EXTENSIONS DU GROUPE DE LORENTZ PAR UN GROUPE DE JAUGE

F. LURCAT et L. MICHEL

Le but de cet article est double : d'une part, nous donnons la démonstration de résultats mathématiques sur les extensions du groupe de Lorentz par un groupe abélien, résultats que nous avons utilisés par ailleurs[1] ; d'autre part, nous nous proposons d'initier le lecteur physicien à des concepts et des méthodes mathématiques modernes, dont nous pensons que la physique sera amenée à se servir toujours davantage, et qui n'ont pas encore été expliqués ailleurs que dans les articles ou livres destinés aux mathématiciens.

La première partie rappelle des notions générales de théorie des groupes, et donne ensuite l'essentiel de la théorie générale des extensions des groupes. La seconde partie expose les résultats sur les extensions du groupe de Lorentz par un groupe abélien ; des théorèmes essentiels et une partie des résultats nous ont été fournis par J. P. Serre.

Tirage restreint de la première version d'un article dont nos amis ont déjà trop entendu parlé. Nous leur demandons de bien vouloir la lire d'un oeil critique et de nous prodiguer leurs conseils.

I. NOTIONS PRELIMINAIRES, PROBLEMES DES ECTENSIONS D'UN GROUPE L PAR UN GROUPE G

1 - Ensembles. Applications

Considérons un ensemble E ; les éléments de E sont notés x, y ... et on note "x appartient à E" ainsi : $x \in E$. Soit E' un autre ensemble, dont les éléments sont notés x', y'... On appelle produit $E \times E'$ des ensembles E, E' l'ensemble des couples ordonés (x, x'), où $x \in E$, $x' \in E'$. Les ensembles E et E' peuvent être identiques, auquel cas il faut remarquer que les éléments (x,y) et (y,x) de $E \times E$ sont distincts.

On dit qu'on a défini une relation sur E si on s'est donné une partie R de $E \times E$: on note la relation $R(x,y)$, ce qui veut dire $(x,y) \in R$. Nous rencontrerons souvent dans la suite des relations d'équivalence, qui sont caractérisées par les trois propriétés suivantes : une relation d'équivalence (notée $x \sim y$) est

symétrique, c'est-à-dire que $x \sim y$ implique $y \sim x$ (le mot implique se note $\Rightarrow$)

réflexive, c'est-à-dire que quelque soit $x \in E$, on a $x \sim x$ (quelque soit se note $\forall$)

transitive, c'est-à-dire que $x \sim y$ et $y \sim z \Rightarrow x \sim z$.

Considérons un ensemble E, une relation d'équivalence R définie sur E, et un élément $x \in E$; l'ensemble de tous les $y \in E$ tels que $x \sim y$ se nomme classe d'équivalence de x. Soit z un élément de E distinct de x ; ou bien $x \sim z$, et alors les classes d'équivalence de x et z sont identiques, ou bien on n'a pas $x \sim z$, et alors les classes d'équivalence de x et z sont disjointes, c'est-à-dire n'ont aucun élément commun ; en effet, si il existait un élément commun y, on aurait $x \sim y$ et $y \sim z$, donc par transitivité $x \sim z$. Nous pouvons donc partager l'ensemble E en classes disjointes ; l'ensemble de ces classes s'appelle ensemble quotient de E par la relation R, et se note E/R.

Soient deux ensembles E et E'. On dit que l'on a défini une <u>application f de E dans E'</u> si on a une loi qui fait correspondre, à tout $x \in E$, un élément $x' \in E'$; cet élément est appelé <u>image</u> de x par l'application f ; on le note $x' = f(x)$. L'application sera souvent notée $E \xrightarrow{f} E'$.

Soit A une partie de E, c'est-à-dire un ensemble dont tout les éléments sont des éléments de E : on note $A \subset E$. On appelle image de A par l'application f l'ensemble $f(A) \subset E'$ des images de tous les éléments de A. En particulier, l'image de E est une partie de E', appelée <u>image</u> de l'application f, et notée Imf. En général, l'image de E n'est pas tout E' mais seulement une partie ; si $f(E) = E'$ on dit que f est une application de E <u>sur</u> E', ou encore que f est <u>surjective</u>.

Considérons une partie A' de E'. L'ensemble des éléments de E dont l'image par f est dans A' est une partie de E appelée <u>image réciproque</u> de A' ; on note $A = f^{-1}(A')$. On a ainsi défini une application de l'ensemble des parties de E' dans l'ensemble des parties de E ; bien entendu, A peut ne contenir aucun élément, auquel cas on dit que A est la <u>partie vide</u> de E. Pour que, $\forall A' \subset E'$, $f^{-1}(A')$ contienne au moins un élément de E, il faut et suffit que f soit surjective. D'autre part, considérons l'image réciproque de la partie de E' réduite au seul élément x', partie notée $\{x'\}$; si pour tout $x' \in E'$ $f^{-1}(\{x'\})$ contient au plus un élément de E, on dit que f est une <u>injection</u>, ou une application <u>injective</u> ; deux éléments distincts de E ont alors pour images deux éléments distincts de E'.
Exemple : $A \subset E$, $x \in A$, l'application f de A dans E définie par : $x = f(x)$ est une injection appelée <u>injection canonique</u>.

Si f est injective et surjective, on dit qu'elle est <u>bijective</u>, ou encore qu'il y a une correspondance biunivoque (<u>bijection</u>) entre les éléments de E et ceux de E'.

Soit f une application quelconque de E dans E'. La relation $f(x) = f(y)$ est une relation d'équivalence R sur E, comme on peut aisément le vérifier. La classe d'équivalence de x est l'image réciproque $f^{-1}\left[\{f(x)\}\right]$
L'application de E/R dans E', qui à la classe de x fait correspondre f(x),

est une injection ; l'application de E/R sur l'image de f est une bijection.

