COTE : BKI 02-1.4

LOIS DE COMPOSITION

Rédaction n° 033 bis

Nombre de pages : 44

Nombre de feuilles : 44

Université Henri Poincaré - Nancy I
INSTITUT ÉLIE CARTAN - UMR 7502
Bibliothèque de mathématiques
B.P. 239
54506 Vandoeuvre-Lès-Nancy

Algèbre

Lois de composit

(Urredaktion

33 bis

LOIS DE COMPOSITION

§ I. LOIS DE COMPOSITION RELIANT DEUX ENSEMBLES.

Nous considérerons une théorie mathématique qui comporte deux ensembles fondamentaux P et γ et dont la structure est donnée par une fonction définie sur $P \times \gamma$ et à valeurs dans γ. Une telle fonction s'appelle une <u>loi de composition</u> entre les éléments de P et de γ. (α, a) étant un élément de $P \times \gamma$, nous désignerons par $\alpha \top a$ l'élément de γ qui lui correspond par la fonction en question. On l'appellera le composé de α et de a.

α étant un élément fixe de P, la fonction $f_\alpha(x) = \alpha \top x$ est une fonction définie sur γ et à valeurs dans γ, ou, si on veut, une application de γ dans γ. On voit donc qu'à chaque élément $\alpha \in P$ on peut faire correspondre une application de γ dans lui-même : on l'appelle application produite par α. On exprime encore ce fait en disant que la loi de composition définit P comme <u>domaine d'opérateurs</u> de γ.

Inversement, si nous nous donnons une fonction qui à chaque $\alpha \in P$ fasse correspondre une application $f_\alpha(x)$ de γ dans lui-même, nous aurons défini une loi de composition entre éléments de P et éléments de γ, donnée par la formule

$$\alpha \top x = f_\alpha(x).$$

A étant une partie de γ, nous dirons que A est <u>invariant</u> par les opérateurs de P (ou plus simplement invariant par P)

lorsque les conditions $\alpha \in \rho$, $x \in A$ entraînent $\alpha \top x \in A$. Dans ce cas la fonction $\alpha \top x$, dont on restreint le champ de définition aux couples $(\alpha, x) \in \rho \times A$ est une loi de composition entre éléments de ρ et de A : la structure définie par cette loi de composition est appelée la <u>structure induite</u> sur A par celle de $\mathcal{V}$.

Il est clair que si $\mathcal{F}$ est une famille de parties de $\mathcal{V}$ invariantes par ρ, l'intersection des ensembles de $\mathcal{F}$ est encore invariante par ρ .

B étant une partie quelconque de $\mathcal{V}$, soit A l'intersection de toutes les parties de $\mathcal{V}$ invariantes par ρ qui contiennent B. A est invariant par ρ , contient B et est contenu dans toute autre partie de $\mathcal{V}$ invariante par ρ et contenant B : c'est pourquoi on appelle A <u>le plus petit ensemble invariant par</u> ρ <u>et contenant</u> B. On dit encore que A est la partie <u>engendrée</u> par les éléments de B ou que les éléments de B forment un <u>système de générateurs</u> de A, ou que la structure induite sur A est la structure engendrée par les éléments de B .

De même, si Σ est une partie de ρ , la fonction $\alpha \top x$, en restreignant son champ de définition aux couples qui appartiennent à $\Sigma \times \mathcal{V}$ définit une loi de composition entre éléments de Σ et éléments de $\mathcal{V}$. On pourra avoir à considérer des parties de γ qui sont invariantes par Σ sans l'être nécessairement par ρ .

Considérons maintenant un second ensemble $\mathcal{T}$ admettant encore ρ pour domaine d'opérateurs. Il existe donc une fonction $\alpha \perp \mathcal{T}$ définie dans $\rho \times \mathcal{T}$ et à valeurs dans $\mathcal{T}$.

Considérons une application f(x) de $\mathcal{V}$ dans $\mathcal{F}$. Nous dirons que cette application est une <u>homomorphie</u> de $\mathcal{V}$ dans $\mathcal{F}$ si l'on a pour tout couple d'éléments $\alpha \in \mathcal{P}$, $x \in \mathcal{V}$,

$$f(\alpha \top x) = \alpha \perp f(x)$$

Si de plus, f(x) est une application de $\mathcal{V}$ <u>sur</u> $\mathcal{F}$, on parlera d'une homomorphie de $\mathcal{V}$ <u>sur</u> (ou <u>avec</u>) $\mathcal{F}$.

La donné de f(x) définit une décomposition de $\mathcal{V}$ en classes, donc une relation d'équivalence "$x \sim x'$" qui sera vraie si et seulement si $f(x) = f(x')$. Il en résulte que :

α <u>étant un élément de</u> $\mathcal{P}$, <u>la relation</u> $x \sim x'$ <u>entraîne</u> $\alpha \top x \sim \alpha \top x'$.

Inversement, nous dirons qu'une relation d'équivalence "$x \sim x'$" entre éléments de $\mathcal{V}$ est <u>compatible</u> avec la loi $\top$ si la condition précédente est vérifiée. Supposons qu'il en soit ainsi : soit $\mathcal{F}$ l'ensemble des classes d'équivalence définies par la relation en question. $\mathcal{C}$ étant l'une de ces classes, tous les éléments $\alpha \top x$ (pour $x \in \mathcal{C}$) sont équivalents entre eux et appartiennent à une même classe que nous pouvons désigner par $\alpha \top \mathcal{C}$. Nous avons donc défini une loi de composition entre éléments de $\mathcal{P}$ et éléments de $\mathcal{F}$; de plus, l'application de $\mathcal{V}$ sur $\mathcal{F}$ qui à chaque élément de $\mathcal{V}$ fait correspondre la classe à laquelle il appartient est une homomorphie de $\mathcal{V}$ sur $\mathcal{F}$.

La structure définie par $\mathcal{F}$ et par la loi de composition que nous venons d'indiquer s'appelle une <u>structure-quotient</u> de $\mathcal{V}$.

Soit maintenant f(x) une homomorphie de $\mathcal{V}$ sur un ensemble $\mathcal{F}'$ structuré par une loi de composition désignée par le signe $\perp$ entre éléments de ρ et de $\mathcal{F}'$. La donnée de f(x) définit dans γ une relation d'équivalence compatible avec la loi $\top$, donc aussi une structure quotient $\mathcal{F}$ de γ. La valeur de f(x) ne dépend que de la classe $\mathcal{C} \in \mathcal{F}$ à laquelle appartient x : on obtient ainsi une fonction $f(\mathcal{C})$ définie sur $\mathcal{F}$ et à valeurs dans $\mathcal{F}'$, qui est évidemment une isomorphie des structures $\mathcal{F}$ et $\mathcal{F}'$.

Disons qu'une structure $\mathcal{F}$ définie par une loi de composition entre éléments de ρ et de $\mathcal{F}'$ est <u>homomorphe</u> à γ s'il existe une homomorphie de γ sur $\mathcal{F}'$: nous avons le théorème suivant :

<u>Toute structure homomorphe à</u> γ <u>est isomorphe à une structure-quotient de</u> γ .

$\mathcal{F}$ étant une structure quotient de γ, considérons une relation $\bar{R}(\mathcal{C}, \mathcal{Y})$ entre éléments de $\mathcal{F}$ qui soit compatible avec la loi de composition $\alpha \top \mathcal{C}$. Soit R(x,y) la relation entre éléments de γ qui s'exprime de la manière suivante : $\mathcal{C}$, $\mathcal{Y}$ étant les classes de x, y, la proposition $\bar{R}(\mathcal{C}, \mathcal{Y})$ est vraie. R(x, y) est une relation d'équivalence entre éléments de γ . En effet, x, y, z désignant trois éléments de γ et $\mathcal{C}$, $\mathcal{Y}$, $\mathcal{Z}$ leurs classes : a) la proposition vraie $\bar{R}(\mathcal{C}, \mathcal{C})$ entraîne R(x, x) ; b) la proposition R(x, y) entraîne $\bar{R}(\mathcal{C}, \mathcal{Y})$, donc aussi $\bar{R}(\mathcal{Y}, \mathcal{C})$ et R(y,x) ; c) les propositions R(x,y), R(y,z) entraînent $\bar{R}(\mathcal{C}, \mathcal{Y})$ et $\bar{R}(\mathcal{Y}, \mathcal{Z})$, donc $\bar{R}(\mathcal{C}, \mathcal{Z})$, et aussi R(x, z). De plus, R(x, y) est compatible avec la loi de composition $\alpha \top x$. En effet, si $\alpha \in \rho$, la condition R(x,y) entraîne $\bar{R}(\mathcal{C}, \mathcal{Y})$, donc aussi $\bar{R}(\alpha \top \mathcal{C}, \alpha \top \mathcal{Y})$ qui entraîne $R(\alpha \top x, \alpha \top y)$.

Ceci posé, les relations $\bar{R}(\mathcal{C}, \mathcal{Y})$, $R(x,y)$ définissent l'une une structure quotient $\overline{\mathcal{U}}$ de $\mathcal{F}$, l'autre une structure -quotient $\mathcal{U}$ de $\mathcal{V}$. Les structures $\overline{\mathcal{U}}$, $\mathcal{U}$ sont isomorphes. En effet, x étant dans $\mathcal{V}$, et $\mathcal{C}$ étant la classe (par rapport à la relation " $x \sim y$ " qui définit $\mathcal{F}$) qui contient x, désignons par $f(x)$ la classe (suivant la relation $\bar{R}$) d'éléments de $\mathcal{F}$ à laquelle appartient $\mathcal{C}$: f est une application de $\mathcal{V}$ sur $\mathcal{U}$. $\bar{\mathcal{C}}$ étant un élément de $\overline{\mathcal{U}}$, choisissons un $\mathcal{C} \in \mathcal{F}$ tel que $\mathcal{C} \in \bar{\mathcal{C}}$ et un $x \in \mathcal{V}$ tel que $x \in \mathcal{C}$: on a $f(x) = \bar{\mathcal{C}}$, donc f est une application de $\mathcal{V}$ sur $\overline{\mathcal{U}}$. On a

$$f(\alpha \top x) = \alpha \top f(x)$$

donc f est une homomorphie de $\mathcal{V}$ sur $\overline{\mathcal{U}}$. Comme d'autre part, les conditions $f(x) = f(y)$ et $R(x, y)$ sont équivalentes, f définit une isomorphie de $\mathcal{U}$ avec $\overline{\mathcal{U}}$.

On remarquera que la relation $x \sim y$ entraîne $R(x, y)$.

Inversement, soit $R(x,y)$ une relation d'équivalence entre éléments de $\mathcal{V}$ compatible avec la loi de composition $\alpha \top x$ et telle que la relation $x \sim y$ entraîne $R(x, y)$. Alors, les conditions $R(x, y)$, $x \sim x'$, $y \sim y'$ entraînent $R(x', y')$; en effet, les conditions $x \sim x'$, $R(x, y)$ entraînent $x' \sim x$, $R(x, y)$ et aussi $R(x', x)$, $R(x, y)$, donc encore $R(x', y)$; les relations $R(x', y)$, $y \sim y'$ entraînent $R(x', y)$ et $R(y, y')$, donc aussi $R(x', y')$. Nous pouvons définir une relation $\bar{R}(\mathcal{C}, \mathcal{Y})$ entre éléments de $\mathcal{F}$ qui sera vraie si et seulement si les conditions $x \in \mathcal{C}$, $y \in \mathcal{Y}$ entraînent $R(x, y)$. La relation $\bar{R}$ est une relation d'équivalence. En effet : a) les conditions $x \in \mathcal{C}$, $y \in \mathcal{C}$ entraînent $x \sim y$, donc $R(x,y)$, donc $\overline{R}(\mathcal{C}, \mathcal{C})$; b) $\overline{R}(\mathcal{C}, \mathcal{Y})$ entraîne, si $x \in \mathcal{C}$, $y \in \mathcal{Y}$, $R(x, y)$, donc aussi $R(y,x)$ et $\overline{R}(\mathcal{Y}, \mathcal{C})$; c) les relations $\overline{R}(\mathcal{C}, \mathcal{Y})$, $\overline{R}(\mathcal{Y}, \mathcal{Z})$ entraînent, si $x \in \mathcal{C}$, $y \in \mathcal{Y}$, $z \in \mathcal{Z}$, $R(x,y)$ et $R(y,z)$, donc aussi $R(x,z)$ et $\overline{R}(\mathcal{C}, \mathcal{Z})$. De plus, la relation $\overline{R}$ est compatible avec la loi de composition $\alpha \top \mathcal{C}$: car les conditions $x \in \mathcal{C}$, $y \in \mathcal{Y}$, $\overline{R}(\mathcal{C}, \mathcal{Y})$ entraînent $R(x, y)$, donc aussi $R(\alpha \top x, \alpha \top y)$ et $\overline{R}(\alpha \top \mathcal{C}, \alpha \top \mathcal{Y})$.

