seule, qui satisfasse encore à ces trois conditions et induise sur Z la relation précédente (cf. chap. VI).

En effet, remarquons d'abord que, si n est un entier >0 , les conditions précédentes entraînent $1/n>0$; sinon on aurait $1/n<0$ (puisque Q doit être totalement ordonné), donc $-1/n>0$, et $n.(-1/n)=-1>0$, ce qui est absurde. On en conclut que, si p et q sont deux entiers >0 , le nombre rationnel p/q est >0 ; comme tout nombre rationnel est de l'une des formes p/q , $-p/q$ (p et q entiers >0), on voit que l'ensemble Q_+^* des nombres rationnels >0 est identique à l'ensemble des nombres de la forme p/q , où p et q parcourent l'ensemble des entiers >0 . Comme, d'après la condition a), la relation $x \leqslant y$ doit être équivalente à $y-x \geqslant 0$,

on voit que s'il existe une relation d'ordre sur Q satisfaisant aux conditions imposées, c'est nécessairement la relation $y-x \in Q_+^*$. Inversement, on vérifie immédiatement que cette relation est bien une relation d'ordre sur Q satisfaisant aux conditions a),b) et c), et induisant sur Z la relation définie antérieurement.

Quand nous parlerons de Q comme d'un ensemble ordonné, il sera toujours entendu, sauf mention expresse du contraire, qu'il s'agit de la relation d'ordre que nous venons de définir.

Les nombres rationnels $\geqslant 0$ (resp. $\leqslant 0$, >0, <0) sont dits positifs (resp. négatifs, strictement positifs, strictement négatifs). On remarquera que l'ensemble Q_+^* des nombres rationnels >0 est un sous-groupe du groupe multiplicatif Q^* des nombres rationnels $\neq 0$; tout nombre rationnel $\neq 0$ se mettant d'une manière et d'une seule sous l'une des formes $(+1)x$, $(-1)x$, avec $x > 0$, on voit que le groupe multiplicatif Q^* est le produit direct du sous-groupe Q_+^* et du sous-groupe $\{+1, -1\}$.

Exercices. 1) Quelles sont les structures de corps parmi les structures d'anneau déterminées dans l'exerc.1 du § 6 .

2) Une anneau fini sans diviseurs de 0 est un corps.

3) Soit A un anneau à opérateurs dans lequel les seuls idéaux à gauche sont (0) et A . Montrer que : ou bien A.A=(0), et le groupe additif à opérateurs A est simple, ou bien A est un corps.

En écartant la première de ces alternatives, on montrera successivement que : a) il existe $a \in A$ tel que $A.a \neq (0)$; b) il existe $e \in A$ tel que $ea = a$ et $e^2=e$; c) e est élément unité de A (considérer l'ensemble des éléments x-xe et l'ensemble des éléments x-ex , où x parcourt A).

4) Montrer que, dans le corps Q des nombres rationnels, il n'existe aucun sous-corps distinct de Q.

5) Soit K un corps commutatif de caractéristique $\neq 2$; soit G un sous-groupe du groupe additif de K, tel que, si H désigne l'ensemble formé de 0 et des inverses des éléments $\neq 0$ de G, H soit aussi un sous-groupe du groupe additif de K. Montrer qu'il existe un élément $a \in K$ et un sous-corps K' de K tels que $G = a.K'$ (établir d'abord que, si x et y sont deux éléments de G tels que $y \neq 0$, $x^2/y \in G$; en déduire que, si x,y,z sont trois éléments de G tels que $z \neq 0$, $xy/z \in G$).

6) Soit A un anneau commutatif ayant un élément unité, $\overline{A}$ l'anneau des fractions de A. Si S est une partie de A, stable pour la mutliplication, et ne contenant aucun diviseur de 0, on désigne par A_S le sous-anneau de $\overline{A}$ formé des éléments x/s, où x parcourt A et s parcourt S.

a) Si $\mathfrak{a}$ est un idéal de A, l'idéal de A_S engendré par $\mathfrak{a}$ est identique à l'ensemble $\mathfrak{a}.A_S$ des éléments x/s, où x parcourt $\mathfrak{a}$ et s parcourt S. Si $\mathfrak{a}$ et $\mathfrak{b}$ sont deux idéaux de A, on a $(\mathfrak{a}+\mathfrak{b}).A_S = \mathfrak{a}.A_S + \mathfrak{b}.A_S$, et $(\mathfrak{a} \cap \mathfrak{b}).A_S = (\mathfrak{a}.A_S) \cap (\mathfrak{b}.A_S)$.

b) Si $\mathfrak{b}$ est un idéal de A_S, on a $(\mathfrak{b} \cap A).A_S = \mathfrak{b}$.

c) Si $\mathfrak{a}$ est un idéal de A, on a $\mathfrak{a} \subset (\mathfrak{a}.A_S) \cap A$; l'idéal $(\mathfrak{a}.A_S) \cap A$ est l'ensemble des éléments $x \in A$ tels qu'il existe $s \in S$ tel que $sx \in \mathfrak{a}$.

d) Soit $\mathfrak{a}$ un idéal de A, φ l'application canonique de A sur l'anneau quotient $A/\mathfrak{a}$; pour que les éléments de $\varphi(S)$ soient réguliers pour la multiplication dans $A/\mathfrak{a}$ il faut et il suffit que $(\mathfrak{a}.A_S) \cap A = \mathfrak{a}$; l'anneau quotient $A_S/(\mathfrak{a}.A_S)$ est alors isomorphe à $(A/\mathfrak{a})_{\varphi(S)}$.

e) Pour que le complémentaire S d'un idéal $\mathfrak{p}$ de A soit stable pour la multiplication, il faut et il suffit que $\mathfrak{p}$ soit premier (§ 6, exerc. 15) ; l'anneau quotient $A_S/(\mathfrak{p}.A_S)$ est alors un corps, isomorphe au corps des fractions de l'anneau d'intégrité $A/\mathfrak{p}$.
