Enseignement du troisième cycle
de la Physique en Suisse Romande (CICP)

Semestre d'hiver 1971-1972

Extensions et Cohomologie de groupes

E. Ascher

Battelle Institute, Advanced Studies Center
1227 Carouge, Geneva - Switzerland

0 Introduction

0.1 Préface

Ce cours est consacré à certaines méthodes contemporaines utilisées en théorie de groupes et en algèbre. Il sera organisé autour d'une étude des extensions de groupes et de la cohomologie de groupes.La cohomologie de groupes est importante dans l'étude des extensions parce qu'elle permet de relier ce chapitre particulier de la théorie des groupes à des problèmes que l'on rencontre un peu partout en algèbre. La cohomologie de groupes est née d'ailleurs de la rencontre de la théorie des extensions avec certains problèmes topologiques. Ainsi une étude de la cohomologie de groupes place la théorie des extensions dans un contexte mathématique plus large. Du même coup, elle met à la disposition de ceux qui s'intéressent aux extensions des moyens développés dans d'autres branches des mathématiques. Les avantages se font sentir jusqu'au calcul explicite des extensions.

Mais où rencontre-t-on des extensions ? Partout. Le groupe d'Euclide est une extension du groupe des translations par un groupe orthogonal, de même le groupe de Poincaré. Ces extensions-là sont d'un type simple que nous appellerons plus tard trivial : ce sont des produits semi-directs. Les sous-groupes de ces groupes sont encore des extensions d'un sous-groupe du groupe des translations par un sous-groupe d'un groupe orthogonal, mais d'un type plus compliqué : ce ne sont plus des produits semi-directs. La théorie des extensions révèle la structure de ces groupes. Elle montre aussi comment à partir de deux groupes donnés on peut construire un nouveau groupe, l'extension de l'un par l'autre. L'extension n'est pas la seule manière de construire un nouveau groupe à partir de deux groupes donnés, mais c'est celle que l'on rencontre souvent "en nature", i.e. dans les théories mathématiques utilisées pour décrire la nature. Ainsi on a beaucoup étudié ces derniers temps la façon dont on peut construire à partir du groupe de Poincaré (ou d'Euclide) et d'un groupe dit de symétrie interne un groupe de symétrie totale pour une classe de particules élémentaires.

Dans ce cours notre but n'est pas d'étudier telle ou telle extension particulière. Nous nous efforcerons de nous familiariser avec certaines notions et certaines méthodes utiles dans la théorie des extensions et l'algèbre cohomologique qui se rapportent à ce problème. Ces méthodes ont leur importance aussi en dehors des problèmes d'extension. Nous aborderons quelques extensions particulières dans le dernier chapitre du cours, dans lequel nous étudierons des sous-groupes des groupes d'Euclide et de Poincaré.

Ces notes ont été rédigées avant chaque cours. Avant d'être distribuées, la semaine suivante, elles ont été revues et améliorées par T. Dreyfus. Je tiens à le remercier pour la façon lucide et efficace dont il s'est acquitté de cette tâche.

0.2 Bibliographie

a Les articles importants dans la théorie des extensions ont été écrits par les auteurs suivants :

HÖLDER, O.: Die Gruppen der Ordnung p^3, pq^2, pqr, p^4; Math. Annalen 43 (1893) 301.

SCHREIER, O.: Über die Erweiterung von Gruppen;
I: Monatshefte Math. und Phys. (Wien) 34 (1926) 165;
II: Abh. Math. Seminar, Hamburg Univ. 3 (1923) 321.

BAER, R.: Erweiterung von Gruppen und ihren Isomorphismen, Math. Zeitschrift 38 (1934) 375.

TURING, A.M.: The extensions of a group, Compositio Mathematica 5 (1938) 357.

EILENBERG, S. + MACLANE, S.: Group extensions and homology, Ann. of Math. 4 (1942) 757.

ECKMANN, B.: Der Cohomologie-Ring einer beliebigen Gruppe, Comm. Math. Helv. 18 (1945) 232.

EILENBERG, S. + MACLANE S.: Cohomology theory in abstract groups; I: Ann. of Math. 48 (1947) 51;
II: Ann. of Math. 48 (1947) 326.

FADDEEV, D.K.: O factor-sistemah v abelevyh gruppah s operatorami, Dokl. Ak. Nauk SSSR 58 (1947) 361.

b Plus important est de connaître quelques livres utiles. Un livre qui contient un bon exposé de la théorie des extensions (avec quelques rudiments de cohomologie) et qui est d'ailleurs l'un des meilleurs qui soient sur la théorie des groupes, précis mais non pédantique, d'une lecture agréable est

KUROSH, A.G.: The thoery of groups I and II, Chelsea, New York, 1960.

Un autre bon livre est

HALL, M., Jr.: The theory of groups. MacMillan, New York, 1959.

Hall a d'ailleurs lui-même contribué à la théorie des extensions de groupes.

Un dernier livre sur la théorie des groupes que je voudrais recommander est

ROTMAN, J.J.: The theory of groups, an introduction. Allyn + Bacon, Boston, 1965.

Il est plus élémentaire que les deux précédents, mais contient un choix de sujets importants, dont les extensions et l'algèbre homologique, traités dans un esprit moderne. La lecture en est passionnante. En ce qui concerne l'algèbre elle-même des livres utiles à consulter me semblent être les suivants :

MACLANE, S. + BIRKHOFF, G.: Algebra, MacMillan, New York, 1967. Traduction française: Gauthier-Villars, Paris, 1970.

LANG, S.: Algebra, Addison-Wesley, Reading 1965.

On trouvera une bonne discussion de la cohomologie des groupes dans (le livre anglais!)

MACLANE, S.: Homology, Springer, Berlin 1963.

Mais

NORTHCOTT, D.G.: An introduction to homological algebra, Cambridge University Press, 1960,

peut aussi être utile.

c Pour ce que nous comptons dire des sous-groupes des groupes d'Euclide et de Poincaré les articles ci-dessous seront utiles.

BIEBERBACH, L.: Über die Bewegungsgruppen der Euklidischen Räume; I: Math. Annalen 70 (1911) 297, II: Math. Annalen 72 (1912) 400.

FROBENIUS, G.: Über die unzerlegbaren diskreten Bewegungsgruppen, Sitzber. preuss. Ak. Wiss., Phys.-Math. Kl. (1911) 654.

BURCKHARDT, J.J.: Zur Theorie der Bewegungsgruppen, Comm. Math. Helv. 6 (1933) 159.

ZASSENHAUS, H.: Über einen Algorithmus zur Bestimmung der Raumgruppen, Comm. Math. Helv. 21 (1948) 117.

ASCHER E. + JANNER A.: Algebraic Aspects of crystallography. I: Space groups as extensions, Helv. Phys. Acta 38 (1965) 551, II: Non-primitive translations in space groups, Commun. Math. Phys. 11 (1968) 138.

JANNER A. + ASCHER E.: Crystallographic concepts for inhomogeneous subgroups of the Poincaré group, Physica 54 (1971) 77.

1 Préparation

Un but de cette préparation est de rappeler brièvement quelques notions sur les structures algébriques et sur les applications qui conservent ces structures. Nous nous efforcerons de mentionner tout ce dont nous aurons besoin dans la suite, mais évidemment très rapidement, car je suppose que la plupart d'entre vous ont déjà rencontré et utilisé la plupart des notions introduites dans ce chapitre. Un autre but est de préciser le vocabulaire et d'introduire certaines notations. Ici et là nous serons légèrement plus généraux que strictement nécessaire; ceci dans l'intention d'ouvrir des perspectives même si leur exploration ultérieure dépasse le cadre de ce cours. Enfin, cette préparation doit nous servir en quelque sorte aussi "à chauffer nos muscles".