Considérons trois ensembles E, E', E'', une application f de E dans E', une application f' de E' dans E''. On appelle <u>application composée</u> $g = f' \circ f$ l'application de E dans E'' définie par : $g(x) = f'\left[f(x)\right]$.
Exemple : Nous avons montré que $E \xrightarrow{f} E'$ se décompose canoniquement en $f = f''' \circ f'' \circ f'$ ainsi définies

$$E \underset{\text{surjection}}{\xrightarrow{f'}} E/R \underset{\text{bijection}}{\xrightarrow{f''}} \operatorname{Im} f \underset{\text{injection}}{\xrightarrow{f'''}} E'$$

2 - Groupes. Homomorphismes

On dit qu'un ensemble G est muni d'une structure de <u>groupe</u>, si on a défini une application de $G \times G$ dans G, qui fait correspondre à tout couple ordonné (x,y) un élément $z \in G$ appelé <u>produit</u> de x par y, $z = xy$, et qui possède les propriétés suivantes :

a) associativité : $(xy)z = x(yz)$

b) existence d'une unité : il existe un élément e tel que, $\forall x \in G$, $ex = xe = x$. On montre aisément que cet élément est unique.

c) existence d'un inverse : $\forall x \in G$, il existe un élément unique $x^{-1} \in G$, tel que $x^{-1}x = xx^{-1} = e$.

Soient A, B deux parties de G ; nous noterons AB l'ensemble des éléments de G de la forme ab, $a \in A$, $b \in B$. Nous utiliserons aussi la notation $a.B$ si $A = \{a\}$.

Dans le cas particulier où $\forall x$ et $y \in G$, $xy = yx$, G est dit <u>abélien</u> ; le produit de x par y est alors souvent noté $x + y$.

Une application f d'un groupe G dans un groupe G' est un <u>homomorphisme</u> si :

$$\forall x, y \in G, \qquad f(x)\, f(y) = f(xy)$$

Si l'homomorphisme f est bijectif, f est alors un <u>isomorphisme</u>.

Le lecteur vérifiera aisément que "G isomorphe à G" est une relation d'équivalence parmi les groupes. Aussi on ne considère souvent que les classes d'équivalence des groupes définis à un isomorphisme près. (On dit aussi groupes abstraits).

Nous noterons G isomorphe à G' : $G \approx G'$

Soit $G \xrightarrow{f} G'$ un homomorphisme quelconque : <u>Imf est un groupe</u>. En effet, soient e, e' les unités de G et G' respectivement ; $\forall x \in G$, $xe = ex = x$, donc $f(x)f(e) = f(e)f(x) = f(x)$, donc $f(e) = e'$: Imf contient donc l'unité de G'. Si x' et $y' \in$ Imf, c'est que $x' = f(x)$, $y' = f(y)$; donc $x'y' = f(xy)$, c'est-à-dire que $x'y' \in$ Imf. Enfin, si $x' = f(x)$, $f(x)f(x^{-1}) = f(e) = e'$, donc $f(x^{-1}) = [f(x)]^{-1}$, donc $x'^{-1} \in$ Imf.

On dit que Imf est un <u>sous-groupe</u> de G' : c'est un sous-ensemble de G', et il forme un groupe, la loi de multiplication étant <u>la même</u> que sur G'.

Nous avons vu au § 1 qu'à toute application d'un ensemble E dans un ensemble E' correspond une bijection de E/R sur Imf, R étant la relation d'équivalence : $f(x) = f(y)$; dans le cas d'un homomorphisme d'un groupe G dans un groupe G', cette relation R s'écrit :

$$e' = f(x)\,[f(y)]^{-1} = f(x)f(y^{-1}) = f(xy^{-1}) = f(e) \qquad (2)$$

e étant l'unité de G. Ou encore :

$$[f(x)]^{-1}\,f(y) = f(x^{-1})f(y) = f(x^{-1}y) = f(e) \qquad (2')$$

Soit $K = f^{-1}(e)$ l'image réciproque de l'unité de G' : les équations (2) et (2') sont équivalentes respectivement à :

$$R(x, y) \;:\; xy^{-1} \in K \qquad (3)$$

$$R(x, y) \;:\; x^{-1}y \in K \qquad (3')$$

L'ensemble quotient de G par la relation d'équivalence R a donc pour éléments les ensembles :

$$x.K \;=\; K.x \tag{4}$$

On note encore souvent cet ensemble quotient G/K. Nous utiliserons souvent (4) sous la forme :

$$xKx^{-1} \;=\; K \tag{4'}$$

La bijection $G/K \xrightarrow{f''}$ Imf est aussi un homomorphisme :

$$f(xK)\ f(yK) = f(xKyK) = f(xyK) \qquad \text{(grâce à (4))}$$

c'est donc un isomorphisme et le groupe G/K, isomorphe à Imf est dit groupe quotient de G par K. Son élément $x.K = K.x$ est appelé translaté de K par x. Il faut noter que K n'est pas un sous groupe quelconque de G. Il doit satisfaire (4') pour tous $x \in G$. Un tel sous-groupe est dit sous-groupe distingué (langage de N. Bourbaki ; on dit souvent aussi "invariant").

<u>Sous-groupes distingués</u>

Un sous-groupe K de G est distingué s'il satisfait (4) pour $\forall x \in G$. On constate alors que les relations d'équivalence (3) et (3') sont identiques (même quotient G(K)) et sont compatibles avec la loi de groupe : $x \sim x'$, $y \sim y' \Longrightarrow xy \sim x'y'$, ce qui permet de munir canoniquement l'ensemble quotient G/K de la loi de groupe quotient

$$(xK)\ (yK) = xyK$$

Tout groupe a au moins deux sous-groupes distingués : lui-même et $\{1\}$, le groupe constitué du seul élément unité.

Tous les sous-groupes d'un groupe abélien sont distingués.

Nous signalons au lecteur, pour piquer sa curiosité qu'il existe aussi des groupes non abeliens dont tout sous-groupe est distingué.

Attention ! La relation K "sous-groupe de" G est transitive, mais la relation K "sous-groupe distingué de" ne l'est pas en général. Grâce à (4) on établit aisément que dans homomorphisme $G \xrightarrow{f} G'$ l'image de tout sous-groupe distingué est un sous-groupe distingué.

3 - Suites exactes d'homomorphismes

Soit une suite d'applications (ou bien homomorphisme)

$$\cdots \longrightarrow G_n \xrightarrow{f_n} G_{n+1} \xrightarrow{f_{n+1}} G_{n+2} \xrightarrow{f_{n+2}} G_{n+3} \xrightarrow{f_{n+3}} \cdots \qquad (5)$$

Si $x_{n+1} = f_n(x_n)$, $x_{n+2} = f_{n+1}(x_{n+2})$ on vérifie que la correspondance $G_n \ni x_n \longrightarrow x_{n+2} \in G_{n+2}$ est une application (ou bien un homomorphisme), qui est noté $f_{n+1} \circ f_n$, et est appelée "composé de f_n et f_{n+2}" (nous écrivons à droite la première application, ou bien homomorphisme, exécutée). Vérifier que o est une loi de composition associative.