De plus, si à partir de la relation $\overline{R}$ on reconstruit par le procédé indiqué un peu plus haut une relation entre éléments de $\mathcal{V}$, on retombe sur R.

Il résulte de tout ceci que :

<u>Les structures-quotient d'une structure quotient $\mathcal{F}$ de $\mathcal{V}$ définie par une relation</u> "$x \sim y$" <u>sont isomorphes aux structures-quotient de $\mathcal{V}$ définies par les relations</u> $R(x, y)$ <u>qui sont des relations d'équivalence compatibles avec la loi</u> $\top$ <u>et qui sont des conséquences de la relation</u> "$x \sim y$".

<u>II. LOIS DE COMPOSITION DANS</u> $\mathcal{V}$.

Un intérêt particulier s'attache au cas dans lequel on a $\mathcal{P} = \mathcal{V}$. On a dans ce cas une loi de composition $x \top y$ entre éléments de $\mathcal{V}$.

Nous avons déjà rencontré plusieurs exemples de pareilles lois de composition. Ainsi, l'addition, la multiplication, l'exponentiation sont des lois de composition dans l'ensemble des entiers naturels.

$\mathcal{E}$ désignant un ensemble quelconque, soit $\mathcal{T}$ l'ensemble des applications de $\mathcal{E}$ dans $\mathcal{E}$. $f(x)$ et $g(x)$ étant des applications de $\mathcal{E}$ dans $\mathcal{E}$, il en est de même de $f(g(x))$. Cette nouvelle application est appelée le produit des applications f et g et se désigne par fg. Cette multiplication des applications est une loi de composition dans $\mathcal{T}$.

$\mathcal{T}$ désignant un ensemble ordonné, x et y étant des éléments de $\mathcal{T}$, on a ou bien $x < y$ ou bien $y \leqslant x$. Posons dans le premier cas _borne_ $(x, y) = x$ et dans le second cas _borne_ $(x, y) = y$. Nous avons ainsi défini une loi de composition dans $\mathcal{T}$. On définit de même l'élément $\overline{\text{borne}}$ (x, y) comme égal à y dans le premier cas et à x dans le second cas.

$\mathcal{T}$ étant un ensemble structuré par une loi de composition $\top$, et $\mathcal{E}$ un ensemble quelconque, soit $\mathcal{F}$ l'ensemble des fonctions définies sur $\mathcal{E}$ et à valeurs dans $\mathcal{T}$. f et g désignant deux éléments de $\mathcal{F}$, la formule

$$h(x) = f(x) \top g(x) \qquad \text{(pour tout } x \in \mathcal{E}\text{)}$$

définit un nouvel élément $h \in \mathcal{F}$ que l'on désigne par $f \top g$: nous obtenons ainsi une loi de composition dans $\mathcal{F}$. Lorsque $\mathcal{E} = \mathcal{T}$, il faut se garder de confondre cette loi de composition avec la multiplication déjà définie des applications de $\mathcal{E}$ dans lui-même.

Enfin, comme dernier exemple, soit $\mathcal{T}$ l'ensemble des suites finies d'éléments d'un ensemble $\mathcal{E}$. Soient $S = (x_0, x_1, \ldots, x_{n-1})$ et $S' = (x'_0, x'_1, \ldots, x'_{n-1})$ deux de ces suites. Nous pouvons à partir de ces suites en construire une nouvelle

$SS' = (x''_0, x''_1, \dots, x''_{n+n'-1})$ définie par les formules

$$x''_p = x_p \quad \text{si } p < n \; ; \quad x''_p = x'_{p-n} \quad \text{si } p \geqslant n$$

Nous dirons que la suite SS' résulte de la juxtaposition de S' à la droite de S. On désigne souvent la suite SS' par la notation $(x_0, x_1, \dots, x_{n-1}, x'_0, x'_1, \dots, x'_{n'-1})$. La juxtaposition ainsi définie est une loi de composition dans l'ensemble des suites finies.

L'ensemble $\mathcal{T}$ étant structuré par une loi de composition $\top$ entre ses éléments, cette loi permet de définir de deux manières $\mathcal{T}$ comme domaine d'opérateurs de lui-même. a étant un élément de $\mathcal{T}$ on peut en effet lui faire correspondre les fonctions

$$f_a(y) = a \top y \quad ; \quad g_a(y) = y \top a$$

qui sont toutes deux des applications de $\mathcal{T}$ dans lui-même. Ce fait introduit quelques complications dans les notions de structure induite et de structure quotient.

A étant une partie de $\mathcal{T}$, nous pouvons, pour définir une structure induite sur A, distinguer plusieurs cas :

<u>1 a.</u> Si les conditions $x \in \mathcal{T}$, $a \in A$ entraînent $x \top a \in A$, on dit que A est <u>invariant à gauche</u> par les opérateurs de $\mathcal{T}$.

<u>1 b.</u> Si les conditions $x \in \mathcal{T}$, $a \in A$ entraînent $a \top x \in A$, on dit que A est <u>invariant à droite</u> par les opérateurs de $\mathcal{T}$.

Dans chacun de ces cas, il existe une loi de composition entre éléments de $\mathcal{T}$ et de A, définie dans le cas 1 a. par la fonction $f_x(y)$, dans le cas 1 b. par $g_x(y)$.

2. Dans les cas précédents, $\mathcal{T}$ se trouve défini comme domaine d'opérateurs de A. Mais on peut aussi chercher les cas dans lesquels la loi de composition dans $\mathcal{T}$ induit une loi de composition entre

éléments de A. Pour qu'il en soit ainsi, il faut et suffit que les conditions $x \in A$, $y \in A$ entraînent $x \top y \in A$. On dit alors que A est fermé par rapport à la loi $\top$. Il est évident que cette condition est remplie par toute partie qui est invariante à gauche ou à droite. Mais la réciproque n'est pas vraie en général.

Quand nous parlerons de structure induite sur une partie de $\mathcal{T}$, c'est au cas 2. que nous nous référerons en principe, sauf indication supplémentaire.

Il est clair que l'intersection d'une famille de parties de $\mathcal{T}$ fermées par rapport à la composition dans $\mathcal{T}$ possède encore la même propriété. Nous pourrons donc encore définir, comme au § 1, la structure induite <u>engendrée</u> par les éléments d'une partie de $\mathcal{T}$, et la notion de <u>système de générateurs</u> d'une structure induite.

Les mêmes discriminations interviennent du point de vue de la recherche des structures-quotient. Soit donnée une relation d'équivalence "$x \sim x'$" entre éléments de $\mathcal{T}$. Nous aurons à distinguer les cas suivants :

<u>1°a</u>. La relation peut être compatible avec la composition à gauche avec les éléments de $\mathcal{T}$: c'est-à-dire que les conditions $y \in \mathcal{T}$, $x \sim x'$ entraînent $y \top x \sim y \top x'$; dans ce cas, l'ensemble $\mathcal{F}$ des classes d'équivalence admet $\mathcal{T}$ comme domaine d'opérateurs, la loi de composition étant définie de la manière suivante : si $\mathcal{C}$ est une classe, $y \top \mathcal{C}$ est la classe qui contient tous les éléments $y \top x$ pour $x \in \mathcal{C}$.

<u>1'b</u>. La relation peut être compatible avec la composition à droite avec les éléments de $\mathcal{T}$: c'est-à-dire que les conditions $y \in \mathcal{T}$, $x \sim x'$ entraînent $x \top y \sim x' \top y$. On tire alors des conclusions analogues aux précédentes.

<u>2'</u>. Si nous supposons maintenant que les conditions $x \sim x'$, $y \sim y'$ entraînent $x \top y \sim x' \top y'$, l'ensemble $\mathcal{F}$ des classes d'équivalence admettra une loi de composition : $\mathcal{X}$ et $\mathcal{Y}$ étant deux de ces classes $\mathcal{X} \top \mathcal{Y}$ sera la classe qui contiendra tous les éléments $x \top y$ pour $x \in \mathcal{X}$, $y \in \mathcal{Y}$. Nous dirons dans ce cas que la relation d'équivalence considérée est une <u>relation de congruence</u> (par rapport à la loi $\top$).

Il est clair que la condition 2'. est équivalente à l'ensemble des conditions 1'a., 1'b. .

Quand nous parlerons de structure quotient de $\mathcal{T}$, nous nous référerons, sauf indication du contraire, au cas 2!

De la même manière, nous aurons plusieurs catégories d'homomorphies :

<u>1"a</u>. Les homomorphies par rapport à la composition à gauche avec les éléments de $\mathcal{T}$: ce sont des applications de $\mathcal{T}$ sur des ensembles $\mathcal{F}$ structurés par des lois de composition $\perp$ entre éléments de $\mathcal{T}$ et de $\mathcal{F}$ telles que l'on ait $f(x \top y) = x \perp f(y)$.

<u>1"b</u>. Les homomorphies par rapport à la composition à droite avec les éléments de $\mathcal{T}$: ce sont les applications de $\mathcal{T}$ sur des ensembles $\mathcal{F}$ structurés par des lois de composition $\perp$ entre éléments de $\mathcal{T}$ et de $\mathcal{F}$ telles que l'on ait $f(x \top y) = y \perp f(x)$.

<u>2"</u>. Les homomorphies (tout court) de $\mathcal{T}$: ce sont les applications $f(x)$ de $\mathcal{T}$ sur des ensembles $\mathcal{F}$ munis de lois de composition internes désignées par le signe $\perp$, telles que $f(x \top y) = f(x) \perp f(y)$.

Conformément à nos conventions précédentes, quand nous parlerons d'homomorphies sans préciser, nous nous référerons au cas 2°.

En raisonnant comme au § I, on verra facilement que les <u>structures homomorphes à $\mathcal{T}$ sont les structures isomorphes aux structures quotient de</u> $\mathcal{T}$.

On voit également que les structures quotient d'une structure quotient $\mathcal{F}$, définie par une relation de congruence "$x \equiv y$", sont isomorphes aux structures quotient de $\mathcal{T}$ définies par les relations de congruence qui sont des conséquences de "$x \equiv y$".

§ III. ASSOCIATIVITÉ

Soit $\mathcal{T}$ un ensemble structuré par une loi de composition $\top$ entre éléments de $\mathcal{T}$. La loi $\top$ est dite <u>associative</u>, si, x, y, z désignant trois éléments de $\mathcal{T}$, on a toujours

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

Nous avons montré par exemple que l'addition et la multiplication des entiers naturels sont des lois de composition associatives. Il n'en est pas de même de l'exponentiation.

La multiplication des applications d'un ensemble $\mathcal{E}$ dans lui-même est toujours associative. En effet, soient f, g, h trois de ces applications. x étant un élément quelconque de $\mathcal{E}$, on a

$$((fg)h)(x) = (fg)(h(x)) = f(g(h(x))) = f((gh)(x)) = (f(gh))(x)$$

d'où $(fg)h = f(gh)$.