1.1 Applications

D Soient X et Y deux ensembles. Une application f de X à Y fait correspondre à chaque élément x de X ($x \in X$) un et un seul

D élément fx de Y ($fx \in Y$). L'ensemble X est appelé le domaine de f:

$$\text{Dom } f = X \quad .$$

D L'ensemble Y est appelé le codomaine de f.

$$\text{Cod } f = Y \quad .$$

Nous écrirons

$$f : X \longrightarrow Y$$

ou

$$X \xrightarrow{f} Y \quad .$$

Pour indiquer que l'application f applique (envoie) l'élément $x \in X$ sur l'élément $fx \in Y$ nous utiliserons la flèche barrée :

$$x \longmapsto fx \quad .$$

D L'image, Im f, de $f : X \longrightarrow Y$ est l'ensemble de tous les éléments $fx \in Y$:

$$\mathrm{Im}\, f = \{y \in Y \mid \exists x \in X \quad fx = y\} \quad .$$

Nécessairement

$$\mathrm{Im}\, f \subset \mathrm{Cod}\, f \quad .$$

Dans notre usage la relation d'inclusion, notée par le signe $\subset$,

D n'exclut pas l'égalité. Une application f est surjective (une surjection, une application sur) si elle satisfait à (S) :

(S) $\mathrm{Im}\, f = \mathrm{Cod}\, f$.

En d'autres termes, si pour tout $y \in Y$ il existe un $x \in X$ tel que $fx = y$, ce que nous écrivons symboliquement

$$\forall y \in Y \quad \exists x \in X \quad fx = y \quad .$$

Remarquons à cet endroit que nous noterons parfois la tournure "tel que" (au masculin et féminin du singulier et du pluriel) par "$\ni$". Aussi le signe "ssi" signifiera "si et seulement si". Dans une définition chaque "si" est évidemment un "ssi" sans que l'on l'écrive expressément.

D Deux applications f et g sont égales si

(i) $\mathrm{Dom}\, f = \mathrm{Dom}\, g$

(ii) $\mathrm{Cod}\, f = \mathrm{Cod}\, g$

(iii) $\forall x \in \mathrm{Dom}\, f \quad fx = gx$.

Considérons maintenant deux applications f et g définies comme suit :

$$f : \mathbb{R} \longrightarrow \mathbb{R}$$

$$f : x \longmapsto x^2$$

et

$$g:\ \mathbb{R} \longrightarrow \mathbb{R}^+$$
$$g:\ x \longmapsto x^2 \quad .$$

Ici $\mathbb{R}$ désigne l'ensemble des nombres réels et $\mathbb{R}^+$ l'ensemble des nombres réels non négatifs. D'après notre définition

$$f \neq g \quad .$$

En effet g est surjectif tandis que f ne l'est pas. Pour que la notion de surjectivité ait un sens, il faut bien inclure la condition de l'égalité des codomaines dans la définition de l'égalité de deux applications.

D Une application f est <u>injective</u> (une injection, 1 à 1) si elle satisfait à (I) :

(I) $\forall x_1, x_2 \in \mathrm{Dom}\, f \qquad fx_1 = fx_2 \Longrightarrow x_1 = x_2 \quad .$

Ici le signe "$\Longrightarrow$" doit être lu de la façon suivante: "$fx_1 = fx_2$ entraîne $x_1 = x_2$" ou "si $fx_1 = fx_2$ alors $x_1 = x_2$". Un signe $\Longleftrightarrow$ signifiera la même chose que "ssi". En prenant le négatif de la définition (I), on peut donc dire qu'une application est injective si elle envoie des éléments distincts de son domaine en éléments distincts de son codomaine.

D Si $X \subset Y$ nous appellerons <u>injection naturelle</u> ou <u>insertion</u> ou encore <u>inclusion</u> l'application f qui à chaque $x \in X$ fait correspondre l'élément $x \in Y$:

$$\forall x \in X \qquad fx = x \in Y \quad .$$

Dans les diagrammes, nous mettrons souvent entre parenthèses, (f), ces insertions et dans les formules nous les omettrons de préférence.

D Etant donné un ensemble X, l'<u>application identité</u>

$$1_X:\ X \longrightarrow X$$

est l'application qui envoie chaque élément de X sur lui-même:

$$1_X: \; x \longmapsto x \quad .$$

Soient f et g deux applications telles que

$$\mathrm{Cod}\, g = \mathrm{Dom}\, f \quad .$$

D Alors l'application fg, dite <u>application composée</u> ou <u>application produit</u> , est définie ainsi

$$fg: \; \mathrm{Dom}\, g \longrightarrow \mathrm{Cod}\, f$$

$$fg: \; x \longmapsto f(gx) \quad .$$

Notez que fg signifie chez nous d'abord g et après f :

$$\mathrm{Dom}\, g \xrightarrow{g} \mathrm{Cod}\, g \xrightarrow{f} \mathrm{Cod}\, f \quad .$$

On peut exprimer cette définition à l'aide de la notion de

D <u>diagramme commutatif</u>. Un diagramme d'ensembles et d'applications est commutatif si tout chemin menant le long de flèches du diagramme d'un ensemble à un autre définit la même application. Soient alors deux applications f: Y -> Z et g: X -> Y. La définition du composé fg peut s'exprimer en disant que le diagramme suivant est commutatif :

$$\begin{tikzcd} X \arrow[r, "g"] \arrow[dr, "fg"'] & Y \arrow[d, "f"] \\ & Z \end{tikzcd}$$

La composition d'applications obéit à la loi associative; c'est-à-dire

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

chaque fois que les composés qui interviennent sont définis. C'est une conséquence de la définition d'une application composée. En terme de diagramme l'associativité veut dire que le diagramme suivant est commutatif :

$$\begin{tikzcd} \bullet \arrow[r, "h"] \arrow[d] \arrow[dr] & \bullet \arrow[d, "g"] \arrow[dl] \\ \bullet & \bullet \arrow[l, "f"] \end{tikzcd} \quad .$$

Soit $j\colon\ X \longrightarrow Y$ une insertion et $f\colon\ Y \longrightarrow Z$ une application. Le composé fj est une application de X en Z que

D l'on appelle la <u>restriction</u> de f à X et que l'on note aussi f_X.

$$f_X = fj\colon\ X \longrightarrow Z \quad .$$

Soit

$$f\colon\ X \longrightarrow Y \quad ;$$

une application g

$$g\colon\ Y \longrightarrow X$$

D est appelé <u>inverse à gauche</u> (respectivement inverse à droite) de f, si

$$gf = 1_X \qquad (\text{resp. } fg = 1_Y) \quad .$$

Si les deux relations

$$gf = 1_X \quad \text{et} \quad fg = 1_Y$$

D sont vérifiées g est appelé <u>inverse</u> de f.

<u>Proposition 1.1</u>. Une application (avec domaine non vide) est une injection ssi elle a un inverse à gauche.