La suite d'homomorphismes (5) est dit exacte si pour tout n :

$$\operatorname{Im} f_n = \operatorname{Ker} f_{n+1} \qquad (6)$$

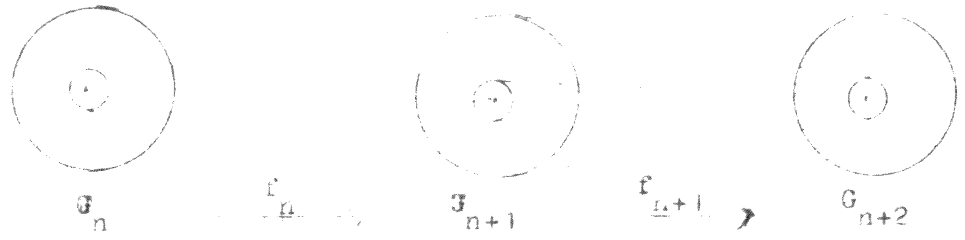
Notons que cela entraîne :

$$f_{n+1} \circ f_n = 0 \qquad (7)$$

en définissant l'homorphisme 0, par l'homomorphisme qui a pour image un seul élément. Par contre (7) n'implique pas (6), mais seulement $\operatorname{Im} f_n \subset \operatorname{Ker} f_{n+1}$

Lorsque nous écrirons qu'une ou des suites d'homomorphisme sont exactes, nous mettrons simplement ε : devant la suite.

Le lecteur peut se représenter intuitivement une suite exacte par la figure :



Traduisons en langage de suites exactes des notions déjà rencontrées. (Nous notons simplement **1**, le groupe d'un élément)

- $\varepsilon : 1 \longrightarrow G \xrightarrow{f} G'$ signifie $\mathrm{Ker}\, f = 1$, donc l'application de f est <u>injective</u>. Il existe une application f' (pas nécessairement un homomorphisme) telle que f'o f = I (application identique de G)
- $\varepsilon : G \xrightarrow{f} G' \longrightarrow 1$ signifie Imf = G', donc l'application de l'homomorphisme f est <u>surjective</u> ; de même, il existe une application f' de G' dans G telle que f o f' = I (de G'). Renverser le sens des flèches correspond à une dualité
- $\varepsilon : 1 \longrightarrow G \xrightarrow{f} G' \longrightarrow 1$, l'application de f est injective et surjective donc bijective, donc f est un <u>isomorphisme</u> et
- $\varepsilon : 1 \longrightarrow G \xrightarrow{f} G' \longrightarrow 1 \Longrightarrow \varepsilon : 1 \leftarrow G \leftarrow G' \leftarrow 1$

De plus, au [illegible] 2, nous avons établi, à partir de $G \xrightarrow{f} G'$ Imf = G/Ker f, soit en notation de suite exacte :

- $\varepsilon : 1 \longrightarrow \mathrm{Ker}\, f \longrightarrow G \longrightarrow \mathrm{Im}\, f \longrightarrow 1$

En général, on ne peut ajouter des flèches d'homomorphismes en sens inverse ; cependant lorsqu'on a entre 3 groupes G', G, G" les suites exactes :

- $\varepsilon : 1 \longrightarrow G' \longrightarrow G \longrightarrow G'' \longrightarrow 1$ (8)

([illegible] G")
on dit que G est le produit semi-direct de G" par G'. (On dit aussi "produit direct croisé")

- $\varepsilon : 1 \longrightarrow G' \longrightarrow G \longrightarrow G'' \longrightarrow 1$ (9)

On dit que G est le produit direct de G' et G" et nous noterons $G = G' \times G''$

De façon générale, lorsque :

$$- \quad \varepsilon : 1 \to G' \to G \to G'' \to 1 \tag{10}$$

ont dit que G est une extension de G" par G'.

Un problème que nous voulons étudier est : étant donnés G' et G", trouver les extensions G de G" par G'. NOus préciserons ce problème au § 6

Nous continuons ici à étudier simplement le produit direct. La relation (10) implique que l'ensemble $G = G' \times G''$, produit des ensembles G' et G".

Appelons $\bar{G}'$ l'injection (c'est-à-dire l'image de l'isomorphisme injectif) de G' dans G. Si nous notons x', y'... les éléments de G', x", y" ceux de G", nous pouvons noter (x', x") ceux de G. Par exemple, nous notons (x', 1) ceux de $\bar{G}'$, et l'isomorphisme $x' \to (x', 1)$ nous donne pour la loi de groupe de $\bar{G}'$:

$$(x', 1)\ (y', 1) = (x'y', 1) \tag{11}$$

et nous savons que $\bar{G}'$est sous-groupe distingué de G.

Au lecteur physicien, qui peut trouver pédante cette distinction entre G' et $\bar{G}'$, nous demandons un peu de patience ici. Il nous arrivera souvent de ne pas distinguer deux réalisations du même groupe abstrait, mais nous les distinguons ici, et nous le ferons encore chaque fois que c'est utile pour éviter des confusions. Si (8) ou (9)sont vraies, nous appelons $\bar{G}''$ l'injection de G" nous avons l'isomorphisme $x'' \leftrightarrow (1, x'')$ et la loi de groupe de G" :

$$(1, x'')\ (1, y'') = (1, x''\, y'') \tag{11'}$$

Nous allons établir que, G', G" étant donnés, (9) définit un groupe G unique, dont nous écrirons la loi de groupe. Notons d'abord que (11) et (11') nous donnent :

$$(x', 1)^{-1} = (x'^{-1}, 1) \text{ et } (1, x'')^{-1} = (1, x''^{-1})$$

Puisque $\bar{G}'$ et $\bar{G}''$ sont sous-groupes distingués, on a $\forall x', x''$

$(1,x'')(x',1)(1,x''^{-1}) \in \bar{G}'$ donc aussi $(1,x'')(x',1)(1,x''^{-1})(x'^{-1},1) \in \bar{G}'$

$(x',1)(1,x''^{-1})(x'^{-1},1) \in \bar{G}''$ donc aussi $(1,x'')(x',1)(1,x''^{-1})(x'^{-1},1) \in \bar{G}''$

et comme $\bar{G}' \cap \bar{G}''$ n'a que l'élément unité $(1,1)$, on en déduit :

$$(1,x'')(x',1) = (x',1)(1,x'') \tag{12}$$

nous pourrons noter cet élément (x', x'') et comme conséquence de (11), (11'), (12) nous obtenons pour la loi de groupe de G

$$(x', x'')(y',y'') = (x'y', x''y'') \tag{13}$$

Réciproquement, si on se donne sur l'ensemble $G' \times G''$ la loi de groupe (13), on voit aisément que (9) est vérifié et on a ainsi formé le produit direct $G' \times G''$.