Les lois de composition <u>borne</u> et $\overline{\text{borne}}$ dans un ensemble ordonné $\mathcal{T}$ sont associatives. Soient en effet x,y,z trois éléments de $\mathcal{T}$. On est certainement dans l'un des 6 cas suivants (éventuellement dans plusieurs en même temps) : 1) $x \leqslant y \leqslant z$; 2) $x \leqslant z \leqslant y$;

3) $y \leqslant z \leqslant x$; 4) $y \leqslant x \leqslant z$; 5) $z \leqslant x \leqslant y$; 6) $z \leqslant y \leqslant x$. Dans les cas 1) et 2), les éléments $\underline{\text{borne}}\,(x,\underline{\text{borne}}\,(y,z))$ et $\underline{\text{borne}}\,(\underline{\text{borne}}\,(x,y),z)$ sont égaux à x ; dans les cas 3),4), ils sont égaux à y ; dans les cas 5) et 6), ils sont égaux à z . On a donc dans tous les cas

$$\underline{\text{borne}}\,(x,\underline{\text{borne}}\,(y,z)) = \underline{\text{borne}}\,(\,\underline{\text{borne}}\,(x,y),z)$$

ce qui prouve l'associativité de la $\underline{\text{borne}}$. Vérification analogue pour $\overline{\text{borne}}$.

Si $\mathcal{V}$ est un ensemble structuré par une loi de composition associative $\top$, la loi de composition $\top$ définie au § II dans l'ensemble des fonctions à valeurs dans $\mathcal{V}$ définies sur un ensemble $\mathcal{E}$ est également associative.

Nous laissons de même au lecteur le soin de vérifier que la juxtaposition des suites finies est une loi de composition associative.

Il est évident que toute structure induite par une structure associative est associative (nous disons qu'une structure est associative quand elle est donnée par une loi de composition associative).

De plus, toute structure quotient d'une structure associative est associative. En effet, $\mathcal{X}$, $\mathcal{Y}$, $\mathcal{Z}$ désignant trois classes, et x, y, z désignant des éléments de ces classes, la classe $(\mathcal{X} \top \mathcal{Y}) \top \mathcal{Z}$ contient $(x \top y) \top z = x \top (y \top z)$ qui est aussi élément de $\mathcal{X} \top (\mathcal{Y} \top \mathcal{Z})$. D'où $(\mathcal{X} \top \mathcal{Y}) \top \mathcal{Z} = \mathcal{X} \top (\mathcal{Y} \top \mathcal{Z})$.

On peut encore formuler autrement la condition d'associativité: à chaque $x \in \mathcal{V}$ faisons correspondre l'opérateur de composition à gauche avec x, soit $f_x(y) = x \top y$. L'application $x \longrightarrow f_x$ est une application de $\mathcal{T}$ dans l'ensemble $\mathcal{A}$ des applications de $\mathcal{T}$ dans $\mathcal{T}$. Nous considérerons $\mathcal{A}$ comme structuré par la multiplication que nous y avons définie. Dans ces conditions, l'associativité de la loi $\top$ est équivalente au fait suivant : <u>l'application</u> $x \longrightarrow f_x$ <u>est une homomorphie de</u> $\mathcal{T}$ <u>dans</u> $\mathcal{A}$. En effet, la condition d'homomorphie est $f_{x \top y} = f_x f_y$, c'est-à-dire que pour tout z, on ait $f_{x \top y}(z) = f_x(f_y(z))$ ou encore $(x \top y) \top z = x \top (y \top z)$: nous retrouvons la condition d'associativité.

Dans un ensemble $\mathcal{T}$ structuré par une loi de composition associative, on peut définir la composition de plusieurs éléments, pourvu qu'ils soient rangés dans un certain ordre. D'une manière précise donnons-nous une suite finie non vide $S = \{x_0, x_1, \dots, x_{n-1}\}$ d'éléments de $\mathcal{T}$. Définissons par récurrence sur i (pour $i \leqslant n$) un élément y_i par les formules suivantes :

$$y_0 = x_0 \qquad y_i = y_{i-1} \top x_i \qquad (0 < i \leqslant n)$$

L'élément y_n se nomme le <u>composé des éléments de la suite</u> S. On le désigne suivant les cas par l'une des notations

$$\overset{n-1}{\underset{i=0}{\top}} x \,, \qquad \underset{S}{\top} x$$

ou $x_0 \top x_1 \top \dots \top x_{n-1}$. Si la suite S est définie par une application dans $\mathcal{T}$ d'une partie finie E de l'ensemble des entiers naturels, l'élément composé se désignera par

$$\underset{i \in E}{\top} x_i$$

notation dans laquelle on pourra remplacer l'indication $i \in E$ par l'indication des conditions auxquelles doit satisfaire l'entier i pour être dans E . Si E se compose de tous les entiers i satisfaisant aux inégalités $a \leqslant i \leqslant b$, où a, b sont des entiers tels que $a \leqslant b$, l'élément composé se désigne encore par la notation

$$\mathop{\top}_{i=a}^{b} x_i$$

ou par $x_a \top x_{a+1} \top \ldots \top x_b$.

Il est à noter que le signe $\top$ que nous avons introduit ne sert qu'à noter une loi de composition arbitraire. La plupart des lois de composition que nous aurons à utiliser seront ou bien des additions (dans lesquelles le signe " + " joue le rôle que joue le signe " $\top$ " dans ce qui précède), ou bien des multiplications dans lesquelles le composé de deux éléments -leur produit- se désigne en écrivant les deux éléments à côté l'un de l'autre, avec éventuelle interposition d'un point). Dans le premier cas, le signe $\top$ sera à remplacer par le signe $\sum$, et dans le second par le signe $\prod$. S étant une suite finie, l'élément $\sum_S x$ s'appelle la <u>somme</u> des éléments de la suite et l'élément $\prod_S x$ s'appelle leur produit terme .

Signalons encore la notation suivante : si tous les éléments d'une suite finie à n termes sont égaux à un même élément x, leur composé se note quelquefois $\overbrace{x \top x \top \ldots \top x}^{n \text{ fois}}$.

$\mathcal{N}$ étant l'ensemble des entiers naturels, posons $\mathcal{N}' = \mathcal{N} - \{0\}$. La fonction

$$(1) \qquad f(n, x) = \overbrace{x \top x \top \ldots \top x}^{n \text{ fois}}$$

est une fonction définie sur $\mathcal{N}' \times \mathcal{V}$ et à valeurs dans $\mathcal{V}$: c'est une loi de composition entre éléments de $\mathcal{N}'$ et de $\mathcal{V}$.

Si $\mathcal{V} = \mathcal{N}$ et si $\top$ représente l'addition des entiers naturels, on a $f(n,x) = nx$. C'est pourquoi, quand la loi de composition $\top$ est une addition (c'est-à-dire quand elle est représentée par le signe +), on pose souvent

$$nx = f(n,x) = \overbrace{x + x + \ldots\ldots + x}^{n \text{ fois}}$$

Si $\mathcal{T} = \mathcal{N}$ et si $\top$ représente la multiplication des entiers naturels, on a $f(n,x) = x^n$. C'est pourquoi, quand la loi de composition $\top$ est une multiplication, on pose souvent

$$x^n = f(n,x) = \overbrace{x.x \ldots\ldots x}^{n \text{ fois}}$$

Dans le cas d'une loi associative $\top$ quelconque, on remarquera que, si $m, n \in \mathcal{N}'$, on a

$$(2) \qquad f(m + n,x) = f(m,x) \top f(n,x)$$

$$f(mn,x) = f(m,f(n,x))$$

comme on le vérifiera tout de suite. Ces formules donnent, dans les cas particuliers de l'addition et de la multiplication,

$$(m + n)x = mx + nx \qquad\qquad x^{m+n} = x^m x^n$$

$$mn.x = m.nx \qquad\qquad x^{mn} = (x^n)^m$$

Lorsque $\mathcal{T} = \mathcal{N}$, on retrouve des formules connues.

Notons que la définition que nous avons donnée du composé des éléments d'une suite finie s'applique que la loi de composition soit associative ou non. Mais l'intérêt de cette définition repose sur le théorème suivant, qui n'est vrai que pour les lois associatives :

<u>Théorème.</u> <u>Si une suite finie non vide S d'éléments de $\mathcal{T}$ résulte de la juxtaposition d'une suite finie</u> $\{S_0, S_1, \ldots, S_{h-1}\}$ <u>de suites finies non vides</u> $(S = S_0 S_1 \ldots S_{h-1})$, <u>on a</u>

$$\mathop{\top}_{S} x = \mathop{\top}_{i=0}^{h-1} \left(\mathop{\top}_{S_i} x \right)$$

Nous le démontrerons par récurrence sur le nombre n des éléments de S. La proposition est évidente pour $n = 1$. Supposons la démontrée pour les suites finies de n termes et soit $S = \{x_0, x_1, \ldots, x_n\}$ une suite finie de $n + 1$ termes, résultant de la juxtaposition de la suite $\{S_0, S_1, \ldots, S_{h-1}\}$.

Soient S' la suite à n termes $\{x_0, x_1, \ldots, x_{n-1}\}$ et S'' la suite à 1 terme $\{x_n\}$. On a $S = S'S''$. Distinguons deux cas :

a) On a $S_{h-1} = S''$. Dans ce cas S' résulte de la juxtaposition de la suite de suites $\{S_0, S_1, \ldots, S_{h-2}\}$. On a donc

$$\mathop{\top}\limits_{S} x = \Big(\mathop{\top}\limits_{S'} x\Big) \top x_n = \Big(\mathop{\top}\limits_{i=0}^{h-2}\Big(\mathop{\top}\limits_{S_i} x\Big)\Big) \top \Big(\mathop{\top}\limits_{S_{h-1}} x\Big) = \mathop{\top}\limits_{i=0}^{h-1}\Big(\mathop{\top}\limits_{S_i} x\Big)$$

b) On a $S_{h-1} \neq S''$. Dans ce cas S_{h-1} se met sous la forme $S'_{h-1}S''$, S'_{h-1} étant une nouvelle suite finie non vide. La suite S' résulte de la juxtaposition de la suite de suites $\{S_0, S_1, \ldots, S_{h-2}, S'_{h-1}\}$ et on a

$$\mathop{\top}\limits_{S} x = \Big(\mathop{\top}\limits_{S'} x\Big) \top x_n = \Big(\Big(\mathop{\top}\limits_{i=0}^{h-2}\Big(\mathop{\top}\limits_{S_i} x\Big)\Big) \top \Big(\mathop{\top}\limits_{S'_{h-1}} x\Big)\Big) \top x_n$$

qui s'écrit encore, en vertu de l'associativité

$$\Big(\mathop{\top}\limits_{i=0}^{h-2}\Big(\mathop{\top}\limits_{S_i} x\Big)\Big) \top \Big(\Big(\mathop{\top}\limits_{S'_{h-1}} x\Big) \top x_n\Big) = \Big(\mathop{\top}\limits_{i=0}^{h-2}\Big(\mathop{\top}\limits_{S_i} x\Big)\Big) \top \Big(\mathop{\top}\limits_{S_{h-1}} x\Big) = \mathop{\top}\limits_{i=0}^{h-1}\Big(\mathop{\top}\limits_{S_i} x\Big)$$

ce qui démontre le théorème.