<u>Dém.</u>: Supposons que

$$f\colon\ X \longrightarrow Y$$

a un inverse à gauche

$$g\colon\ Y \longrightarrow X \ :$$

$$gf = 1_X \quad .$$

Soit

$$fx_1 = fx_2 \quad .$$

Il s'ensuit

$$gfx_1 = gfx_2$$

et

$$x_1 = x_2 \quad ,$$

ce qui signifie que f est injective. Supposons, réciproquement, que f soit injective. Pour chaque $y \in \mathrm{Im}\, f$, il existe alors un unique $x \in X$ tel que $fx = y$:

$$\forall y \in \mathrm{Im}\, f, \ \hat{\exists} x \in X, \ \ fx = y \quad .$$

(Notez que nous employons le signe "$\hat{\exists}$" pour signifier "il existe un unique".) Désignons alors cet unique élément x par gy et posons $gy = x_o \in X$ chaque fois que y n'est pas dans l'image de f:

$$gy = x \qquad\qquad \text{si } fx = y$$

$$gy = x_o \qquad\qquad \text{si } y \notin \mathrm{Im}\, f \quad .$$

(Le signe "$\notin$" signifie "n'est pas élément".) Nous avons défini ainsi une application

$$g: \ Y \longrightarrow X$$

et évidemment

$$\forall x \in X \qquad gfx = x \qquad . \ //$$

(Le signe "//" signifie "fin de la démonstration".) Notez qu'une injection f, qui n'est pas une surjection, n'a pas d'inverse à gauche unique; il y a un inverse à gauche pour chaque choix de x_o dans la démonstration.

<u>Proposition 1.2</u> . Une application f (avec domaine non vide) est une surjection ssi elle a un inverse à droite .

<u>Dém.</u>: Exercice 1.a. La démonstration utilise l'axiome de choix que l'on peut énoncer comme suit. Soit X un ensemble, $\{X_i\}$ une famille de sous-ensembles non-vides et disjoints de X. Il existe une fonction f, dite fonction de choix, définie sur $\{X_i\}$ et dont les valeurs sont des éléments de X, telle que

$$f(X_i) = x_i \in X_i \qquad .$$

Une application qui est à la fois injective et surjective est <u>bijective</u> (une bijection).

D

<u>Proposition 1.3</u> . Soient X et Y des ensembles non-vides et f une application $f = X \longrightarrow Y$. Les propriétés suivantes sont équivalentes

(i) f est une bijection

(ii) f a un inverse à gauche g et un inverse à droite d

(iii) f a un inverse j .

<u>Corollaire</u>. Une bijection f a un inverse unique, et bijectif, noté f^{-1} .

$$f^{-1} = g = d = j \quad .$$

<u>Dém</u>.: de la proposition et du corollaire: Exercice 1.b.

<u>Proposition 1.4</u> . Soient $f\colon Y \longrightarrow Z$ et $g\colon X \longrightarrow Y$ deux bijections. Alors fg est une bijection et

$$(fg)^{-1} = g^{-1}f^{-1} \quad .$$

<u>Dém</u>.: Exercice 1.c.

<u>Proposition 1.5</u> .

(i) L'application f est injective ssi, fg et fg' étant définis, on a la propriété (M) suivante :

(M) $fg = fg' \Longrightarrow g = g'$.

(ii) L'application f est surjective ssi, gf et g'f étant définis, on a la propriété (E) suivante :

(E) $gf = g'f \Longrightarrow g = g'$.

<u>Dém</u>.: Exercice 1.d. (Il est plus facile de démontrer que non-surjective implique non-(E).)

Remarque : On peut énoncer la propriété (M) en disant

D que f est <u>simplifiable à gauche</u>; d'une façon analogue, une

D fonction satisfaisant à (E) est dite <u>simplifiable à droite</u>.

Proposition 1.6 .

(i) Si fg est une injection, g est une injection.

(ii) Si fg est une surjection, f est une surjection.

(iii) Si fg est une bijection, g est une injection et f est une surjection.

Dém.: Exercice 1.e.

D Le produit cartésien $X \times Y$ de deux ensembles X et Y est l'ensemble des couples (x,y) avec $x \in X$ et $y \in Y$.

$$X \times Y = \{(x,y) \mid x \in X, y \in Y\}$$

soient $f\colon X \longrightarrow F$ et $g\colon Y \longrightarrow G$ deux applications.

D Le produit cartésien $f\times g\colon X\times Y \longrightarrow F\times G$ est défini ainsi:

$$(f\times g)(x,y) = (fx, gy) \quad .$$

1.2 Structures algébriques

Notre exposé tournera autour de la notion de groupe. Les groupes ne seront pas pour autant les seuls objets auxquels nous aurons affaire. Nous rencontrerons aussi des anneaux, des modules, etc. Tous ces objets sont des ensembles ayant une structure algébrique et qui vous sont plus ou moins connus. Nous les rappellerons ici seulement très brièvement.

D Soit **S** un ensemble. Une <u>loi interne</u> (ou loi de composition, ou opération algébrique) n-aire (ou d'ordre n) sur S est une application :

$$\Lambda : \underbrace{S\times\ldots\times S}_{n\text{-fois}} \longrightarrow S \quad .$$

Pour n=0 une opération algébrique consiste du choix d'un élément de S indépendant des autres éléments de S.

Soient Ω_i (i:1,2,...) et S des ensembles. On appelle

D <u>loi externe n-aire</u> (ou <u>opération n-aire</u>) sur S une application

$$\phi : \Omega_1 \times\ldots\times \Omega_n \times S \longrightarrow S \quad ;$$

on voit que l'application ϕ induit une application

$$\varphi : \Omega_1 \times\ldots\times \Omega_n \longrightarrow S^S$$

dans l'ensemble S^S des applications de S dans S. Les ensembles

D Ω_i s'appellent <u>domaines d'opérateurs</u>, leurs éléments s'appellent

D <u>opérateurs</u>.

D Une <u>structure algébrique</u> sur un ensemble S consiste en une ou plusieurs lois internes Λ_j et une ou plusieurs lois externes ϕ_j, ces lois pouvant être assujetties à satisfaire à certaines conditions. Dans tous les exemples de structure qui vont suivre l'ordre des lois internes ne dépassera pas 2 et, sauf mention du contraire, loi interne signifiera toujours loi interne binaire. Aussi chaque loi externe sera définie pour un seul domaine d'opérateurs mais il pourrait y avoir plusieurs lois externes.

Un <u>semigroupe</u> $(S,\cdot)$ est un ensemble S avec une loi interne

$$S \times S \longrightarrow S$$

$$(s_1,s_2) \longmapsto s_1 \cdot s_2$$

qui est associative

$$(s_1 \cdot s_2) \cdot s_3 = s_1 \cdot (s_2 \cdot s_3) \qquad .$$

Si la loi est commutative

$$s_1 \cdot s_2 = s_2 \cdot s_1$$

D on dit que le semigroupe est abélien.

Les éléments de S^S, par exemple, forment un semigroupe si l'on prend comme loi interne la composition des applications.

Disons dès maintenant que nous parlerons le plus souvent - par abus - du semigroupe S et que nous omettrons les signes spéciaux des différentes lois internes ou externes chaque fois que cela est possible sans nuire à la clarté.

D Un monoïde $(S,\cdot)$ est un semigroupe avec élément unité 1

$$1 \cdot x = x \cdot 1 = x \quad .$$

Puisque dans S^S, il y a un élément unité, cet ensemble forme aussi un monoïde.