Bien que la notation (9) semble symétrique en G', G'', les ensembles $G' \times G''$ et $G'' \times G'$ sont distincts et les groupes $G' \times G''$ et $G'' \times G'$ le sont donc aussi, bien qu'ils soient isomorphes par la bijection $(x', x'') \to (x'', x')$

On peut définir le produit direct d'un nombre fini de groupes $G = G_1 \times G_2 \times G_3 \times G_4 \times \ldots$ par la loi de groupe

$$(x_1,x_2,x_3,x_4,\ldots)(y_1,y_2,y_3,y_4,\ldots) = (x_1y_1, x_2y_2, x_3y_3, x_4y_4, \ldots)$$

Le produit $\times$ est associatif.

Exemples de produits directs et semi-directs

Soit R le groupe additif des nombres réels. Le groupe $\mathcal{T}_3$ des translations dans l'espace euclidien à 3 dimensions est isomorphe à $R^3 = R \times R \times R$. Le groupe $\mathcal{T}_4$ des translations dans l'espace-temps est isomorphe à $R^4 = R \times R \times R \times R$.

Soit $\mathcal{R}_3$ le groupe des rotations et $\mathcal{O}_3$ le groupe des rotations et symétries laissant fixe un point de l'espace euclidien à 3 dimensions. (Nous noterons **s** la symétrie par rapport à ce point fixe). $\mathcal{R}_3$ est sous-groupe invariant de $\mathcal{O}_3$ et $\mathcal{O}_3 = \mathcal{R}_3 \times Z_2$, les deux éléments du groupe Z_2 étant l'identité et **s**. Soit $\mathcal{D}_3$ le groupe des déplacements de l'espace euclidien, et $\mathcal{D}'_3$ le groupe conservant les distances (engendré par les déplacements et symétries).

$\mathcal{T}_3$ est sous groupe invariant de $\mathcal{D}_3$ et $\mathcal{D}'_3$. Les quotients sont respectivement $\mathcal{R}_3$ et $\mathcal{O}_3$. Il s'agit de produits semi-directs. Soit α, β, ... les éléments de $\mathcal{T}_3$ (notés additivement) et a, b, ... les éléments de $\mathcal{R}_3$ (notés multiplicativement). Le groupe $\mathcal{R}_3$ opère dans le groupe $\mathcal{T}_3$ ainsi : $a\,\alpha\,a^{-1} = a(\alpha)$ que nous noterons simplement $a\alpha$ quand il n'y a pas d'ambiguité. Si :

$$(\alpha, a) = (\alpha, 1)\,(0, a) \tag{14}$$

la loi de groupe de $\mathcal{D}_3$ est :

$$(\alpha, a)\,(\beta, b) = (\alpha + a\beta,\ ab) \tag{14'}$$

Nous laissons au lecteur le soin de vérifier la loi (14'), et d'en déduire la forme de $(\alpha,a)^{-1}$ et vérifier que $\mathcal{T}_3$ est bien sous-groupe invariant. La loi (14')-au lieu de (13)- montrer que $\mathcal{D}_3$ n'est pas produit direct de $\mathcal{R}_3$ par $\mathcal{T}_3$, mais la relation $(0,a)\,(0,b) = (0, ab)$ montre qu'il s'agit d'un produit semi-direct.

4 - Diagrammes d'homomorphismes

Dans ce qui suit nous serons amenés à considérer des suites exactes d'homomorphismes ayant des groupes en commun. Leur représentation graphique forme un diagramme par ex :

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[d, "h_1"'] & B \arrow[r, "g"] \arrow[d, "h_2"'] & C \arrow[d, "h_3"'] \\ A' \arrow[r, "f'"'] & B' \arrow[r, "g'"'] & C' \end{tikzcd}$$

Pour tous les diagrammes que nous écrirons désormais, il sera donc entendu (sauf mention expresse du contraire) que les flèches alignées représentent une suite exacte d'homomorphismes. Il sera de plus toujours convenu que le diagramme sera <u>commutatif</u>, c'est-à-dire s'il existe plusieurs chemins, en descendant les flèches, pour aller d'un groupe à un autre, ces différents chemins représentent le même homomorphisme.

Sur l'exemple donné :

$$h_3 \circ g \circ f \;=\; g' \circ h_2 \circ f \;=\; g' \circ f' \circ h_1$$

Etudions maintenant le plus simple des diagrammes commutatifs : la commutativité signifie que h est le composé de f et g

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[dr, "h"'] & B \arrow[d, "g"] \\ & C \end{tikzcd}$$

$$h = g \circ f$$

Soit $a \in \text{Ker } f$, on a $h(a) = g \circ f(a) = g(1) = 1$, donc $a \in \text{Ker } h$ donc $\text{Ker } f \subset \text{Ker } h$ ce que nous pouvons écrire : $1 \to \text{Ker } f \to \text{Ker } h$

Soit $\bar{f}$ la restriction de f à Ker h (c'est-à-dire l'homomorphisme de Ker h dans B telque $\forall\, a \in \text{Ker } h$, $\bar{f}(a) = f(a)$).

Si $a \in \text{Ker } h$; $1 = h(a) = g \circ f(a) = g(\bar{f}(a))$, donc $\text{Im}\bar{f} \subset \text{Ker } g$

d'où l'homomorphisme $\text{Ker } h \xrightarrow{\bar{f}} \text{Ker } g$, dont le noyau est $\text{Ker } f = \text{Ker } f$.