On remarquera d'autre part que si $f(x)$ est une homomorphie d'un ensemble $\mathcal{V}$ structuré par une loi de composition $\top$ dans un ensemble $\mathcal{Z}$ structuré par une loi de composition $\perp$, on a

$$f(x_0 \top x_1 \top \ldots \top x_{n-1}) = f(x_0) \perp f(x_1) \perp \ldots \perp f(x_{n-1})$$

<u>Application</u>. $\mathcal{V}$ étant l'ensemble des suites finies d'éléments d'un ensemble $\mathcal{E}$, structuré par la juxtaposition, il est clair que l'application de $\mathcal{V}$ sur l'ensemble des entiers naturels qui à chaque suite S fait correspondre son nombre de termes $n(S)$ est une homomorphie de $\mathcal{V}$ sur l'ensemble des entiers naturels structuré au moyen de l'addition. Il en résulte que : <u>si une suite finie</u> S

<u>résulte de la juxtaposition d'une suite finie de suites finies</u> $\{S_0, S_1, \ldots, S_{h-1}\}$ <u>on a</u> $n(S) = \sum_{i=0}^{h-1} n(S_i)$.

§ IV. ÉLÉMENT UNITÉ

$\mathcal{V}$ étant un ensemble structuré par une loi de composition $\top$, on dit qu'un élément $e \in \mathcal{V}$ est élément unité par rapport à la loi de composition $\top$ si on a, pour tout $x \in \mathcal{V}$,

$$e \top x = x \top e = x$$

Par exemple : le nombre 0 est élément unité pour l'addition des entiers naturels ; le nombre 1 est élément unité pour la multiplication des entiers naturels. $\mathcal{E}$ étant un ensemble quelconque l'application identique e définie par $e(x) = x$ (pour $x \in \mathcal{E}$) est élément unité de la multiplication des applications de $\mathcal{E}$ dans $\mathcal{E}$. L'exponentiation des entiers naturels n'a pas d'élément unité.

$\mathcal{V}$ étant un ensemble ordonné, s'il a un plus grand élément e, e est élément unité pour la loi de composition <u>borne</u> (x, y) ; sinon, cette loi de composition n'a pas d'élément unité. De même, le plus petit élément (s'il existe) est élément unité pour la loi de composition $\overline{\text{borne}}$ (x, y).

Si un ensemble $\mathcal{V}$ est structuré par une loi de composition $\top$ qui comporte un élément unité e, l'ensemble $\mathcal{F}$ des fonctions définies sur un ensemble $\mathcal{E}$ et à valeurs dans $\mathcal{V}$, structuré par la loi de composition $\top$ que nous y avons définie au § I, possède pour élément unité ϵ la fonction $\epsilon(x)$ définie par $\epsilon(x) = e$ (pour tout $x \in \mathcal{E}$).

<u>Il existe dans $\mathcal{V}$ au plus un élément unité.</u> En effet, supposons que chacun des éléments e, e' soit élément unité.

On a $\qquad e = e \top e' = e'$.

D'autre part, on remarquera que, si e est élément unité, les opérateurs $f_e(x) = e \top x$, $g_e(x) = x \top e$ de composition à gauche et à droite avec e sont tous deux égaux à l'application identique de $\mathcal{T}$ dans $\mathcal{T}$. Inversement cette propriété caractérise l'élément unité.

Lorsque $\mathcal{T}$ comporte un élément unité e, il est commode d'étendre la définition du composé des éléments d'une suite finie au cas où la suite est une suite à 0 terme (suite vide) : par définition, le composé de la suite vide sera e. Le théorème du § précédent reste valable (pour les lois associatives) sans supposer les suites non vides avec cette nouvelle convention, comme le lecteur s'en assurera facilement.

De plus, la définition de la fonction $f(n,x)$ par la formule (1) du § III peut s'étendre au cas $n = 0$, en posant $f(0,x) = e$. Les formules (2) restent valables dans le cas où n ou m est nul.

Si une partie A de $\mathcal{T}$ est fermée par rapport à la loi de composition dans $\mathcal{T}$ et si $e \in A$, e est encore élément unité de la structure induite par $\mathcal{T}$ sur A. Mais il convient de remarquer que, si $e \notin A$, il peut se produire que la structure induite sur A comporte un élément unité autre que e.

Si $\mathcal{F}$ est une structure quotient de $\mathcal{T}$ et si $\mathcal{T}$ comporte un élément unité e, $\mathcal{F}$ possède également un élément unité, qui est la classe $\mathfrak{n}$ qui contient e. De plus, $\mathfrak{n}$, considéré comme partie de $\mathcal{T}$, est fermé par rapport à la composition dans $\mathcal{T}$. En effet, en désignant par "$x \equiv y$" la relation de congruence qui définit la structure quotient $\mathcal{F}$, les conditions $x \equiv e$, $y \equiv e$ entraînent $x \top y \equiv e \top e = e$, d'où $x \top y \in \mathfrak{n}$.

__Convention de notations__. Si la loi de composition $\top$ est une addition (donc, si elle est représentée par le signe $+$), son élément unité, si elle en a un, se désigne généralement par 0 ; si elle est une multiplication, il se désigne généralement par 1. Il faut cependant prendre garde à ne pas confondre ces signes avec les nombres naturels correspondants.

§ __V__. __ÉLÉMENTS INVERSES__. __ÉLÉMENTS RÉGULIERS__.

Soit $\mathcal{T}$ un ensemble structuré par une loi de composition associative pour laquelle existe un élément-unité e.

x __étant un élément de__ $\mathcal{T}$, __on appelle inverse de__ x __un élément__ x' __tel que l'on ait__

$$x \top x' = x' \top x = e \;.$$

Un élément x possède au plus un inverse. Supposons en effet que x' et x" soient chacun inverse de x. On a

$$x'' = x'' \top e = x'' \top x \top x' = e \top x' = x'$$

Exemples : pour l'addition des entiers naturels, seul 0 a un inverse, qui est 0 ; pour la multiplication des entiers naturels, seul 1 a un inverse qui est 1, d'une manière général, l'élément unité est toujours son propre inverse. Dans la multiplication des applications bi-univoques d'un ensemble $\mathcal{E}$ sur lui-même, les éléments qui ont des inverses sont les applications bi-univoques de $\mathcal{E}$ sur lui-même, ou permutations de $\mathcal{E}$: f(x) étant une permutation de $\mathcal{E}$, son inverse est la fonction réciproque $\overset{-1}{f}(x)$.

$\mathcal{T}$ étant un ensemble ordonné, structuré par l'une des lois de composition __borne__, $\overline{\text{borne}}$, seul l'élément unité, s'il existe, possède un inverse.

21

Généralisant la notation relative à ce dernier exemple, nous noterons ici l'inverse d'un élément x quand il existe par $\overset{-1}{x}$. Il convient de faire remarquer que si la loi de composition est une addition, l'élément inverse de x se note $-x$ et s'appelle l'opposé de x. Lorsque la loi de composition est une multiplication on emploie concuremment avec la notation $\overset{-1}{x}$ la notation x^{-1}.

Désignons par $f_x(y) = x \top y$ et $g_x(y) = y \top x$ les applica--tions de $\mathcal{T}$ dans lui-même produites par un élément x. Nous avons le théorème suivant :

Théorème. Si x possède un inverse, les applications $f_x(y)$, $g_x(y)$ sont des permutations de $\mathcal{T}$. Inversement, la loi de composition étant supposée associative, si, pour un élément x, les applications $f_x(y)$, $g_x(y)$ sont des permutations de $\mathcal{T}$, $\mathcal{T}$ comporte un élément unité et x a un inverse dans $\mathcal{T}$.

En effet 1) si x a un inverse $\overset{-1}{x}$, on a $\overset{-1}{x} \top f_x(y) = y$ et $g_x(y) \top \overset{-1}{x} = y$. Il en résulte que, a étant un élément quelconque de $\mathcal{T}$, il existe un élément y et un seul tel que $f_x(y) = a$, à savoir $y = \overset{-1}{x} \top a$, et qu'il existe un élément y' et un seul tel que $g_x(y') = a$, à savoir $y' = a \top \overset{-1}{x}$. Les applications $f_x(y), g_x(y)$ sont donc des permutations de $\mathcal{T}$; 2) supposons qu'il existe un élément x tel que f_x et g_x soient des permutations de $\mathcal{T}$. Il existe donc un élément $a \in \mathcal{T}$ tel que $f_x(e) = x$, d'où $x \top e = x$. y étant un élément quelconque de $\mathcal{T}$, il existe un élément $z \in \mathcal{T}$ tel que $y = g_x(z)$, d'où $y = z \top x$, et $y \top e = z \top x \top e = z \top x = y$. On voit de même qu'il existe un élément $f \in \mathcal{T}$ tel que, pour tout $y \in \mathcal{T}$, on sait $f \top y = y$. On en déduit $e = f \top e = f$: l'élément $e = f$ est élément unité de $\mathcal{T}$. De plus, il existe un élément x' tel que $f_x(x') = e$, d'où $x \top x' = e$. On a $x \top x' \top x = e \top x = x$. Les égalités $x \top (x' \top x) = x$, $x \top e = x$ entraînent, puisque f_x est bi-univoque, $x' \top x = e$: x' est l'inverse de x, ce qui démontre le théorème.

Il y a intérêt à considérer les éléments x pour lesquels les applications f_x, g_x, sans être nécessairement des permutations de $\mathcal{T}$, sont des applications bi-univoques de $\mathcal{T}$ dans $\mathcal{T}$: ces éléments sont appelés *réguliers* (par rapport à la loi de composition $\top$). Par exemple, tout entier naturel est régulier par rapport à l'addition des entiers naturels ; tout entier naturel sauf 0 est régulier par rapport à la multiplication des entiers naturels.

$\mathcal{T}$ étant un ensemble ordonné structuré par l'une des lois de composition *borne*, $\overline{\text{borne}}$, seul l'élément unité, s'il existe, est régulier.

x étant un élément régulier par rapport à la loi de composition $\top$, on a la propriété suivante : x' et x'' étant des éléments de $\mathcal{T}$, l'égalité $x \top x' = x \top x''$ entraîne $x' = x''$ et il en est de même de l'égalité $x' \top x = x'' \top x$. Inversement cette propriété caractérise les éléments réguliers. On l'exprime en disant que l'on peut simplifier par x des égalités telles que celles que nous avons écrites.

Si A *est une partie de* $\mathcal{T}$ *fermée par rapport à la composition dans* $\mathcal{T}$, *tout élément de* A *qui est régulier dans* $\mathcal{T}$ *est aussi régulier dans la structure induite sur* A. En effet, les applications de A dans lui-même produites par cet élément sont bi-univoques.

Si l'élément x *en question a un inverse dans* $\mathcal{T}$ *et si* $x^{-1} \in A$ *on a aussi* $e \in A$ *et* x^{-1} *est l'inverse de* x *dans la structure induite sur* A

En effet, la formule $e = x \top \overset{-1}{x}$ jointe aux conditions $x \in A$ $\overset{-1}{x} \in A$ entraîne $e \in A$, et $\overset{-1}{x}$ est évidemment l'inverse de x dans A.

<u>L'ensemble</u> R <u>de tous les éléments réguliers de</u> $\mathcal{T}$ <u>est une partie de</u> $\mathcal{T}$ <u>fermée par rapport à la loi de composition, et il en est de même de l'ensemble</u> I <u>des éléments qui ont des inverses</u>.

En effet, soient x, y des éléments de $\mathcal{T}$. En vertu de l'associativité, on a $f_{x \top y} = f_x f_y$ et $g_{x \top y} = g_y g_x$. Si $x, y \in R$, f_x, f_y, g_x, g_y sont des applications bi-univoques. Il en est encore de même de $f_x f_y$ et de $g_y g_x$. Si x, $y \in I$, f_x, f_y, g_x, g_y sont des permutations, et il en est encore de même de $f_x f_y$ et de $g_y g_x$.