En notation additive, nous écrivons o pour l'élément unité

$$o + x = x + o = x \quad .$$

D Un groupe $(S,\cdot)$ est un monoïde où chaque élément a un inverse :

$$\forall x \in S \quad \exists\, x^{-1} \in S \quad xx^{-1} = x^{-1}x = 1$$

D Un groupe à opérateurs $(\Omega, S, \cdot, *)$ consiste de deux ensembles et de deux lois tels que $(S,\cdot)$ soit un groupe et

$$* : \Omega \times S \longrightarrow S$$

$$* : (\omega, s) \longmapsto \omega * s$$

D une loi externe qui est distributive par rapport à la loi du groupe

$$\omega * (s \cdot t) = (\omega * s) \cdot (\omega * t) \quad .$$

D L'ensemble Ω est appelé domaine d'opérateurs. Ce sont des groupes à opérateurs qui jouent un très grand rôle dans tout

D ce qui va suivre. Les plus importants seront les G-modules. C'est un groupe à opérateurs où le groupe est abélien, le domaine d'opérateurs un groupe et où la loi externe remplit deux conditions supplémentaires. Plus exactement un G-module $(G,M,+,*,\cdot)$ consiste de deux ensembles et de trois lois tels que $(M,+)$ soit un groupe abélien, $(G,\cdot)$ un groupe et où la loi externe $* : G \times M \to M$ satisfait aux trois conditions

$$\forall\alpha \in G, \quad \forall a,b \in M, \quad \alpha*(a+b) = (\alpha*a)+(\alpha*b)$$

$$1 \in G, \quad \forall a \in M, \quad 1*a = a$$

$$\forall\alpha,\beta \in G, \quad \forall a \in M, \quad (\alpha\cdot\beta)*a = \alpha*(\beta*a) \quad .$$

Nous parlerons dans ce cas du G-module M et nous écrirons le plus souvent les trois lois ci-dessus simplement ainsi

$$\alpha(a+b) = \alpha a+\alpha b$$

$$1a = a$$

$$(\alpha\beta)a = \alpha(\beta a) \quad .$$

Pour terminer ce paragraphe 1.2, il serait instructif d'établir une liaison entre la notion de G-module et celle plus générale d'un module sur un anneau R.

Pour ce faire nous rappellerons d'abord la définition

D d'un anneau. Un <u>anneau</u> avec unité $(R,\boldsymbol{*},\cdot)$ consiste d'un ensemble R et des deux lois internes $\boldsymbol{*}$ et $\cdot$ appelées respectivement addition et multiplication et telles que $(R,\boldsymbol{*})$ soit un groupe abélien, $(R,\cdot)$ un monoïde et que $\cdot$ soit distributive par rapport à $\boldsymbol{*}$, à gauche et à droite

$$a\cdot(b\boldsymbol{*}c) = (a\cdot b)\boldsymbol{*}(a\cdot c)$$

$$(b\boldsymbol{*}c)\cdot a = (b\cdot a)\boldsymbol{*}(c\cdot a) \quad .$$

D On dit que l'<u>anneau</u> est <u>commutatif</u> si la loi $\cdot$ est commutative.

D Un <u>corps</u> K est un anneau K dans lequel l'ensemble $K^{\cdot}$ des éléments $\neq$ o est un groupe pour la loi de multiplication de K.

Remarque : C'est la nouvelle terminologie, employée par exemple par KUROŠ et par BOURBAKI. Mais dans beaucoup de livres, on appelle corps ce que nous appellerions corps commutatif. S'il s'agit d'un corps non-commutatif on le dit explicitement. En anglais on dit alors aussi "skew-field" ou "division-ring", en allemand "Schiefkörper".

D Un <u>module à gauche, M, sur un anneau R</u> (brièvement <u>R-module</u>) est un groupe abélien M avec un domaine d'opérateurs R qui est un anneau et qui en plus de la condition de distributivité (liée à la définition de "domaine d'opérateurs")

$$\forall\alpha \in R, \quad \forall a,b \in M \qquad \alpha(a+b) = \alpha a+\alpha b$$

satisfait à deux autres conditions

$$\forall\alpha,\beta \in R \quad \forall a \in M \quad \begin{cases} (\alpha+\beta)a = \alpha a+\beta a \\ (\alpha\beta)a = \alpha(\beta a) \end{cases}$$

et à une règle qui précise l'action de l'unité multiplicative de l'anneau

$$1a = a \quad .$$

Nous aurons besoin peut-être de bimodules. Un groupe

D abélien M est un <u>(R,S)-bimodule</u> si c'est un R-module et un S-module et si les opérations sur M, de R et de S commutent. Si R et S opèrent à gauche, cette dernière condition s'écrit

$$\forall a \in M, \quad \forall r \in R, \quad \forall s \in S \qquad r(sa) = s(ra).$$

Si R opère à gauche et S à droite, on a

$$(ra)s = r(as) \quad .$$

Certains modules ressemblent beaucoup aux espaces vectoriels. Ce sont les modules libres. Soit M un module et $[u_i]_{i\in I}$ une famille d'éléments indexés par un ensemble I. Un sous-ensemble L_u de M constitué par tous les éléments de la forme

$$\sum_{i \in I} \lambda_i u_i \quad ,$$

où seulement un nombre fini de $\lambda_i \in R$ est différent de zéro,

D constitue un sous-module de M. Ce sous-module est dit engendré par $[u_i]_{i \in I}$. Si ce sous-module L_u coïncide avec le module M lui-même on dit, évidemment, que les $[u_i]_{i \in I}$ engendrent M et

D on les appelle (un système de) générateurs de M.

Soit $[u_i]_{i \in I}$ un système de générateurs de M. Alors chaque élément $m \in M$ peut s'écrire

$$m = \sum_i \lambda_i u_i$$

Si les λ_i de cette expression sont uniques (i.e. si

$$m = \sum \lambda_i u_i = \sum \mu_i u_i$$

D entraîne $\lambda_i = \mu_i$) alors les $[u_i]$ sont appelés base sur R de

D M ou générateurs libres de M.

D Un module libre est un module qui admet une base. Un module sur un anneau R n'est pas nécessairement libre, mais tout module sur un corps K (i.e. tout espace vectoriel) est un module libre.

Tout groupe abélien M peut être considéré comme module sur les entiers $\mathbb{Z}$:

$$\forall a \in M \qquad \underbrace{a+\dots+a}_{n \text{ fois}} = na$$

Nous avons défini les G-modules. On peut montrer qu'ils peuvent être considérés comme modules sur un certain anneau. Décrivez cet anneau (Exercice 1.f).

1.3 Catégories, morphismes

Soient A et B deux ensembles munis de structures algébri-
D ques du même type. Un homomorphisme $\phi: A \to B$ est une application d'ensembles $A \longrightarrow B$ qui conserve la structure.

Par "même type" il faut entendre qu'il y a une correspondance biunivoque entre les lois internes et externes définissant les deux structures et que ces lois satisfont aux mêmes conditions; A et B sont par exemple des groupes, des espaces vectoriels, des anneaux, etc.

Explicitons maintenant la "conservation de structure" à l'aide de l'exemple des groupes. Soient donc $(A,+)$ et $(B,\cdot)$ deux groupes. Un homomorphisme $\phi: A \to B$ est une application telle que

$$\forall a_1, a_2 \in A \qquad \phi(a_1+a_2) = \phi a_1 \cdot \phi a_2 \quad .$$

On peut représenter la conservation de structure à l'aide d'un diagramme commutatif. On a les applications

$$+ : \; A \times A \longrightarrow A$$

$$\cdot : \; B \times B \longrightarrow B$$

$$\phi : \; A \longrightarrow B$$

$$\phi \times \phi : \; A \times A \longrightarrow B \times B \quad .$$

Le diagramme en question est celui-ci :

$$\begin{tikzcd} A \times A \arrow[r, "\phi \times \phi"] \arrow[d, "+"'] & B \times B \arrow[d, "\cdot"] \\ A \arrow[r, "\phi"'] & B \end{tikzcd}$$

Soient maintenant A et B deux G-modules. Un homomorphisme λ de G-modules est une application de A à B qui

(i) est un homomorphisme des groupes abéliens et

(ii) conserve la structure de groupe à opérateurs :

$$\lambda\left[\alpha^*(a_1+a_2)\right] = \alpha^*\left[\lambda(a_1+a_2)\right] = \alpha^*\left[\lambda a_1+\lambda a_2\right] \quad .$$

avec $\alpha \in G$ et $a_1, a_2 \in A$. Les conditions (i) et (ii) sont représentées par le diagramme suivant :

$$\begin{tikzcd} G\times A \arrow[r, "1_G\times\lambda"] \arrow[d, "*"'] & G\times B \arrow[d, "*"] \\ A \arrow[r, "\lambda"'] & B \end{tikzcd}$$

Ce diagramme nous suggère la généralisation ci-dessous qui nous sera utile dans la suite :

$$\begin{tikzcd} G\times A \arrow[r, "\gamma\times\lambda"] \arrow[d] & H\times B \arrow[d] \\ A \arrow[r, "\lambda"'] & B \end{tikzcd}$$

Il s'agit d'un diagramme qui décrit un homomorphisme entre le G-module A et le H-module B et où γ est un homomorphisme de groupes γ: G → H.