Nous venons donc d'établir la suite exacte :

$$1 \longrightarrow \mathrm{Ker}\, f \longrightarrow \mathrm{Ker}\, h \xrightarrow{\bar f} \mathrm{Ker}\, g \qquad (14)$$

$\bar f$ est-il surjectif ? nous ne pouvons pas le prouver. Admettons que $h = 0$ (homomorphisme nul, c'est-à-dire $\mathrm{Im}\, h = 1$), $f = 0$, g peut être quelconque et donc $\mathrm{Ker}\, g$ peut être n'importe quel sous-groupe invariant de B. Nous ne pouvons donc prolonger la suite exacte (14) qu'en ajoutant une hypothèse. Par exemple :

<u>Théorème 4A</u>

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[dr, "h"'] & B \arrow[r] \arrow[d, "g"] & 1 \\ & C & \end{tikzcd} \Longrightarrow 1 \longrightarrow \mathrm{Ker}\, f \longrightarrow \mathrm{Ker}\, h \xrightarrow{\bar f} \mathrm{Ker}\, g \longrightarrow 1$$

Démonstration : soit $b \in \mathrm{Ker}\, g$, puisque f est surjectif, $\exists$ a tel que $b = f(a)$, $h(a) = g(b) = 1$ donc $a \in \mathrm{Ker}\, h$ et $b = \bar f(a)$

Une autre hypothèse supplémentaire aurait été $h \neq 0$.

<u>Théorème 4B</u>

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[dr, "h"'] & B \arrow[r] & 1 \\ & C & \end{tikzcd} \quad \text{si } \mathrm{Ker}\, f \subset \mathrm{Ker}\, h \Longrightarrow \begin{tikzcd} A \arrow[r, "f"] \arrow[dr, "h"'] & B \arrow[r] \arrow[d, "g"] & 1 \\ & C & \end{tikzcd}$$

c'est-à-dire on peut compléter le diagramme initial.

Démonstration : soit $b \in B$; puisque f est surjectif $f^{-1}(b)$ n'est pas vide et ses éléments sont équivalents : relation d'équivalence (3)

si $a, a' \in f^{-1}(b)$, $a^{-1}a' \in \mathrm{Ker}\, f$ et d'après l'hypothèse

$a^{-1}a' \in \mathrm{Ker}\, h$ donc $h(a) = h(a') = h(f^{-1}(b)) = c$

et qui définit une application $B \xrightarrow{g} C$, telle que $h = g \circ f$, est-ce un homomorphisme ?

$g(b)\, g(b') = h(a)\, h(a')$ où $f(a) = b$, $f(a') = b'$; $g(b)\, g(b') = h(a\, a') =$
$= g(f(a\, a')) = g(f(a)\, f(a')) = g(b\, b')$

5 - Automorphisme d'un groupe. Groupe opérant sur un groupe.

Un homomorphisme de G dans G est appelé endomorphisme. Si un endomorphisme est un isomorphisme, on l'appelle automorphisme. Les automorphismes forment un groupe noté, Aut. G ; pour la loi de composition $\circ$. L'automorphisme identique est la transformation identique $x \dashrightarrow x$ de G ; l'automorphisme inverse de $x \dashrightarrow x' = a($ est noté α^{-1} et est défini par $x' \dashrightarrow x = a^{-1}(\alpha)$. Une famille particulière d'automorphismes est formée par les <u>automorphismes intérieurs</u> : si $u \in G$, on vérifie aisément que $x \dashrightarrow uxu^{-1}$ est un automorphisme que nous notons $x \dashrightarrow u(x)$; l'automorphisme inverse est $x \dashrightarrow u^{-1}xu = u^{-1}(x)$. Les automorphismes intérieurs forment un groupe noté Aut. int. G, qui est homomorphe à G puisque :

$$(u \circ v)(x) = u(vxv^{-1})u^{-1} = uvxv^{-1}u^{-1} = (uv)(x) \qquad (5.1)$$

Le noyau de l'homomorphisme est formé par les u tels que $x = uxu^{-1}$, pour tout $x \in G$; ce groupe des u commutant avec tous les éléments de G est appelé le centre de G . Nous le notons $\mathcal{C}G$. Nous noterons Aut. int. G le groupe des automorphismes inter~~nes~~ leurs de G et nous venons donc d'établir la suite exacte :

$$1 \longrightarrow \mathcal{C}G \longrightarrow G \longrightarrow \text{Aut. int. } G \longrightarrow 1 \qquad (5.2)$$

Nous allons maintenant établir que Aut. int. G est sous-groupe distingué de Aut. G.

Soit $a \in$ Aut. G et $u \in$ Aut. int. G. Il nous suffit de montrer (cf. 4. 1) que $a \circ u \circ a^{-1}$ est un automorphisme intérieur :

$$a \circ u \circ a^{-1}(x) = a(u\, a^{-1}(x)\, u^{-1})$$

et puisqu'il s'agit d'automorphismes

$$a \circ u \circ a^{-1}(x) = a(u)a(a^{-1}(x))\, a(u^{-1}) = a(u)x\, a(u^{-1}) = u'\, x\, u'^{-1}$$

où nous avons posé :

$$a(u) = u' \in G$$

Nous noterons $\mathcal{A}(G)$ le quotient (Aut. G)/(Aut. int. G). d'où la suite exacte :

$$1 \longrightarrow \text{Aut. int. }(G) \longrightarrow \text{Aut. }(G) \longrightarrow \mathcal{A}(G) \longrightarrow 1 \quad (5.3)$$

Evidemment, si G est abélien, Aut. int. (G) = 1 et $\mathcal{A}(G) \approx$ Aut. (G).

Groupe à opérateurs.

Si on se donne un groupe G, un ensemble E et une application f de E dans Aut. G, on dit que G est un groupe à opérateurs. Le lecteur physicien connaît bien un exemple de groupe à opérateurs : l'espace vectoriel. L'addition des vecteurs x + y est une loi de groupe abélien. Les scalaires α, β agissent sur les vecteurs, les transformant en d'autres vecteurs x, suivant entre autres les axiomes :

$$(\alpha + \beta)x = \alpha x + \beta x \ , \quad \alpha(x + y) = \alpha x + \alpha y \qquad (5.4)$$

La dernière égalité exprimant que $x \longrightarrow \alpha x$ est un automorphisme du groupe abélien d'addition des vecteurs.

Nous rencontrerons surtout le cas où E lui-même est un groupe. Si f est alors un homorphisme $E \xrightarrow{f}$ Aut. G. (C'est ce qu'exprime la première égalité de 5. 4 pour le groupe additif des nombres réels). On dit que le groupe E opère sur G. Nous rencontrerons souvent une telle situation qui est caractérisée entièrement par l'homomorphisme $E \xrightarrow{f}$ Aut. G.