La structure induite sur R est une structure dans laquelle tout élément est régulier. Si on remarque que l'inverse de l'inverse d'un élément x n'est autre que x, on voit que la structure induite sur I est une structure dans laquelle tout élément a un inverse.

x et y étant deux éléments de I, l'inverse de $x \top y$ est $\overset{-1}{y} \top \overset{-1}{x}$. En effet, on a $x \top y \top \overset{-1}{y} \top \overset{-1}{x} = x \top e \top \overset{-1}{x} = e$, et $\overset{-1}{y} \top \overset{-1}{x} \top x \top y = \overset{-1}{y} \top e \top y = e$. D'une manière générale, si $\{x_0, x_1, \ldots, x_{n-1}\}$ est une suite finie d'éléments de I, l'inverse du composé $x_0 \top x_1 \top \ldots\ldots \top x_{n-1}$ est $\overset{-1}{x}_{n-1} \top \ldots \top \overset{-1}{x}_1 \top \overset{-1}{x}_0$: <u>pour prendre l'inverse du composé de plusieurs éléments, il faut prendre le composé des inverses, en les rangeant dans l'ordre inverse de celui des éléments donnés</u>.

Si maintenant nous considérons une structure quotient $\mathcal{F}$ et $\mathcal{T}$, nous avons le résultat suivant : <u>si un élément</u> x <u>de</u> $\mathcal{T}$ <u>a un inverse dans</u> $\mathcal{T}$, <u>sa classe</u> $\mathfrak{x}$ <u>a un inverse dans</u> $\mathcal{F}$. En effet, si $\mathfrak{x}'$ est la classe qui contient $\overset{-1}{x}$ et si $\mathfrak{e}$ est la classe unité de $\mathscr{F}$, on a $\mathscr{C} \mathrm{T} \mathscr{C}' = \mathscr{u} = \mathscr{C}' \mathrm{T} \mathscr{C}$. Par contre, il peut arriver que x soit régulier dans $\mathscr{E}$ sans que sa classe soit régulière dans $\mathscr{F}$.

<u>Convention de notations</u>. Nous avons déjà dit que, quand la loi de composition T est une addition, l'élément inverse, ou opposé, d'un élément y (s'il existe) se note -y. D'une manière générale, on pose

$$x - y = x + (-y)$$

x-y est donc le seul élément z tel que l'on ait $x = z + y$. On notera que, y et z étant supposés avoir des opposés, on a

$$x-(y + z) = (x-y)-z$$

$$x + (y-z) = (x + y)-z$$

$$x-(y-z) = (x-y) + z \qquad \text{etc. etc.}$$

Il n'y a du reste aucun inconvénient à supprimer les parenthèses aux seconds membres des formules que nous venons d'écrire.

§ <u>VI</u>. <u>GROUPES</u>.

Définition. <u>On appelle groupe un ensemble $\mathscr{G}$ structuré par une loi de composition associative T qui comporte un élément unité</u> e <u>et dans lequel tout élément possède un inverse</u>.

Par exemple, l'ensemble des permutations d'un ensemble $\mathscr{E}$ structuré par la multiplication des applications de $\mathscr{E}$ dans $\mathscr{E}$ constitue un groupe : le groupe des permutations de $\mathscr{E}$. Deux ensembles de même puissance ont évidemment des groupes de permutation isomorphes.

Si $\mathscr{G}$ est un groupe (avec la loi T) et $\mathscr{E}$ un ensemble quelconque, l'ensemble $\mathscr{F}$ des fonctions définies sur $\mathscr{E}$ et à valeurs dans $\mathcal{G}$, structuré au moyen de la loi de composition $\top$ définie au § II, forme un groupe. En effet, nous savons déjà que la loi de composition dans $\mathcal{F}$ est associative et comporte un élément unité ε. f désignant un élément quelconque de f, soit f' la fonction définie de la manière suivante : pour tout $x \in \mathcal{E}$, $f'(x)$ est l'inverse de $f(x)$. On a $f \top f' = f' \top f = \varepsilon$: f' est l'inverse de f par rapport à la loi $\top$. f' se désigne généralement par f^{-1} : ne pas confondre avec $\overset{-1}{f}$.

$\mathcal{G}$ étant un groupe, et $\mathfrak{g}$ une partie de $\mathcal{G}$ fermée par rapport à la composition dans $\mathcal{G}$, la structure induite sur $\mathfrak{g}$ n'est pas en général une structure de groupe. S'il en est cependant ainsi, $\mathfrak{g}$, muni de sa structure induite, sera appelé un <u>sous-groupe</u> de $\mathcal{G}$.

<u>$\mathfrak{g}$ étant une partie non vide de $\mathcal{G}$, la condition nécessaire et suffisante pour que $\mathfrak{g}$ soit un sous-groupe est que les conditions</u> $x \in \mathfrak{g}$, $y \in \mathfrak{g}$ <u>entraînent</u> $x \top \overset{-1}{y} \in \mathfrak{g}$.

La condition est évidemment nécessaire. Inversement, supposons la remplie. $\mathfrak{g}$ n'étant pas vide contient au moins un élément x_0. On a $e = x_0 \top \overset{-1}{x_0} \in \mathfrak{g}$; x étant un élément quelconque de $\mathfrak{g}$, on a $\overset{-1}{x} = e \top \overset{-1}{x} \in \mathfrak{g}$; x et y désignant deux éléments de $\mathfrak{g}$, soit $z = \overset{-1}{y}$; on a $z \in \mathfrak{g}$, d'où $x \top y = x \top \overset{-1}{z} \in \mathfrak{g}$. Donc $\mathfrak{g}$ est fermé par rapport à la composition dans $\mathcal{G}$; comme de plus $\mathfrak{g}$ contient l'inverse de tout élément de $\mathfrak{g}$, $\mathfrak{g}$ est un sous-groupe.

<u>Toute structure quotient d'un groupe est un groupe.</u>

Nous avons vu déjà que la loi de composition dans une structure quotient d'un groupe est associative et comporte un élément unité ;

de plus, tout élément du groupe ayant un inverse dans le groupe, il en résulte que toute classe de la structure quotient a une inverse : la structure quotient est un groupe.

Les groupes que l'on obtient ainsi à partir d'un groupe $\mathcal{G}$ sont appelés les <u>groupes-quotient</u> de $\mathcal{G}$.

Il existe des relations remarquables entre les groupes quotient et les sous-groupes d'un groupe $\mathcal{G}$. En effet :

<u>$\mathcal{H}$ étant un groupe quotient de $\mathcal{G}$, la classe unité $\mathfrak{g}$ de $\mathcal{H}$ est un sous-groupe de $\mathcal{G}$.</u>

En effet, nous savons déjà que $\mathfrak{g}$ est fermé par rapport à la composition dans $\mathcal{G}$. D'autre part, soit x un élément de $\mathfrak{g}$; si $\mathfrak{g}'$ est la classe qui contient x^{-1}, on a $\mathfrak{g} \top \mathfrak{g}' = \mathfrak{g}' \top \mathfrak{g} = \mathfrak{g}$; donc on a $\mathfrak{g}' = \mathfrak{g}$, ce qui montre que $x^{-1} \in \mathfrak{g}$, et que par suite $\mathfrak{g}$ est un sous-groupe.

<u>De plus, la relation de congruence qui définit $\mathcal{H}$ est entièrement déterminée par la donnée de $\mathfrak{g}$</u>. Soit en effet "$x \equiv y$" cette relation de congruence. x et y étant deux éléments de $\mathcal{G}$, soient $\mathscr{X}$, $\mathscr{Y}$ leurs classes. La relation "$x \equiv y$" est équivalente à "$\mathscr{X} = \mathscr{Y}$" qui est elle-même équivalente à chacune des relations "$\mathscr{X} \top \mathscr{Y}^{-1} = \mathfrak{g}$", "$\mathscr{X}^{-1} \top \mathscr{Y} = \mathfrak{g}$". La première de ces relations est équivalente à "$x \top y^{-1} \in \mathfrak{g}$" et la seconde à "$x^{-1} \top y \in \mathfrak{g}$". Il en résulte que la relation "$x \equiv y$" est équivalente à chacune des relations "$x \top y^{-1} \in \mathfrak{g}$", "$x^{-1} \top y \in \mathfrak{g}$", ce qui prouve notre assertion.

Le groupe quotient lui-même est donc déterminé par la donnée de $\mathfrak{g}$. On l'appelle le groupe quotient de $\mathcal{G}$ par $\mathfrak{g}$ et on le désigne par $\mathcal{G}/\mathfrak{g}$. La relation de congruence qui le détermine s'appelle "congruence modulo $\mathfrak{g}$". On la note "$x \equiv y \pmod{\mathfrak{g}}$".

Inversement, $\mathfrak{g}$ étant un sous-groupe, chacune des relations "$x \top \overset{-1}{y} \in \mathfrak{g}$", "$\overset{-1}{x} \top y \in \mathfrak{g}$" est une relation d'équivalence. En effet : a) $x \top \overset{-1}{x} = e \in \mathfrak{g}$ est une relation vraie pour tout élément de $\mathcal{G}$; b) la condition $z = x \top \overset{-1}{y} \in \mathfrak{g}$ entraîne $y \top \overset{-1}{x} = \overset{-1}{z} \in \mathfrak{g}$; c) les conditions $x \top \overset{-1}{y} \in \mathfrak{g}$, $y \top \overset{-1}{z} \in \mathfrak{g}$ entraînent $x \top \overset{-1}{z} = x \top \overset{-1}{y} \top y \top \overset{-1}{z} \in \mathfrak{g}$ (démonstrations analogues pour la seconde des relations citées). La première des relations en question est compatible avec la composition à droite avec les éléments de $\mathcal{G}$. En effet les conditions $x \top \overset{-1}{y} \in \mathfrak{g}$, $x' \in \mathcal{G}$ entraînent $(x \top x') \top \overset{-1}{\overline{(y \top x')}} = x \top x' \top \overset{-1}{x'} \top \overset{-1}{y} = x \top \overset{-1}{y} \in \mathfrak{g}$. On verrait de même que la seconde des relations est compatible avec la composition à gauche avec les éléments de $\mathcal{G}$. Mais, en général, aucune de ces relations n'est une relation de congruence, de sorte que si $\mathfrak{g}$ est un sous-groupe quelconque, il ne définit pas en général un groupe quotient $\mathcal{G}/\mathfrak{g}$.

Si $\mathfrak{g}$ est la classe unité d'un groupe quotient, nous avons vu que les relations "$x \top \overset{-1}{y} \in \mathfrak{g}$", "$\overset{-1}{x} \top y \in \mathfrak{g}$" sont équivalentes. Inversement, supposons cette dernière condition vérifiée. Alors chacune de ces relations est une relation de congruence. En effet, puisque l'une est compatible avec la composition à droite et l'autre avec la composition à gauche, leur équivalence entraîne que chacune est une relation de congruence. Cette relation de congruence définit alors un groupe quotient, dont $\mathfrak{g}$ est la classe unité.

Définition. <u>On appelle normal un sous-groupe $\mathfrak{g}$ de $\mathcal{G}$ quand les relations</u> "$x \top \overset{-1}{y} \in \mathfrak{g}$", "$\overset{-1}{x} \top y \in \mathfrak{g}$" <u>sont équivalentes.</u>

Il en résulte qu'il existe une correspondance bi-univoque entre les sous-groupes normaux d'un groupe $\mathcal{G}$ et les groupes quotient de $\mathcal{G}$.