L'existence d'un élément unité dans un groupe (dans un G-module, etc) nous permet d'introduire deux notions utiles.

D L'homomorphisme trivial o est un homomorphisme qui applique tout élément du domaine sur l'élément unité du codomaine :

$$o: A \to B$$

$$o: a \mapsto 1 \in B \quad .$$

D Le noyau, Ker ϕ, d'un homomorphisme de groupes ϕ: A → B est l'ensemble des éléments du domaine qui sont envoyés sur l'élément unité du codomaine :

$$\mathrm{Ker}\ \phi = \{a \in A \mid \phi a = 1 \in B\} \quad .$$

Ce noyau n'est jamais vide; il contient l'élément unité du domaine. Le noyau est un sous-groupe normal du domaine. Le noyau d'un homomorphisme ϕ de G-modules est évidemment le noyau de l'homomorphisme sous-jacent, ϕ, de groupes abéliens.

Soit ϕ: $A \to B$ un homomorphisme de groupe; son noyau $K = \mathrm{Ker}\ \phi$ satisfait au diagramme commutatif suivant :

$$\begin{tikzcd} K \arrow[r] \arrow[d, "i"'] & \{1\} \arrow[d] \\ A \arrow[r, "\phi"'] & B \end{tikzcd}$$

Ici i est l'injection naturelle du sous-groupe K dans A et {1}
D est le <u>groupe trivial</u> qui contient un seul élément - l'élément
unité.

Nous allons maintenant introduire quelques homomorphismes spéciaux.

Un homomorphisme de groupes surjectif est appelé
D <u>épimorphisme de groupes</u>. Un homomorphisme de groupes injectif
D est appelé <u>monomorphisme de groupes</u>. Un homomorphisme de groupes
D bijectif est appelé <u>isomorphisme de groupes</u>. J'ai pris soin
d'utiliser dans ces définitions le qualificatif "de groupes". Ce parce que dans les publications contemporaines en théorie des catégories on distingue une surjection d'un épimorphisme, une injection d'un monomorphisme et une bijection d'un isomorphisme. Dans le cas des groupes cependant les deux notions coïncident.

Il est utile ici d'introduire la notion de catégorie. Une

D catégorie C consiste en

(i) une classe $Ob(C)$ d'objets

(ii) une classe $Mor(C)$ d'ensembles $Mor(A,B)$ (dont les éléments sont appelés morphismes de A à B), un tel ensemble correspondant à chaque paire ordonnée (A,B) d'objets de C $[A,B \in Ob(C)]$

D (iii) une loi de composition de morphismes, i.e. d'une application

$$Mor(B,C) \times Mor(A,B) \longrightarrow Mor(A,C)$$

définie pour chaque triplet ordonné (A,B,C) d'objets de C $[A,B,C \in Ob(C)]$.

Ces trois données sont sujettes aux trois conditions suivantes :

CAT 1: Deux ensembles $Mor(A,B)$ et $Mor(A',B')$ sont disjoints sauf si $A = A'$ et $B = B'$.

CAT 2: La loi de composition est associative.

CAT 3: Pour chaque objet A de la catégorie il existe un morphisme $1_A \in Mor(A,A)$ qui -- pour tout objet B de la catégorie -- est une unité droite pour les éléments de $Mor(A,B)$:

$$\forall f \in Mor(A,B) \qquad f1_A = f$$

et est une unité gauche pour les éléments de $Mor(B,A)$

$$\forall g \in Mor(B,A) \qquad 1_A g = g \quad .$$

Remarque: Pour $A,B \in Ob(C)$ l'ensemble $Mor(A,B)$ peut être vide.

Dans la catégorie E des ensembles, les objets sont les ensembles, les morphismes sont les applications d'ensembles. Dans la catégorie G des groupes, les objets sont les groupes, les morphismes sont les homomorphismes de groupes. Dans la suite on rencontrera d'autres exemples de catégories. Essayons maintenant d'étudier les différents types de morphismes que l'on peut rencontrer.

D Un morphisme qui a un inverse à droite s'appelle <u>rétraction</u>.

D Un morphisme qui a un inverse à gauche s'appelle <u>corétraction</u>.

Considérons le diagramme suivant :

$$X \underset{h'}{\overset{h}{\rightrightarrows}} A \xrightarrow{f} B \underset{g'}{\overset{g}{\rightrightarrows}} Y$$

Un morphisme qui remplit la condition (E) de la page 1/7, i.e.

(E) $\forall g, g' : B \to Y \qquad gf = g'f \Longrightarrow g = g'$,

D s'appelle <u>épimorphisme</u>. Un morphisme qui remplit la condition (M) de la même page, i.e.

(M) $\forall h, h' : X \to A \qquad fh = fh' \Longrightarrow h = h'$,

D s'appelle <u>monomorphisme</u>. Un morphisme qui est à la fois une

D rétraction et une corétraction s'appelle <u>isomorphisme</u>.

Malheureusement, la terminologie n'est pas encore tout à fait unifiée. Ainsi, MacLane définit un monomorphisme, un épimorphisme et un isomorphisme par - respectivement - l'injectivité, la surjectivité et la bijectivité. Il appelle un morphisme

D qui remplit la condition (M) un <u>morphisme monique</u>, un morphisme

D qui remplit la condition (E) un <u>morphisme épique</u>.

Dans le cas des morphismes d'ensembles (i.e. des applications d'ensembles) les propositions 1.1, 1.2, 1.3 et 1.5 montrent qu'on a la situation suivante :

$$\begin{tikzcd}[column sep=small] (C) \arrow[rr, Leftrightarrow] \arrow[dr, Leftrightarrow] & & (I) \\ & (M) \arrow[ur, Leftrightarrow] & \end{tikzcd} \qquad \begin{tikzcd}[column sep=small] (R) \arrow[rr, Leftrightarrow] \arrow[dr, Leftrightarrow] & & (S) \\ & (E) \arrow[ur, Leftrightarrow] & \end{tikzcd} \qquad \begin{tikzcd}[column sep=small] (Is) \arrow[rr, Leftrightarrow] \arrow[dr, Leftrightarrow] & & (Bj) \\ & (Bm) \arrow[ur, Leftrightarrow] & \end{tikzcd}$$

Corétraction, injection et monomorphisme sont équivalents;
rétraction, surjection et épimorphisme sont équivalents;

isomorphisme, bijection et bimorphisme (i.e. monomorphisme + épimorphisme) sont équivalents.