L'ensemble des $x \in G$ tel que $\forall a \in E$, $a(x) = x$ forment un sous-groupe de G, appelé souvent sous-groupe des points fixes et noté G^E. Si $G^E = G$, on dit que E opère trivialement sur G. Si G est sous-groupe distingué de E, E opère canoniquement sur G puisque pour tout $a \in E$, $a\,b\,a^{-1} = b$. On pose $a(x) = axa^{-1}$. Le noyau de l'homomorphisme $E \xrightarrow{f}$ Aut. G est formé de tous les $a \in E$ tel que $ax = xa$ pour tout $x \in G$. On appelle l'ensemble de ces a le commutant de G et on le note G'. Notons que $G \cap G' = \mathcal{C}\, G$.

Nous pouvons résumer dans le diagramme ci-contre les résultats établis dans ce § 5. G étant donné, nous avons établi les suites exactes i", s" et i',s' et la suite i,s étant donnée, nous avons établi l'existence de f. Le diagramme est bien commutatif. L'homomorphisme $i' \circ s''$ applique G dans Aut.G par $x \longrightarrow x(\ )$ tel que $x(y) = x\, y\, x^{-1}$ $(x,\ y \in b)$. Il en est de même de l'homomorphisme $f \circ i$.

$$\begin{tikzcd}
 & 1 \arrow[d] & & & \\
 & \mathcal{C}.G \arrow[d, "i''"] & & & \\
1 \arrow[r] & G \arrow[r, "i"] \arrow[d] & E \arrow[r, "s"] \arrow[d] & L \arrow[r] & 1 \\
1 \arrow[r] & \mathrm{Aut.int}\, G \arrow[r, "i'"] \arrow[d] & \mathrm{Aut}\, G \arrow[r, "s'"] & \mathcal{A}G \arrow[r] & 1 \\
 & 1 & & &
\end{tikzcd}$$

Diagramme 5a

$$\begin{tikzcd}
E \arrow[r, "s"] \arrow[d, "f"'] \arrow[dr, "s' \circ f"] & L \arrow[r] & 1 \\
\mathrm{Aut}\, G \arrow[r, "s'"] & \mathcal{A}.G &
\end{tikzcd}$$

Diagramme 5b

Le théorème 4B va nous permettre de compléter ce diagramme. En effet nous avons la situation du diagramme 5b. Ker s = G, Ker s' = Aut. int. G. et $f(G)$ = Aut. int. G donc $G = \mathrm{Ker}\ s \subset \mathrm{Ker}\ s' \circ f = G$ d'où le diagramme 5 c. L'existence de $L \xrightarrow{g} \mathcal{A}G$ signifie simplement que si $a,\ a' \in E$ et $aL = a'L$, $a' = ax$ où $x \in G$ donc $f(a') = f(a)\ f(x)$ où $f(x)$ est un automorphisme interne de G.

$$\begin{tikzcd}
 & 1 \arrow[d] & & & \\
 & \mathcal{C}G \arrow[d] & & & \\
1 \arrow[r] & G \arrow[r] \arrow[d] & E \arrow[r] \arrow[d, "f"'] & L \arrow[r] \arrow[d, "g"'] & 1 \\
1 \arrow[r] & \mathrm{Aut\,Int}\, G \arrow[r] \arrow[d, no head] & \mathrm{Aut}\, G \arrow[r] & \mathcal{A}G \arrow[r] & 1 \\
 & 1 & & &
\end{tikzcd}$$

diagramme 5 c

Dans le cas où G est abélien : $\mathcal{A}G$ = Aut. G, donc L opère sur G..

6 - Problème des extensions d'un groupe L par un groupe G.

Nous avions déjà dit que le problème général est : L, G étant deux groupes donnés, trouver E tel que la suite :

$$1 \longrightarrow G \longrightarrow E \longrightarrow L \longrightarrow 1$$

soit exacte. On divise ce problème général en une réunion de problèmes en se donnant en plus un des homomorphismes possible $L \xrightarrow{g} \mathcal{A}G$. Il s'agit alors de trouver E afin d'obtenir le diagramme 5 c.

Nous résumons cela dans le diagramme 6 a., en notant en traits pleins ce qui est donné, en pointillé ce qu'il faut trouver. Cela correspond au :

Problème des extensions de L par G pour un homomorphisme $L \xrightarrow{g} \mathcal{A}G$ do

Le problème est plus simple si G est abélien. Dans ce cas, il existe toujours au moins une solution, l'extension inessentielle, qui est un produit semi-direct. Dans le cas où $g = 0$ (homomorphisme trivial), une solution est le produit direct $E = G \times L$. Pour dénombrer les solutions, nous allons d'abord préciser ce que nous considérons comme solutions différentes, données par des extensions inéquivalentes, en établissant une relation d'équivalence entre les extensions.

$$\begin{tikzcd}
 & 1 \arrow[d] & & & \\
 & eG \arrow[d] & & & \\
1 \arrow[r, dashed] & G \arrow[r, dashed] \arrow[d] & E \arrow[r, dashed] & L \arrow[r, dashed] \arrow[d, "g"] & {} \\
1 \arrow[r] & \mathrm{Autint}\,G \arrow[r] \arrow[d] & \mathrm{Aut}\,G \arrow[r] & \mathcal{A}G \arrow[r] & {} \\
 & 1 & & &
\end{tikzcd}$$

diagramme 6 a

$$\begin{tikzcd}
1 \arrow[r, dashed] & G \arrow[r, dashed] & E \arrow[r, dashed] & L \arrow[r, dashed] \arrow[d, "g"] & {} \\
 & & & \mathrm{Aut}\,G &
\end{tikzcd}$$

diagramme 6 b

Définition : E et E' sont des extensions équivalentes de L par G, pour $L \xrightarrow{g} \mathcal{A}G$ donné, s'il existe un diagramme 6 c. où les homomorphismes i, i' sont injectifs et s, s' surjectifs. Montrons que f est un isomorphisme :

$$\begin{tikzcd}
 & E \arrow[dd, "f"] \arrow[dr, "s"] & & \\
G \arrow[ur, "i"] \arrow[dr, "i'"'] & & L \arrow[d, "g"] & \\
 & E' \arrow[ur, "s'"'] & \mathcal{A}G &
\end{tikzcd}$$

diagramme 6 c

Soit $x \in \mathrm{Ker}\, f$, $f(x) = 1$, donc
$s' f(x) = s(x) = 1$.
$x \in \mathrm{Ker}\, s$ donc $x \in \mathrm{Im}\, i$; soit
$a \in G$ tel que $i(a) = x$
$i'(a) = f \circ i(a) = f(x) = 1$
et comme i est une injection
$a = 1$ et donc $x = i(1) = 1$.
donc $\mathrm{Ker}\, f = \{1\}$, f est injectif.