On peut donner une autre forme à la condition de normalité. En effet, $\mathfrak{g}$ étant un groupe normal, soient z un élément de $\mathfrak{g}$ et x un élément de $\mathcal{G}$. On a $x \top z \top x^{-1} \in \mathfrak{g}$: en effet, si $\mathcal{C}$ est la classe de $\mathcal{G}/\mathfrak{g}$ qui contient x, la classe de $x \top z \top x^{-1}$ est $\mathcal{C} \top \mathfrak{g} \top \mathcal{C}^{-1} = \mathfrak{g}$. Inversement, si les conditions $z \in \mathfrak{g}$, $x \in \mathcal{G}$ entraînent $x \top z \top x^{-1} \in \mathfrak{g}$, elles entraînent aussi $x^{-1} \top z \top x \in \mathfrak{g}$; $\mathfrak{g}$ est alors un sous-groupe normal. En effet, la condition $x \top y^{-1} \in \mathfrak{g}$ $(x, y \in \mathcal{G})$ entraîne $y^{-1} \top x = x^{-1} \top (x \top y^{-1}) \top x \in \mathfrak{g}$ et aussi $x^{-1} \top y \in \mathfrak{g}$; la condition $x^{-1} \top y \in \mathfrak{g}$ entraîne $y \top x^{-1} = x \top (x^{-1} \top y) \top x^{-1} \in \mathfrak{g}$ et aussi $x \top y^{-1} \in \mathfrak{g}$. Donc :

<u>La condition nécessaire et suffisante pour que le sous-groupe</u> $\mathfrak{g}$ <u>soit normal est que les conditions</u> $z \in \mathfrak{g}$, $x \in \mathcal{G}$ <u>entraînent</u> $x \top z \top x^{-1} \in \mathfrak{g}$.

$\mathfrak{g}$ étant un sous-groupe normal de $\mathcal{G}$, considérons un groupe quotient de $\mathcal{G}/\mathfrak{g}$ par un sous-groupe normal $\bar{\mathfrak{f}}$ de $\mathcal{G}/\mathfrak{g}$. Si $\mathfrak{f}$ est la réunion des classes (mod. $\mathfrak{g}$) qui sont éléments de $\bar{\mathfrak{f}}$, on voit facilement que $\mathfrak{f}$ est un sous-groupe normal de $\mathcal{G}$. D'ailleurs, les relations $\mathcal{C} \top \mathcal{Y}^{-1} \in \bar{\mathfrak{f}}$ et $x \top y^{-1} \in \mathfrak{f}$ se correspondent par le schéma de correspondance établi au § I. Il en résulte que les groupes $(\mathcal{G}/\mathfrak{g})/\bar{\mathfrak{f}}$ et $\mathcal{G}/\mathfrak{f}$ sont isomorphes. D'autre part, les groupes $\mathfrak{f}/\mathfrak{g}$ et $\bar{\mathfrak{f}}$ sont identiques.

Inversement, si $\mathfrak{f}$ est un sous-groupe normal de $\mathcal{G}$ contenant $\mathfrak{g}$, et si $\bar{\mathfrak{f}} = \mathfrak{f}/\mathfrak{g}$, $\bar{\mathfrak{f}}$ est un sous-groupe normal de $\mathcal{G}/\mathfrak{g}$

(cf. § I), et les groupes $\mathcal{G}/\mathcal{H}$, $(\mathcal{G}/\mathfrak{g})/\bar{\mathcal{H}}$ sont isomorphes.

Si $\mathcal{H}$ est un sous-groupe normal ou non de $\mathcal{G}$ contenant $\mathfrak{g}$, on voit facilement que $\mathcal{H}/\mathfrak{g}$ est un sous-groupe de $\mathcal{G}/\mathfrak{g}$, ce qui établit une correspondance bi-univoque entre les sous-groupes de $\mathcal{G}/\mathfrak{g}$ et les sous-groupes de $\mathcal{G}$ qui contiennent $\mathfrak{g}$.

L'intersection d'une famille quelconque de sous-groupes d'un groupe $\mathcal{G}$ est évidemment un sous-groupe de $\mathcal{G}$. L'intersection $\mathfrak{g}$ de tous les sous-groupes qui contiennent une partie B de $\mathcal{G}$ s'appelle le sous-groupe engendré par les éléments de B ; on dit aussi que les éléments de B forment un système de générateurs de $\mathfrak{g}$. Il faut se garder de confondre cette notion avec celle de la plus petite fermée par rapport à la loi de composition contenant B. Le rapport entre ces deux notions est précisé par l'assertion suivante :

Assertion. <u>Si les éléments de</u> B <u>forment un système de générateurs du sous-groupe</u> $\mathfrak{g}$, $\mathfrak{g}$ <u>est la plus petite partie fermée par rapport à la loi de composition qui contienne les éléments de</u> B <u>et leurs inverses</u>.

Cette assertion découle immédiatement de la précédente.

§ VII. COMMUTATIVITÉ.

Soit $\mathcal{T}$ un ensemble structuré par une loi de composition $\top$. Cette loi de composition est dite <u>commutative</u> si, x et y désignant des éléments quelconques de $\mathcal{T}$, on a

$$x \top y = y \top x$$

Par exemple, l'addition et la multiplication des entiers naturels sont des lois de composition commutatives.

Si $\mathcal{T}$ est un ensemble ordonné, les lois de composition $\underline{\text{borne}}$ et $\overline{\text{borne}}$ sont commutatives :

$$\underline{\text{borne}}\,(x,y) = \underline{\text{borne}}\,(y,x) \; ; \; \overline{\text{borne}}\,(x,y) = \overline{\text{borne}}\,(y,x)$$

La commutativité peut encore s'exprimer de la manière suivante : <u>Les deux applications</u> ~~f(x)~~ $f_x(y) = x \top y$, $g_x(y) = y \top x$ <u>de</u> $\mathcal{T}$ <u>dans lui-même qui sont produites par un élément</u> $x \in \mathcal{T}$ <u>sont égales</u>.

Nous supposerons à partir de maintenant que nous avons affaire à une loi de composition commutative et associative.

On notera que dans ce cas les propriétés pour une partie de $\mathcal{T}$ d'être invariante à gauche ou à droite par la composition avec les éléments de $\mathcal{T}$ sont équivalentes. De même, la propriété pour une relation d'équivalence d'être compatible avec la composition à gauche ou à droite avec les éléments de $\mathcal{T}$ sont équivalentes. Toute relation d'équivalence qui possède l'une de ces propriétés est une relation de congruence par rapport à la loi de composition considérée.

Si A est une partie de $\mathcal{T}$ fermée par rapport à la composition dans $\mathcal{T}$, la structure induite sur A est une structure commutative (nous appelons commutative une structure définie par une loi de composition commutative).

De même, on voit que toute structure quotient d'une structure commutative est une structure commutative.

<u>Convention de notations</u>. Si un ensemble $\mathcal{T}$ est structuré par une multiplication associative et commutative, et si un élément y possède un inverse y^{-1}, cet inverse se désigne souvent par $\frac{1}{y}$ (1 représentant, suivant nos conventions, l'élément unité). De même, x étant un élément quelconque de l'ensemble, xy^{-1} se note souvent $\frac{x}{y}$.

Si y' est un nouvel élément pourvu d'un inverse, et x' un nouvel élément quelconque, on a

$$\frac{xx'}{yy'} = \frac{x}{y}\frac{x'}{y'} \qquad \frac{xy'}{yy'} = \frac{x}{y}$$

Si x possède lui-même un inverse, l'inverse de $\frac{x}{y}$ est $\frac{y}{x}$. On devra éviter soigneusement d'employer cette notation, dite fractionnaire, dans le cas d'une loi de composition non commutative.

D'autre part, nous allons montrer que la commutativité s'étend à la composition de plusieurs éléments. D'une manière précise, S et S' désignant deux suites finies $\{u_0, u_1, \ldots, u_{n-1}\}$ et $\{u'_0, u'_1, \ldots, u'_{n-1}\}$ d'éléments de $\mathcal{T}$, ayant même nombre n de termes, nous dirons que ces suites "<u>ne diffèrent que par l'ordre des termes</u>" lorsqu'il existe une permutation $f(k)$ de la section I_n de l'ensemble des entiers naturels telle que l'on ait

$$u'_k = u_{f(k)} \qquad (\text{si } k \in I_n).$$

Le fait de ne différer que par l'ordre des termes constitue évidemment une relation entre les suites S et S' : nous noterons cette relation par le symbole "$S \sim S'$" (nous montrerons tout à l'heure que c'est une relation d'équivalence).

Nous allons maintenant démontrer le théorème suivant :

Théorème. <u>Si les suites</u> $S = \{u_0, u_1, \ldots, u_{n-1}\}$ <u>et</u> $S' = \{u'_0, u'_1, \ldots, u'_{n-1}\}$ <u>ne diffèrent que par l'ordre des termes, on a</u>

$$\prod_{i=0}^{n-1} u_i = \prod_{i=0}^{n-1} u'_i$$

Nous démontrerons la proposition par récurrence sur n (qui est nécessairement $\geqslant 1$). Elle est évidente pour $n = 1$; supposons la démontrée pour tous les couples de suites ne différant que par l'ordre des termes et dont les nombres de termes soient $< n$, n étant un entier $\geqslant 1$. S et S' étant les deux suites de l'énoncé, il existe une permutation f de I_n telle que l'on ait

$$u'_k = u_{f(k)} \qquad (k \in I_n)$$

Posons $a = f(n-1)$. Les suites $S_1 = \{u_i\}_{i<n-1}$ et $S'_1 = \{u'_i\}_{i\neq a}$ sont des suites à n-1 termes qui ne diffèrent évidemment que par l'ordre de leurs termes. D'où

$$\mathop{\top}\limits_{i=0}^{n-2} u_i = \mathop{\top}\limits_{i\neq a} u'_i = \Big(\mathop{\top}\limits_{i<a} u'_i\Big) \top \Big(\mathop{\top}\limits_{i>a} u'_i\Big)$$

et

$$\mathop{\top}\limits_{i=0}^{n-1} u_i = \Big(\mathop{\top}\limits_{i=0}^{n-2} u_i\Big) \top u_{n-1} = \Big(\Big(\mathop{\top}\limits_{i<a} u'_i\Big) \top \Big(\mathop{\top}\limits_{i>a} u'_i\Big)\Big) \top u_{n-1} =$$

$$= \mathop{\top}\limits_{i<a} u'_i \top \Big(\Big(\mathop{\top}\limits_{i>a} u'_i\Big) \top u'_a\Big) = \Big(\mathop{\top}\limits_{i<a} u'_i\Big) \top u'_a \top \Big(\mathop{\top}\limits_{i>a} u'_i\Big) = \mathop{\top}\limits_{i=0}^{n-1} u'_i$$

ce qui démontre le théorème pour les suites S, S'.

On remarquera que la relation "$S \sim S'$" est une relation d'équivalence entre suites finies. En effet : a) il est clair que l'on a toujours $S \sim S$; b) soit $S \sim S'$, $S = \{u_0, u_1, \ldots, u_{n-1}\}$, $S' = \{u'_0, u'_1, \ldots, u'_{n-1}\}$, $u'_k = u_{f(k)}$ où f est une permutation de I_n. f^{-1} est aussi une permutation de I_n, et on a $u_k = u'_{f^{-1}(k)}$ d'où $S' \sim S$; c) supposons qu'on ait en outre $S' \sim S''$, S'' étant une troisième suite finie $\{u''_0, u''_1, \ldots, u''_{n-1}\}$, avec $u''_k = u'_{g(k)}$, g étant une permutation de I_n. On a $u''_k = u_{g(f(k))}$ et gf est encore une permutation de I_n ; d'où $S \sim S''$.

La relation "$S \sim S'$" définit donc un partage en classe de l'ensemble des suites finies d'éléments de $\mathcal{T}$.

Définition. *On appelle système fini d'éléments de $\mathcal{T}$ une classe de suites finies ne différant les unes des autres que par l'ordre de leurs termes.*

Nous venons de démontrer que, pour une suite finie S non vide, la valeur de l'élément $\top_{S} x$ ne dépend que du système fini U auquel appartient S . On peut donc désigner cet élément par $\top_{U} x$: on l'appelle le composé des éléments du système U.