Proposition 1.6 . Dans une catégorie quelconque on a les relations suivantes :

$$\begin{tikzcd}[column sep=small] (C) \arrow[rr, Rightarrow] \arrow[dr, Rightarrow] & & (I) \arrow[dl, Rightarrow] \\ & (M) & \end{tikzcd} \qquad \begin{tikzcd}[column sep=small] (R) \arrow[rr, Rightarrow] \arrow[dr, Rightarrow] & & (S) \arrow[dl, Rightarrow] \\ & (E) & \end{tikzcd} \qquad \begin{tikzcd}[column sep=small] (Is) \arrow[rr, Rightarrow] \arrow[dr, Rightarrow] & & (Bj) \arrow[dl, Rightarrow] \\ & (Bm) & \end{tikzcd}$$

Les propriétés de corétraction, rétraction et d'isomorphisme sont les plus fortes, celles de monomorphisme, d'épimorphisme et de bimorphisme les plus faibles.

Les propriétés (C) $\Longrightarrow$(I), (R)$\Longrightarrow$(S) se démontrent comme dans les propositions 1.1 et 1.2 et (I)$\Longrightarrow$(M), (S)$\Longrightarrow$(E) comme dans 1.5. Dans les démonstrations des réciproques de ces quatre propriétés, nous avions choisi des éléments spéciaux. Il n'est pas dit qu'un tel choix soit compatible avec la conservation de la structure et il faut examiner la question cas par cas.

En dehors des ensembles, je ne connais aucun cas où l'on aurait (I)$\Longrightarrow$(C) ou (S)$\Longrightarrow$(R). Les propriétés (M)$\Longrightarrow$(I) et (E)$\Longrightarrow$(S) sont vraies aussi pour les catégories suivantes : Groupes abéliens, R-modules, groupes (la démonstration n'est pas du tout triviale). La propriété (E)$\Longrightarrow$(S) n'est pas vraie pour la catégorie des anneaux ($\mathbb{Z} \subset \mathbb{Q}$ est un épimorphisme !). La propriété (M)$\Longrightarrow$(I) n'est pas vraie pour la catégorie des groupes abéliens divisibles. Un <u>groupe abélien</u> D est <u>divisible</u> si

$$\forall d \in D, \quad \forall n \in \mathbb{Z}^+ \ \exists \ d' \in D \quad nd' = d \qquad ,$$

($\mathbb{Z}^+$ désigne les entiers positifs). Cela n'est pas en contradiction avec le fait que dans la catégorie des groupes chaque monomorphisme est une injection. Pour éclaircir ce point, revenons à la définition de monomorphisme. Soient $D_1, D_2 \in Ob(\mathcal{D})$ deux groupes abéliens divisibles. Un homomorphisme de groupes $f\colon D_1 \longrightarrow D_2$ est un monomorphisme de groupes abéliens divisibles si pour tout $D \in Ob(\mathcal{D})$ et pour toute paire d'homomorphismes $g, g'\colon D \longrightarrow D_1$ on a la propriété $(M_{\mathcal{D}})$ suivante

$$fg = fg' \Longrightarrow g = g'$$

$$D \overset{g}{\underset{g'}{\rightrightarrows}} D_1 \xrightarrow{f} D_2 \quad .$$

C'est cela la définition d'un monomorphisme dans la catégorie des groupes abéliens divisibles. Il n'est pas possible de montrer qu'un tel monomorphisme soit une injection. En fait, il y a des contre-exemples; la surjection $f\colon \mathbb{Q} \longrightarrow \mathbb{Q}/\mathbb{Z}$ des groupes abéliens divisibles $\mathbb{Q}$ et $\mathbb{Q}/\mathbb{Z}$ (qui n'est pas une injection !) remplit la condition $(M_{\mathcal{D}})$; elle est donc un monomorphisme de groupes abéliens divisibles.

La propriété d'être un monomorphisme de groupes est plus forte que celle d'être un monomorphisme de groupes abéliens divisibles. En effet, un homomorphisme $f\colon D_1 \longrightarrow D_2$ entre deux groupes D_1 et D_2 (qui peuvent être des groupes abéliens divisibles) est un monomorphisme de groupes si pour tout groupe G et toute paire d'homomorphismes $h, h'\colon G \longrightarrow D_1$ on a la propriété (M_G) suivante :

$$fh = fh' \Longrightarrow h = h'$$

$$G \overset{h}{\underset{h'}{\rightrightarrows}} D_1 \xrightarrow{f} D_2 \quad .$$

De (M_G) on peut déduire que f est une injection. De plus (M_G) entraîne $(M_{\mathcal{D}})$ mais la réciproque n'est pas vraie, i.e. un monomorphisme de groupes est aussi un monomorphisme de groupes abéliens divisibles mais la réciproque n'est pas vraie.

La morale de cette histoire est la suivante. Les notions de monomorphisme, d'épimorphisme et de bimorphisme appartiennent vraiment à la théorie des catégories: tous les objets de la catégorie interviennent (et rien que ces objets). En revanche, dans la définition d'une injection et d'une surjection ou d'une rétraction et d'une corétraction seulement une paire d'objets intervient.

En ce qui concerne les morphismes de groupes (et de R-modules), nous avions trouvé les deux schémas suivants :

$$\begin{tikzcd} (C) \arrow[rr, Rightarrow] \arrow[dr, Rightarrow] & & (I) \\ & (M) \arrow[ur, Rightarrow] & \end{tikzcd} \qquad \begin{tikzcd} (R) \arrow[rr, Rightarrow] \arrow[dr, Rightarrow] & & (S) \\ & (E) \arrow[ur, Rightarrow] & \end{tikzcd}$$

et comme conséquence immédiate ce troisième schéma

$$\begin{tikzcd} (Is) \arrow[rr, Rightarrow] \arrow[dr, Rightarrow] & & (Bj) \\ & (Bm) \arrow[ur, Rightarrow] & \end{tikzcd}$$

Mais on peut démontrer plus :

<u>Proposition 1.7</u> . Un bimorphisme f de groupes (ou de R-modules) est un isomorphisme.

<u>Dém.</u>: En tant qu'application d'ensembles, f a une application d'ensembles g comme inverse

$$\begin{tikzcd} A \arrow[r, shift right, "f"'] & B \arrow[l, shift right, "g"'] \end{tikzcd} \qquad fg = 1_B \quad .$$

Cette application est aussi un homomorphisme

$$f(gx \cdot gy) = fgx \cdot fgy = x \cdot y \equiv fg(x \cdot y) \quad .$$

Puisque f est un monomorphisme donc simplifiable à gauche

$$gx \cdot gy = g(x \cdot y) \quad .$$

Ainsi, pour des groupes et R-modules, les notions de bijection, de bimorphisme et d'isomorphisme sont équivalentes :

$$\begin{tikzcd}
(Is) \arrow[rr, Leftrightarrow] \arrow[dr, Leftrightarrow] & & (Bj) \\
& (Bm) \arrow[ur, Leftrightarrow] &
\end{tikzcd}$$

Les espaces topologiques avec les applications continues forment une catégorie. Dans cette catégorie, les isomorphismes sont les applications continues qui ont un inverse continu, i.e. les homéomorphismes. On sait qu'une application continue peut avoir un inverse non continu. Une bijection n'est donc pas nécessairement un isomorphisme.

Dans toutes les catégories considérées jusqu'à maintenant les objets étaient des ensembles avec une structure donnée et les morphismes des applications qui conservaient cette structure.
D De telles catégories s'appellent <u>catégories concrètes</u>. Il y a des catégories où ce n'est pas le cas. Un ensemble ordonné P détermine, par exemple, une catégorie $\mathcal{P}$ de la façon suivante :

$Ob(\mathcal{P}) = P$

i.e. les objets x,y,..., de $\mathcal{P}$ sont les éléments x,y,..., de P. Les ensembles Mor(x,y) sont vides sauf si $x \leq y$. Dans ce cas, ils contiennent exactement un morphisme $f: x \longrightarrow y$. On vérifie que les trois axiomes sont satisfaits.