Soit $x' \in E'$, $\alpha = s'(x')$ et puisque s est surjectif, $\exists$ x tel que $s(x) = \alpha$. Soit $x'' = f(x)$, $s' \circ f = s$ donne $s(x'') = \alpha$ donc $x''^{-1} x \in \operatorname{Ker} s'$. Soit $a \in G$ tel que $i'(a) = x''^{-1} x$ et soit $z = i(a)$, $f(z) = x''^{-1} x'$ et $f(x)\, f(z) = f(xz) = x''\, x''^{-1} x' = x'$; donc f est surjectif.

Nous venons de prouver que la diagramme 6 c. peut être complété en 6 d. Il est aisé de prouver que la relation E et E' appartenant au diagramme 6 d. est une relation d'équivalence. Notons que si $E \simeq E'$ est une condition nécessaire pour 6 d., ça n'est pas une condition suffisante; il faut de plus que l'isomorphisme f fasse correspondre élément par élément les injections de G dans E et E' puisque $f \circ i(a) = i'(a)$ pour $\forall\, a \in G$ (et il existe effectivement des extensions isomorphes non équivalentes).

$$\begin{tikzcd}
 & E \arrow[dr, "s"] \arrow[dd, shift right, "f"'] & \\
G \arrow[ur, "i"] \arrow[dr, "i'"'] & & L \arrow[d, "g"] \\
 & E' \arrow[ur, "s'"'] \arrow[uu, shift right, "f^{-1}"'] & A.G
\end{tikzcd}$$

Diagramme 6 d.

II. ETUDE DES EXTENSIONS D'UN GROUPE L PAR UN GROUPE A ABELIEN POUR UN HOMOMORPHISME $L \xrightarrow{g}$ AUT A DONNE

Dans tout ce paragraphe nous allons nous restreindre au cas plus simple où A est abelien. Alors $\mathcal{A}(A) = \operatorname{Aut} A$
Nous supposerons de plus dans tout ce chapitre II qu'un homomorphisme $L \xrightarrow{g} \operatorname{Aut} A$ a été choisi.

Nous noterons L multiplicativement et emploierons des lettres latines pour désigner ses éléments. Nous noterons A additivement et emploierons des lettres grecques pour désigner ses éléments. Nous noterons multiplicativement le groupe E. Nous aurons soin de distinguer A', l'injection de A dans E, puisque A', sous groupe de E sera noté multiplicativement ; c'est-à-dire (l'injection i est indiquée sur le diagramme 1 a)

$$i(\alpha)\, i(\beta) = i(\alpha + \beta)$$

Nous noterons en général :

$$\alpha' = i(\alpha)$$

1 - Systèmes de facteurs

Considérons une extension E, donnée par le diagramme 1.

$$\begin{tikzcd} 1 \arrow[r] & A \arrow[r, "i"] & E \arrow[r, "s"] & L \arrow[r] \arrow[d, "g"] & 1 \\ & & & \mathrm{Aut}\,A & \end{tikzcd}$$

Diagramme 1

Tout élément $x \in E$ appartient à un certain translaté de A, caractérisé par l'élément $a = s(x) \in L$, et que nous appelerons "translaté a". Pour repérer entièrement l'élément x il faudra de plus se donner sa "position" dans le translaté a, pour cela il faut choisir une "origine" dans le translaté a ; c'est-à-dire un élément $k(a) \in E$, cet élément faisant partie du translaté a, on a

$$s \circ k(a) = a$$

ou encore :

$$s \circ k = I \text{ (identité de L)} \qquad (1)$$

L'application k une fois définie, nous pouvons écrire tout élément de E, de façon unique, sous la forme

$$\alpha' \, k(a) \qquad (1 \text{ bis})$$

La fonction k n'est pas, en général, un homomorphisme de L dans E. Si on peut trouver un k qui soit un homomorphisme c'est-à-dire :

$$k(a) \; k(b) = k(ab) \qquad (2)$$

la relation (1) permet de préciser que l'homomorphisme k est injectif ($\mathrm{Im}\,k \simeq L$), on a donc le diagramme commutatif 2 qui définit le produit semi-direct.

$$\begin{tikzcd} 1 \arrow[r] & A \arrow[r, "i"] & E \arrow[r, shift left, "s"] & L \arrow[l, shift left] \arrow[r, shift left] \arrow[d, "g"] & 1 \arrow[l, shift left] \\ & & & \mathrm{Aut}\,A & \end{tikzcd}$$

Diagramme 2.

Si $g = 0$, c'est-à-dire g est l'homomorphisme trivial, nous verrons que E est alors le produit direct.

Dans le cas général on peut seulement dire que k(ab) et k(a) k(b) sont des éléments du même translaté ab de A puisque

$$s \circ k(ab) = \left[s \circ k(a) \right] \left[s \circ k(b) \right] = ab$$

On a donc :

$$k(a)\ k(b) = \omega'(a,\ b)\ k(ab) \tag{3}$$

La fonction $\omega(a,\ b)$ définie sur l'ensemble $L \times L$ et à valeur dans A ($\omega'(a,\ b)$ est son image dans $A' \subset E$ par l'injection i) est appelée <u>un système de facteurs</u>.

Evidemment on peut choisir une autre fonction k(a), d'où un autre système de facteur $\omega(a,\ b)$, défini par (3).

Remarquons que si nous posons dans (3) a et/ou b = 1, nous obtenons :

$$\omega'(1,\ 1) = \omega'(1,\ b) = k(1) \tag{4}$$

$$\omega'(a,\ 1) = k(a)\ k(1)\ k(a)^{-1} \tag{5}$$

On montre qu'on ne restreint nullement la généralité en convenant que :

$$k(1) = 1 \quad , \text{ élément neutre de } E \tag{6}$$

ce qui entraîne :

$$\omega(a,\ 1) = \omega(1,\ a) = \omega(1,\ 1) = 0 \tag{7}$$

De même (7) entraîne (6). Lorsque ces deux relations seront satisfaites nous dirons que le système de facteur ω est normalisé. Nous conviendrons toujours de (6) dans ce qui suit.