La relation d'équivalence "$S \sim S'$" est une relation de congruence par rapport à la juxtaposition des suites S : le lecteur vérifiera en effet facilement que les conditions $S \sim S'$, $T \sim T'$ entraînent $ST \sim S'T'$. Il en résulte que l'ensemble $\mathcal{U}$ des systèmes finis d'éléments de $\mathcal{V}$ peut-être considéré comme une structure-quotient de l'ensemble des suites finies, structuré par la juxtaposition. L'ensemble $\mathcal{U}$ comporte donc une loi de composition, qu'on appelle encore juxtaposition, et que nous désignerons additivement par le signe + : U et V étant des systèmes finis, U + V sera le système fini qui contient toutes les suites ST pour $S \in U$, $T \in V$.

D'autre part, on voit facilement que, S et T étant deux suites finies, on a $ST \sim TS$. Il en résulte que $U + V = V + U$: la juxtaposition des systèmes finis est une loi de composition commutative.

On désigne généralement un système fini en donnant l'une des suites qui le composent. Ainsi, on parlera du système fini $\{x_0, x_1, \ldots, x_{n-1}\}$.

Le théorème sur l'associativité de la composition de plusieurs éléments prend pour une loi de composition associative et commutative la forme suivante :

<u>Si</u> $\{U_0, U_1, \ldots, U_{h-1}\}$ <u>est un système fini de systèmes finis d'éléments de</u> $\mathcal{T}$, <u>et si</u> $U = U_0 + U_1 + \ldots + U_{h-1}$ <u>est leur juxtaposition, on a</u>

$$\top_{U} x = \top_{i=0}^{n-1} \left(\top_{U_i} x \right)$$

Nous allons maintenant donner un autre moyen de définir un système fini. Soit d'abord $S = \{x_0, x_1, \ldots, x_{n-1}\}$ une suite finie d'éléments d'un ensemble $\mathcal{E}$. x désignant un élément de $\mathcal{E}$, soit $E_{x,S}$ l'ensemble des entiers $i \in I_n$ tels que $x_i = x$. $E_{x,S}$ n'est différent de l'ensemble vide que si x appartient à l'ensemble des éléments de la suite. Désignons par $N_S(x)$ le nombre d'éléments de $E_{x,S}$. Ce nombre $N_S(x)$ est appelé le <u>nombre de fois</u> que x figure dans la suite finie S.

Soit maintenant $S' = \{x'_0, x'_1, \ldots, x'_{n-1}\}$ une suite finie ne différant de S que par l'ordre des termes. Il existe donc une permutation f de I_n telle que $x'_k = x_{f(k)}$. On en déduit $E_{x,S'} = f(E_{x,S})$ et

$$N_{S'}(x) = N_S(x)$$

Le nombre $N_S(x)$ ne dépend donc que du système fini U auquel appartient S : on peut le désigner par $N_U(x)$. On appelle $N_U(x)$ le nombre de fois que x figure dans le système fini U. Nous allons maintenant montrer que le système U est bien déterminé par la donnée de la fonction $N_U(x)$. Pour cela, S et S' étant deux suites finies, nous allons montrer que l'égalité $N_S(x) = N_{S'}(x)$ (pour tout x) entraîne $S \sim S'$. En effet, soient F,F' les ensembles des éléments des suites S,S'. Les conditions "$x \in F$", "$N_S(x) \neq 0$", "$N_{S'}(x) \neq 0$", "$x \in F'$" sont équivalentes. D'où F = F'. De plus, on a

$$I_n = \sum_{x \in F} E_{x,S} = \sum_{x \in F'} E_{x,S'}$$

Pour chaque $x \in F$ les ensembles $E_{x,S}$, $E_{x,S'}$ ont par hypothèse même puissance. Il existe donc une application bi-univoque f_x de $E_{x,S}$ sur $E_{x,S'}$; la fonction f définie sur I_n par les égalités $f(k) = f_x(k)$ si $k \in E_{x,S}$ est donc une permutation de I_n. On a $f\,(E_{x,S}) = E_{x,S'}$, et par suite $x'_k = x_{f(k)}$, d'où $S \sim S'$: c'est ce que nous voulions démontrer.

Inversement toute fonction $N(x)$ définie sur $\mathcal{T}$, prenant ses valeurs dans l'ensemble des entiers naturels et telle que l'ensemble des x pour lesquels $N(x) \neq 0$ soit fini peut servir à caractériser un système fini d'éléments de $\mathcal{T}$ qu'on construira facilement.

On remarquera que, si U et V sont des systèmes finis, on a

$$N_{U+V}(x) = N_U(x) = N_V(x).$$

§ VIII. PROLONGEMENTS DE STRUCTURES.

Nous avons vu que dans une structure $\mathcal{T}$ définie par une loi de composition $\top$, il faut en général distinguer les notions d'élément régulier et d'élément ayant un inverse. Nous dirons que la structure $\mathcal{T}$ est <u>achevée</u> (par rapport à la loi $\top$) si tout élément régulier y possède un inverse.

Nous allons maintenant démontrer le

Théorème. <u>Toute structure associative et commutative est isomorphe à une structure induite par une structure achevée sur l'une de ses parties.</u>

Signalons tout de suite que ce théorème extrêmement utile devient en général faux si on y supprime la condition relative à la commutativité. Ce fait est à l'origine des grandes difficultés que l'on éprouve à étudier certaines structures non commutatives.

Pour démontrer le théorème, nous désignerons par $\mathcal{T}$ une structure associative et commutative définie par une loi de composition $\top$, et par R l'ensemble des éléments réguliers de $\mathcal{T}$. Si R est vide il n'y a rien à démontrer. Nous supposerons qu'il n'en est pas ainsi. Nous formerons alors le produit $\mathcal{T} \times R$ et nous y définirons une loi de composition (que nous désignerons encore par $\top$) au moyen de la formule

$$(x,y) \top (x',y') = (x \top x', y \top y')$$
$$(x,x' \in \mathcal{T} ; y,y' \in R)$$

On vérifie tout de suite que la loi de composition ainsi définie dans $\mathcal{T} \times R$ est associative et commutative.

Nous allons maintenant définir une relation "$(x,y) \equiv (x',y')$" entre éléments de $\mathcal{T} \times R$ de la manière suivante : la proposition "$(x,y) \equiv (x',y')$" sera par définition équivalente à "$x \top y' = x' \top y$".

La relation ainsi définie est une relation d'équivalence. En effet : a) la proposition $(x,y) \equiv (x,y)$ est vraie de tout élément $(x,y) \in \mathcal{T} \times R$; b) la proposition $(x,y) \equiv (x',y')$ entraîne $x' \top y = x \top y'$ d'où $(x',y') \equiv (x,y)$; c) les propositions $(x,y) \equiv (x',y')$ et $(x',y') \equiv (x'',y'')$ entraînent $x \top y' = x' \top y$ et $x' \top y'' = x'' \top y'$, d'où, en tenant compte de l'associativité et de la commutativité, $x \top y' \top y'' = x' \top y \top y'' = x' \top y'' \top y = x'' \top y' \top y = x'' \top y \top y'$. On en déduit l'égalité $(x \top y'') \top y' = (x'' \top y) \top y'$ qui entraîne, en tenant compte du fait que y' est régulier, $x \top y'' = x'' \top y$, c'est-à-dire $(x, y) \equiv (x'', y'')$.

Montrons maintenant que la relation d'équivalence $(x,y) \equiv (x',y')$ est une relation de congruence par rapport à la loi de composition $\top$ dans $\mathcal{V} \times R$. La loi $\top$ étant commutative, il suffit de montrer que les conditions $(z,u) \in \mathcal{V} \times R$, $(x,y) \equiv (x',y')$ entraînent $(z,u) \top (x,y) \equiv (z,u) \top (x', y')$. Or les conditions données entraînent $x \top y' = x' \top y$, d'où $z \top x \top y' \top u = z \top x' \top y \top u$ ou encore $z \top x \top u \top y' = z \top x' \top u \top y$ c'est-à-dire $(z \top x, u \top y) = (z \top x', u \top y')$ qui est précisément ce que nous voulions démontrer.

La relation de congruence ainsi définie nous donne donc une structure quotient $\mathcal{F}$ de $\mathcal{V} \times R$: c'est la structure cherchée comme nous allons maintenant le montrer.

x étant un élément de $\mathcal{V}$, considérons tous les couples (y,z) tels que $z \in R, y = x \top z$. R n'étant pas vide, il existe de ces couples. Si $(y,z),(y',z')$ sont deux de ces couples, on a $y = x \top z$ et $y' = x \top z'$ d'où $z \top y' = z \quad x \quad z' = x \quad z \quad z' = y \quad z'$, et par suite $(y,z) \quad (y',z')$. Tous les couples en question appartiennent donc à une même classe $\mathcal{C} \in \mathcal{F}$. Nous poserons $f(x) = \mathcal{C}$. f est donc une application de $\mathcal{V}$ dans $\mathcal{F}$.

x' désignant un nouvel élément de $\mathcal{V}$, soit z un élément de R. Posons $y = x \top z$, $y' = x' \top z$, d'où $(y,z) \in f(x)$, $(y',z) \in f(x')$. On a $x \top z \top x' \top z = y \top y' = (x \top x') \top (z \top z)$, et $z \top z \in R$. On en déduit que $f(x \top x') = f(x) \top f(x')$: f est une homomorphie de $\mathcal{V}$ dans $\mathcal{F}$.

De plus, l'égalité $f(x) = f(x')$ entraîne $(y,z) \equiv (y',z)$, ou $y \top z = y' \top z$; z étant régulier, cette égalité entraîne $y = y'$, d'où $x \top z = x' \top z$ et, z étant régulier, $x = x'$: f est une application bi-univoque. f est donc une isomorphie de $\mathcal{T}$ avec une partie $f(\mathcal{T})$ de $\mathcal{F}$.

Reste à montrer que la structure $\mathcal{F}$ est achevée. Tout d'abord, elle comporte un élément unité. En effet, z étant un élément de R, on a, pour tout couple $(x,y) \in \mathcal{T} \times R$, $(x,y) \top (z,z) \equiv (x,y)$, et par suite la classe $\mathcal{N}$ ~~ex~~ de (z, z) est élément unité de $\mathcal{F}$.

$\mathcal{C}$ étant un élément régulier de $\mathcal{F}$, soit (x,y) un couple de la classe $\mathcal{C}$. Nous allons montrer que x est nécessairement régulier dans $\mathcal{T}$. Soient x', x'' des éléments de $\mathcal{T}$ tels que $x \top x' = x \top x''$. On a aussi $(x,y) \top (x',y) = (x,y) \top (x'',y)$, d'où, puisque $\mathcal{C}$ est régulier dans $\mathcal{F}$, $(x',y) \equiv (x'',y)$ et $x' \top y = x'' \top y$. y étant régulier on en déduit $x' = x''$: donc x est régulier. Il en résulte que (y,x) est encore dans $\mathcal{T} \times R$. Si $\mathcal{C}'$ est la classe de ce couple, la classe $\mathcal{C} \top \mathcal{C}'$ contient $(x,y) \top (y \top x) = (x \top y, x \top y)$ qui est dans $\mathcal{N}$. Donc $\mathcal{C} \top \mathcal{C}' = \mathcal{N}$, et par suite $\mathcal{C}'$ est l'inverse de $\mathcal{C}$, ce qui achève la démonstration.

On remarquera que si x est régulier dans $\mathcal{T}$, l'élément $\mathcal{N} = f(x)$ est régulier dans $\mathcal{F}$. En effet, soient $\mathcal{C}'$, $\mathcal{C}''$ des éléments de $\mathcal{F}$ tels que $\mathcal{C} \top \mathcal{C}' = \mathcal{C} \top \mathcal{C}''$. Choisissons dans $\mathcal{C}$, $\mathcal{C}''$ des éléments (x',y'), (x'',y'') : on a $(x \top x', y \top y') \equiv (x \top x'', y \top y'')$ qui peut s'écrire $x \top y \top x' \top y'' = x \top y \top x'' \top y'$; $x \top y$ étant régulier, on en déduit $x' \top y'' = x'' \top y'$, d'où $(x',y') \equiv (x'',y'')$ et $\mathcal{C}' = \mathcal{C}''$: $\mathcal{C}$ est régulier.