Dans ce cours, nous aurons affaire seulement à des catégories concrètes. Mentionnons-en quelques-unes.

Soit $\mathcal{C}$ une catégorie. Nous pouvons construire une nouvelle catégorie, $\mathcal{C}^2$, dont les objets sont les morphismes des $\mathcal{C}$. Si $f: A \longrightarrow B$ et $\overline{f}: \overline{A} \longrightarrow \overline{B}$ sont deux morphismes de $\mathcal{C}$ (et ainsi des objets de $\mathcal{C}^2$), nous définissons un morphisme $f \longrightarrow \overline{f}$ de $\mathcal{C}^2$ ainsi: c'est une paire de morphismes de $\mathcal{C}$: $\phi: A \longrightarrow \overline{A}$ et

ψ: $B \longrightarrow \bar{B}$ qui rend le diagramme

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[d, "\phi"'] & B \arrow[d, "\psi"] \\ \bar{A} \arrow[r, "\bar{f}"'] & \bar{B} \end{tikzcd}$$

commutatif.

Pour finir, une catégorie que nous rencontrerons souvent : la catégorie des suites exactes courtes de groupes dont les objets sont les suites exactes courtes de groupes (voir p.1/29):

E: $1 \longrightarrow A \longrightarrow B \longrightarrow G \longrightarrow 1$

et dont les morphismes Γ: $E \longrightarrow \bar{E}$ sont des triplets (λ,μ,ν) d'homomorphismes de groupes tels que les diagrammes

$$\begin{tikzcd} E: \arrow[d, "\Gamma"'] & 1 \arrow[r] & A \arrow[r] \arrow[d, "\lambda"'] & B \arrow[r] \arrow[d, "\mu"] & G \arrow[r] \arrow[d, "\nu"] & 1 \\ \bar{E}: & 1 \arrow[r] & \bar{A} \arrow[r] & \bar{B} \arrow[r] & \bar{G} \arrow[r] & 1 \end{tikzcd}$$

soient commutatifs.

<u>Proposition 1.8</u>. (i) Si gf est un monomorphisme, f est un monomorphisme. (ii) Si gf est un épimorphisme, g est un épimorphisme.

<u>Dém.</u>: (i) soit $fh = fh'$. Alors $gfh = gfh'$ et, par hypothèse $h = h'$. Donc f est un monomorphisme. (ii) soit $hg = h'g$. Alors $hgf = h'gf$ et, par hypothèse $h = h'$; donc g est un épimorphisme. //

1.4 Suites, diagrammes

Tout ce paragraphe sera formulé pour des groupes; les résultats restent cependant valables pour les R-modules.

D Une paire (κ,σ) d'homomorphismes (de groupes) avec $\mathrm{Cod}\ \kappa = \mathrm{Dom}\ \sigma = B$,

$$A \xrightarrow{\kappa} B \xrightarrow{\sigma} C \quad ,$$

D est appelé différentielle en B si

$$\sigma\kappa = o : A \to C$$

i.e. si

$$\mathrm{Im}\ \kappa \subset \mathrm{Ker}\ \sigma \quad .$$

D C'est une paire exacte (en B), si

$$\mathrm{Im}\ \kappa = \mathrm{Ker}\ \sigma \quad .$$

D Une suite $(\ldots,f_{n-1},f_n,f_{n+1},\ldots)$ d'homomorphismes,

$$\ldots \longrightarrow A^{n-1} \xrightarrow{f_{n-1}} A^n \xrightarrow{f_n} A^{n+1} \xrightarrow{f_{n+1}} \ldots \quad ,$$

est dite différentielle, si chaque paire d'homomorphismes consécutifs (f_{n-1},f_n) est différentielle en A^n; c'est une

D suite exacte si chaque paire (f_{n-1},f_n) est exacte (en A^n).

Proposition 1.9 . (i) La suite

$$1 \longrightarrow A \xrightarrow{\kappa} B$$

est exacte ssi κ est injectif.

(ii) La suite

$$A \xrightarrow{\sigma} B \longrightarrow 1$$

est exacte ssi σ est surjectif.

(iii) La suite

$$1 \longrightarrow A \xrightarrow{\phi} B \longrightarrow 1$$

est exacte ssi ϕ est bijectif.

<u>Remarque</u>: Dans ces diagrammes 1 désigne le groupe trivial contenant un seul élément, l'élément unité 1; nous écrivons donc 1 à la place de {1}, pour simplifier l'écriture.

<u>Dém.</u>: La démonstration résulte immédiatement des définitions.

<u>Notation</u>: Nous utiliserons souvent les signes suivants :

$\rightarrowtail$	pour un homomorphisme injectif
$\twoheadrightarrow$	pour un homomorphisme surjectif
$\rightarrowtail\!\!\!\!\twoheadrightarrow$	pour un homomorphisme bijectif
$=\!=$	pour l'homomorphisme identité.

Dans des formules, c'est le signe $\cong$ qui désigne un isomorphisme.

Une notion utile est celle de dualité. Etant donné une
D catégorie, deux <u>diagrammes</u> de morphismes dans cette catégorie sont <u>duaux</u> si l'un peut être obtenu à partir de l'autre par un renversement du sens de toutes les flèches. Ainsi le diagramme définissant un morphisme injectif et celui définissant un morphisme surjectif sont duaux, tandis que celui qui correspond à un morphisme bijectif est évidemment son propre dual.

<u>Proposition 1.10</u> . Soit un homomorphisme $\phi: A \to B$. Alors la suite

$$1 \longrightarrow \operatorname{Ker} \phi \longrightarrow A \longrightarrow A/\operatorname{Ker} \phi \longrightarrow 1$$

est exacte.

<u>Dém.</u>: Cela résulte de la définition du groupe quotient.

D Le groupe $A/\operatorname{Ker} \phi$ s'appelle <u>coimage</u> de ϕ :

$$\operatorname{Coim} \phi = \operatorname{Dom} \phi \,/\, \operatorname{Ker} \phi \quad .$$

Il est peut-être utile de rappeller la définition du groupe quotient. Etant donné un sous-groupe normal N d'un groupe G ($N \triangleleft G$),
D le <u>groupe quotient G modulo N</u> (G/N) est le groupe dont les éléments sont les classes latérales de N dans G que nous écrivons

gN - ou simplement [g] s'il est clair de quel sous-groupe normal il s'agit. La multiplication dans G/N est induite par celle dans G :

$$(gN)(hN) = (gh)N \quad \text{ou} \quad [g]\,[h] = [gh] \quad .$$

L'application σ qui associe à chaque $g \in G$ la classe latérale gN (ou [g]) à laquelle il appartient est un homomorphisme surjectif.

$$\sigma:\ G \twoheadrightarrow G/N$$

$$\sigma:\ g \longmapsto (gN) \quad \text{ou} \quad \sigma:\ g \longmapsto [g]$$

D Cet homomorphisme est appelé <u>surjection canonique</u>. Si deux éléments $g,h \in G$ appartiennent à la même classe latérale de N nous écrivons

$$g \equiv h \pmod N \quad .$$

<u>Proposition 1.11</u> . Soit

$$A \xrightarrow{\kappa} B \xrightarrow{\sigma} G$$

une suite exacte. Alors

$$\operatorname{Im} \sigma \cong B/\operatorname{Im} \kappa \qquad (\sigma B \cong B/\kappa A) \quad .$$

<u>Dém.</u>: Etant donné la suite ci-dessus, l'exactitude en B signifie $\operatorname{Ker} \sigma = \operatorname{Im} \kappa \lhd B$. Considérons alors le diagramme suivant (à lignes exactes) :

$$\begin{tikzcd} A \arrow[r, "\kappa"] \arrow[d, equal] & B \arrow[r, "\bar\sigma"] \arrow[d, equal] & B/\kappa A \arrow[r] & 1 \\ A \arrow[r, "\kappa"'] & B \arrow[r, "\sigma"'] & G \end{tikzcd}$$

avec $\bar\sigma$ la surjection canonique. Définissons une application

$$\gamma:\ B/\kappa A \longrightarrow G$$

$$\gamma:\ [b] \longmapsto \sigma b \quad .$$

Cette application est bien définie. En effet

$$[b] = [c] \in B/\kappa A$$

signifie $bc^{-1} \in \kappa A$ et donc

$$\sigma(bc^{-1}) = 1 \in G$$

ou

$$\sigma b = \sigma c \quad .$$

Mais cela veut dire précisément

$$\gamma[b] = \gamma[c] \quad .$$

L'application γ rend le diagramme commutatif et Im γ = Im σ .