Remarquons que pour définir le système de facteur $\omega'(a,\ b)$ nous n'avons pas utilisé le fait que A est abélien. Nous allons explicitement l'utiliser maintenant.

Nous noterons $a\alpha$ l'élément de A qui correspond à α par l'automorphisme $g(a)$ (voir diagramme 1) ; comme nous l'avons vu (page 16, texte du diagramme I. 5a), cela définit la façon dont E opère sur G : Si $k(a)$ est un élément du translaté a de E,

$$k(a) \quad \alpha \quad = \quad a\alpha \tag{8}$$

ou encore, pour E, $k(a)$ définit un automorphisme intérieur, et

$$k(a) \quad \alpha' \ k(a)^{-1} = (a\alpha)'$$

que nous noterons $a\alpha'$.

Ceci nous permet de décrire le produit de deux éléments arbitraires de E

$$\begin{aligned} \alpha' k(a) \quad \beta' k(b) \quad &= \quad \alpha' k(a) \ \beta' (k(a))^{-1} \ k(a) \ k(b) \quad = \\ \alpha' \ k(a) \ \beta' \ k(\ \beta) \quad &= \quad \alpha' \ (a\beta') \quad \omega'(a,\ b) \ k(ab) \end{aligned} \tag{9}$$

Vérifions que la loi de groupe est associative. On calcule aisément :

$$\begin{aligned} \alpha' k(a) \ \beta' k(b) \ \gamma' k(c) &= \alpha'(a\beta') \ \omega\ '(a,\ b) \ \ (ab\gamma') \ \omega'(ab,c) \ \ k(abc) \\ &= \alpha'(a\beta') \ \ (ab\gamma')(a \quad '(b,c) \ \ \omega'(a,bc) \ \ k(a,b,c) \end{aligned}$$

La condition suivante :

$$\omega(a, b) + \omega(a, b, c) - \omega(a, bc) - a\,\omega(b, c) = 0 \qquad (10)$$

est donc nécessaire pour que la loi de groupe soit associative.

Réciproquement, donnons-nous les groupes A, L, l'homomorphisme $g : L \longrightarrow \mathrm{Aut}\, A$, et le système normalisé de facteurs $\omega(a, b)$, vérifiant les relations (10) et (7) ; nous pouvons alors définir une extension E de la façon suivante : un élément de E est un couple (α, a) et la loi de groupe est :

$$(\alpha, a)(\beta, b) = (\alpha + a\beta + \omega(a, b), ab) \qquad (11)$$

On vérifie immédiatement que, par suite de (10), cette loi est associative et que l'élément neutre est $(0, 1)$.

Enfin pour calculer l'inverse de (α, a) nous devons résoudre l'équation :

$$(\alpha, a)(\beta, b) = (0, 1)$$

On obtient :

$$(\alpha, a)^{-1} = (\beta, b) = (-a^{-1}\alpha - a^{-1}\omega(a, a^{-1}) \quad a^{-1})$$

et :

$$\omega(a, a^{-1}) = a\,\omega(a^{-1}, a)$$

l'inverse de (α, a) s'écrit donc encore :

$$(\alpha, a)^{-1} = (-a^{-1}\alpha - \omega(a^{-1}, a)\ , a^{-1}) \qquad (12)$$

La condition (10) est donc nécessaire et suffisante pour que la fonction $\omega(a, b)$ définisse, à l'aide de l'équation (11), une extension de L par A.

Comment ω (a, b) dépend-il du choix de la fonction k(a) ? Choisissons une autre fonction $\hat{k}(a)$, satisfaisant elle aussi la condition (1). Définissons la fonction φ' :

$$\varphi'(a) = k(a) \left[\hat{k}(a)\right]^{-1} \qquad (13)$$

Puisque k(a) et $\hat{k}(a)$ appartiennent au même translaté a de A, $\varphi(a) \in A$. L'équation (3) s'écrit :

$$\varphi'(a)\, \hat{k}(a)\, \varphi'(b)\, \hat{k}(b) = \omega'(a, b)\, \varphi'(ab)\, \hat{k}(ab)$$

le premier membre peut êtretransformé par (13) en :

$$\varphi'(a)\, \big(a\, \varphi'(b)\big)\, \hat{k}(a)\, \hat{k}(b) = \varphi'(a)\, \big(a\, \varphi'(b)\big)\, \hat{\omega}(a,b)\, \hat{k}(ab)$$

d'où la relation entre le nouveau système de facteur $\hat{\omega}(a,b)$ et l'ancien $\omega(a,b)$:

$$\omega(a,b) - \omega(a, b) = \theta(a,b) \qquad (14)$$

où

$$\theta(a,b) = \varphi(ab) - \varphi(a) - a\, \varphi(b) \qquad (15)$$

Notons que $\theta(a,b)$ satisfait lui-même à la relation (10), qui caractérise les systèmes de facteurs. On dit que $\vartheta(a,b)$ est un système de facteurs trivial. Si on a un système de facteur $\theta(a,b)$ obtenu avec la fonction $\hat{k}(a)$ et satisfaisant (15) on peut prendre la fonction k(a) définit par (13) : $k(a) = \varphi'(a)\, \hat{k}(a)$ et le nouveau système de facteur obtenu $\omega(a,b)$ sera identiquement nul. Il s'agira donc d'un produit semi-direct.

De facon plus générale, deux extensions de L par A abélien, correspondant au même homomorphisme $L \xrightarrow{g}$ Aut A, et données par leurs systèmes de facteurs $\omega(a,b)$ et $\omega_2(a,b)$ sont équivalentes s'il existe $\theta(a,b)$ de la forme (15) telle que $\omega_1(a,b) - \omega_2(a,b) = \theta(a,b)$. En effet il suffit de poser $\hat{k}(a) = \varphi(a)\, k_1(a)$ et constater alors que $\widehat{\omega_1}(a,b) = \omega_2(a,b)$

Nous allons maintenant étudier la réciproque : quelle relation existe-t-il entre les systèmes de facteurs de deux extensions équivalentes, au sens défini en I. 6 (Page 17).