De plus, la structure $\overline{\mathcal{F}}$ que nous venons de construire est en un certain sens la plus petite structure satisfaisant aux conditions imposées. D'une manière précise, nous allons montrer que :

Soit $\overline{\mathcal{F}}$ une structure définie par une loi de composition $\top$ entre éléments de $\overline{\mathcal{F}}$ et qui jouit des propriétés suivantes :

1) Il existe une isomorphie φ entre $\mathcal{T}$ et une structure induite par $\overline{\mathcal{F}}$ sur l'une de ses parties ;

2) L'isomorphie φ change les éléments réguliers de $\mathcal{T}$ en éléments qui ont des inverses dans $\overline{\mathcal{F}}$;

Alors $\overline{\mathcal{F}}$ induit sur l'une de ses parties une structure isomorphe à $\mathcal{F}$.

R désignant toujours l'ensemble des éléments réguliers de $\mathcal{T}$, et (x,y) désignant un couple de $\mathcal{T} \times R$, nous poserons $\varphi(x,y) = \varphi(x) \top \varphi^{-1}(y)$. La congruence $(x,y) \equiv (x',y')$ entraîne $x \top y' = x' \top y$, d'où $\varphi(x) \top \varphi(y') = \varphi(x') \top \varphi(y)$ ou encore $\varphi(x,y) = \varphi(x',y')$: autrement dit, la valeur de $\varphi(x,y)$ ne dépend que de la classe $\mathcal{C}$ de $\mathcal{F}$ à laquelle appartient (x,y) : nous pouvons désigner cette valeur que $\overline{\varphi}(\mathcal{C})$: $\overline{\varphi}$ est une application de $\mathcal{F}$ dans $\overline{\mathcal{F}}$.

$\mathcal{C}$ et $\mathcal{C}'$ étant deux éléments de $\mathcal{F}$, soient (x,y), (x',y') des couples de $\mathcal{T} \times R$ tels que $(x,y) \in \mathcal{C}$, $(x',y') \in \mathcal{C}'$. On a

$$\overline{\varphi}(\mathcal{C} \top \mathcal{C}') = \varphi(x \top x' , y \top y') = \varphi(x \quad x') \top \overline{\varphi}^{1}(y \top y') =$$
$$= \varphi(x) \top \varphi(x') \top \overline{\varphi}^{1}(y) \top \overline{\varphi}^{1}(y') = \varphi(x,y) \top \varphi(x',y') =$$
$$= \overline{\varphi}(\mathcal{C}) \top \overline{\varphi}(\mathcal{C}')$$

Donc $\overline{\varphi}$ est une homomorphie de $\mathcal{F}$ dans $\overline{\mathcal{F}}$. De plus, si nous supposons $\overline{\varphi}(\mathcal{C}) = \overline{\varphi}(\mathcal{C}')$, nous avons $\varphi(x) \top \varphi^{-1}(y) = \varphi(x') \top \varphi^{-1}(y')$ ou $\varphi(x \top y') = \varphi(x' \top y)$ et $x \top y' = x' \top y$ d'où $\mathcal{C} = \mathcal{C}'$: $\overline{\varphi}$ est donc une isomorphie de $\mathcal{F}$ avec une partie de $\overline{\mathcal{F}}$, ce qui démontre notre assertion.

40

On remarquera de plus que, si f est l'isomorphie que nous avons construite entre $\mathcal{T}$ et une partie de $\mathcal{F}$, on a, sur $\mathcal{T}$,

$$\bar{\varphi}\, f = \varphi$$

La structure $\mathcal{F}$ est parfaitement déterminée par la donnée de $\mathcal{T}$. D'autre part, parmi les structures jouissant des propriétés 1), 2), elle est caractérisée (à une isomorphie près) par la propriété supplémentaire suivante :

3) <u>Tout élément de</u> $\mathcal{F}$ <u>se met sous la forme</u> $\varphi(x) \top \varphi^{-1}(y)$, <u>avec</u> $x \in \mathcal{T}$, $y \in R$.

On remarquera enfin que l'ensemble des éléments réguliers de $\mathcal{F}$ constitue un groupe par la loi de composition $\top$. Cet ensemble, est, comme nous l'avons vu au cours de la démonstration, identique à l'ensemble des éléments de $\mathcal{F}$ qui peuvent se mettre sous la forme $\varphi(x) \top \varphi^{-1}(y)$, avec $x, y \in R$. En particulier, si tous les éléments de $\mathcal{T}$ sont réguliers, la structure $\mathcal{F}$ est une structure de groupe commutatif.

§ IX. SYSTÈMES A COMPOSITION MULTIPLE. DISTRIBUTIVITÉ.

Très souvent les structures que l'on a à considèrer comportent simultanément plusieurs lois de composition.

Considérons une structure $\mathcal{T}$ définie par des ensembles fondamentaux $\mathcal{T}$; $\mathcal{P}$; $\mathcal{P}'$; ... ainsi que par la donnée de diverses lois de composition entre éléments de $\mathcal{T}$ et de lois de composition entre les éléments de $\mathcal{P}$, $\mathcal{P}'$,.... et éléments de $\mathcal{T}$.

Pour trouver les structures induites par la structure en question, nous aurons à considérer des parties A de $\mathcal{T}$ qui soient simultanément : 1) fermées par rapport aux diverses lois de composition dans $\mathcal{T}$; 2) invariantes par les opérateurs de $\mathcal{P}$, $\mathcal{P}'$,....

Il est clair que l'intersection d'une famille de parties dont chacune jouit simultanément de toutes ces propriétés jouit encore de ces propriétés. Nous pourrons donc encore parler de la structure induite *engendrée* par une partie quelconque B de $\mathcal{T}$, et définir les *systèmes de générateurs* de $\mathcal{T}$.

Pour trouver les structures-quotient de $\mathcal{T}$, nous devrons prendre des relations d'équivalence entre éléments de $\mathcal{T}$ qui soient simultanément : 1) des relations de congruence par rapport aux lois de composition dans $\mathcal{T}$; 2) compatibles avec les compositions avec les éléments de $\mathcal{P}$, $\mathcal{P}'$,....

Là encore, toute structure quotient d'une structure quotient de $\mathcal{T}$ est isomorphe à une structure quotient de $\mathcal{T}$.

Considérons notamment le cas où on donne 1) une loi de composition $x \top y$ entre éléments de $\mathcal{T}$ 2) une loi de composition $\alpha \perp x$ entre éléments $a \in \mathcal{P}$ et $x \in \mathcal{T}$.

Définition. *On dit que la loi de composition $\perp$ est distributive par rapport à la loi $\top$ si on a, x et y désignant des éléments quelconques de $\mathcal{T}$, et a un élément quelconque de $\mathcal{P}$*

$$a \perp (x \top y) = (a \perp x) \top (a \perp y)$$

Par exemple, supposons que la loi $\top$ soit commutative et associative, que $\mathcal{P}$ soit l'ensemble $\mathcal{N} - \{0\}$ des entiers naturels autres que 0 et que la loi $\perp$ soit définie par la formule (cf. § III).

$$a \perp x = \overbrace{x \top x \top \dots \top x}^{a \text{ fois}}$$

Dans ces conditions, la loi $\perp$ est distributive par rapport à la loi $\top$. En effet, on a, en vertu des hypothèses faites sur

$$a \perp (x \top y) = \overbrace{(x \top y) \top (x \top y) \top \dots \top (x \top y)}^{a \text{ fois}} = \overbrace{(x \top x \top \dots \top x)}^{a \text{ fois}}$$
$$\top \overbrace{(y \top y \top \dots \top y)}^{a \text{ fois}} = (a \perp x) \top (a \perp y)$$

D'autres exemples se rapportent au cas où $\mathcal{P} = \mathcal{T}$: par exemple, dans l'ensemble des entiers naturels, la multiplication est, comme nous l'avons vu, distributive par rapport à l'addition. Enfin, supposons que la loi $\top$ soit associative, et soit $\mathcal{P}$ l'ensemble de $\mathcal{T}$ qui ont un inverse par rapport à la loi $\top$. a étant dans $\mathcal{P}$ et $x \in \mathcal{T}$, posons

$$a \perp x = a \top x \top a^{-1}$$

Nous obtenons une loi de composition entre éléments de $\mathcal{P}$ et de $\mathcal{T}$. Cette loi est distributive par rapport à la loi $\top$. En effet, on a, en désignant par e l'élément unité de la loi $\top$,

$$a \perp (x \top y) = a \top x \top y \top a^{-1} = a \top x \top e \top y \top a^{-1} =$$
$$(a \top x \top a^{-1}) \top (a \top y \top a^{-1}) = (a \perp x) \top (a \perp y)$$

Dans le cas où $\mathcal{T}$ constitue un groupe par rapport à la loi $\top$, on voit que les sous-groupes normaux de $\mathcal{T}$ sont les sous-groupes qui sont invariants par rapport à la composition au sens de la loi $\perp$ avec les éléments de $\mathcal{P}$ (qui sont ici les mêmes que ceux de $\mathcal{T}$).

On peut formuler autrement la définition de la distributivité de la loi $\perp$ par rapport à la loi $\top$. En effet, cette distributivité est équivalente au fait suivant : l'<u>application</u> $f_a(x) = a \perp x$ <u>de $\mathcal{T}$ dans lui-même produite par un élément</u> $a \in \mathcal{P}$ <u>est une homomorphie (par rapport à la loi $\top$) de $\mathcal{T}$ dans $\mathcal{T}$</u>.

On vérifie tout de suite que toute structure induite par une structure définie par deux lois de composition dont la première est distributive par rapport à la seconde jouit encore de la même propriété. Il en est encore de même des structures-quotient d'une telle structure.

Dans le cas où $\rho = \mathcal{T}$, donc où $\perp$ et $\top$ représentent deux lois de composition entre éléments de $\mathcal{T}$, il convient encore de considérer la <u>double distributivité</u> :

<u>$\mathcal{T}$ étant un ensemble muni des deux lois de composition $\perp$, $\top$ la loi $\perp$ est dite doublement distributive par rapport à la loi $\top$ si on a, pour</u> x, y, z $\mathcal{T}$,

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

Si la loi $\perp$ est commutative, cette propriété est équivalente à la distributivité simple de la loi $\perp$ par rapport à la loi $\top$.

D'autre part, la loi $\perp$ étant supposée doublement distributive par rapport à la loi $\top$, supposons que cette dernière soit associative, et que la loi $\perp$ comporte un élément unité e. Dans ces conditions, la structure induite par la loi $\top$ sur l'ensemble R des éléments réguliers par rapport à $\top$ est commutative. En effet, soient x, y deux éléments de R. On a

$$(x \top y) \perp (e \top e) = ((x \top y) \perp e) \top ((x \top y) \perp e) = x \top y \top x \top y$$

et aussi

$$(x \top y) \perp (e \top e) = (x \perp (e \top e)) \top (y \perp (e \top e))$$
$$= x \top x \top y \top y$$

x étant régulier, l'égalité $x \top (y \top x \top y) = x \top (x \top y \top y)$ entraîne $y \top x \top y = x \top y \top y$; y étant régulier, cette égalité entraîne à son tour $x \top y = y \top x$, ce qui prouve notre assertion.

En particulier : *si la loi $\perp$ comporte un élément unité et si $\mathcal{G}$ constitue un groupe par rapport à la loi $\top$, ce groupe est commutatif.*

Les relations qui peuvent exister entre diverses lois de composition sont extrêmement variées. Nous aurons l'occasion d'en rencontrer divers types par la suite. Nous les décrirons au fur et à mesure des besoins.