En effet

$$[b] = \bar{\sigma}b$$

donc

$$\gamma[b] = \gamma\bar{\sigma}b = \sigma b \quad .$$

L'application γ est un homomorphisme.

$$\gamma(\bar{\sigma}b\cdot\bar{\sigma}c) = \gamma\bar{\sigma}(bc) = \sigma(bc) = \sigma b\cdot\sigma c \equiv \gamma\bar{\sigma}b\cdot\gamma\bar{\sigma}c \quad .$$

L'homomorphisme γ est injectif. En effet, soit

$$\gamma[b] = \sigma b = 1 \quad ;$$

alors

$$b \in \mathrm{Ker}\,\sigma = \mathrm{Im}\,\kappa$$

et

$$[b] = 1 \in B/\kappa A \quad .$$

Finalement on a le diagramme commutatif suivant (à lignes exactes) :

$$\begin{tikzcd}
A \arrow[r, "\kappa"] \arrow[d, equal] & B \arrow[r, "\bar{\sigma}"] \arrow[d, equal] & B/\kappa A \arrow[r] \arrow[d, "\gamma"] & 1 \\
A \arrow[r, "\kappa"'] & B \arrow[r, "\sigma"'] & G &
\end{tikzcd}$$ //

<u>Proposition 1.12</u> . L'homomorphisme γ, construit dans la démonstration de la proposition précédente, est unique.

<u>Dém.</u>: Cela résulte de la commutativité du diagramme et de la surjectivité de $\bar{\sigma}$. Soit en effet

$$\sigma = \gamma_1 \bar{\sigma} = \gamma_2 \bar{\sigma} \quad .$$

En vertu de la propriété (E) d'un homomorphisme surjectif

$$\gamma_1 = \gamma_2 \quad .$$

<u>Proposition 1.13</u> . Si dans le diagramme ci-dessus σ est surjectif, alors

$$G \simeq B/\kappa A \quad ,$$

si, en plus, κ est injectif, alors

$$G \simeq B/A \quad .$$

<u>Dém.</u>: C'est immédiat.

D Soit alors une <u>suite exacte courte</u>

$$1 \longrightarrow A \xrightarrow{\kappa} B \longrightarrow G \longrightarrow 1 \quad ,$$

i.e. une suite exacte de quatre homomorphismes, où les deux groupes aux extrêmes sont triviaux. Se donner cette suite équivaut à dire que $G \simeq B/\kappa A$. La proposition 1.12 peut donc être résumée par le diagramme commutatif, à lignes, colonnes et diagonales exactes :

$$\begin{tikzcd}
 & & & 1 \arrow[d] & 1 \\
 & & & \mathrm{Im}\,\sigma \arrow[ur] \arrow[d] & \\
 & A \arrow[r, "\kappa"] \arrow[d] & B \arrow[r, "\sigma"'] \arrow[ur, "\gamma\bar{\sigma}"] & G & \\
 & \mathrm{Im}\,\kappa \arrow[ur] \arrow[d] & & & \\
1 \arrow[ur] & 1 & & &
\end{tikzcd}$$

Une généralisation de la proposition 1.12 est facile à démontrer.

<u>Proposition 1.14</u> . Soit

$$\begin{tikzcd}
A \arrow[r, "\kappa"] \arrow[d, "\lambda"'] & B \arrow[r, "\sigma"] \arrow[d, "\mu"] & G \arrow[r] & 1 \\
\bar{A} \arrow[r, "\bar{\kappa}"'] & \bar{B} \arrow[r, "\bar{\sigma}"'] & \bar{G} &
\end{tikzcd}$$

un diagramme commutatif à lignes exactes. Alors il existe un unique homomorphisme

$$\gamma:\ G \longrightarrow \overline{G}$$

qui rend le diagramme commutatif.

Soient

$$1 \longrightarrow A \longrightarrow B \longrightarrow G \longrightarrow 1$$

et

$$1 \longrightarrow \overline{A} \longrightarrow \overline{B} \longrightarrow \overline{G} \longrightarrow 1$$

deux suites exactes courtes. Un triplet (α,β,γ) d'homomorphismes de groupes (ou de R-modules)

$$\alpha:\ A \longrightarrow \overline{A}, \quad \beta:\ B \longrightarrow \overline{B}, \quad \gamma:\ G \longrightarrow \overline{G}$$

qui rend le diagramme suivant :

$$\begin{tikzcd}
1 \arrow[r] & A \arrow[r] \arrow[d, "\alpha"'] & B \arrow[r] \arrow[d, "\beta"'] & G \arrow[r] \arrow[d, "\gamma"'] & 1 \\
1 \arrow[r] & \overline{A} \arrow[r] & \overline{B} \arrow[r] & \overline{G} \arrow[r] & 1
\end{tikzcd}$$

commutatif, est un morphisme dans la catégorie des suites exactes courtes de groupes (voir p.1/24).

<u>Proposition 1.15</u> . ("Short Five Lemma"). Etant donné un morphisme de suites exactes courtes de groupes

$$\begin{tikzcd}
1 \arrow[r] & A \arrow[r, "\kappa"] \arrow[d, "\lambda"'] & B \arrow[r, "\sigma"] \arrow[d, "\mu"] & G \arrow[r] \arrow[d, "\gamma"] & 1 \\
1 \arrow[r] & \overline{A} \arrow[r, "\overline{\kappa}"'] & \overline{B} \arrow[r, "\overline{\sigma}"'] & \overline{G} \arrow[r] & 1
\end{tikzcd}$$

on trouve les propriétés suivantes :

(i) si μ est surjectif, alors γ l'est aussi

(ii) si μ est injectif, alors λ l'est aussi

(iii) si μ est bijectif, alors λ est injectif et γ est surjectif.

(iv) si μ est bijectif et λ surjectif, alors γ est bijectif

(v) si μ est bijectif et γ injectif, alors λ est bijectif

(vi) si λ et γ sont surjectifs, alors μ l'est aussi

(vii) si λ et γ sont injectifs, alors μ l'est aussi

(viii) si λ et γ sont bijectifs, alors μ l'est aussi.

<u>Remarques</u>. Le plus souvent seulement les propriétés (vi), (vii) et (viii) sont connues sous le nom de "Short Five Lemma". La technique de démonstration que l'on va utiliser s'appelle "chasse dans le diagramme" (diagram chasing). Nous avons noté en détail le parcours de cette chasse. En pratique on le fait souvent seulement mentalement. Pour la démonstration de l'ensemble des huit propriétés on a besoin du diagramme entier, mais pour une seule des propriétés on n'utilise qu'une partie du diagramme. Il est utile de présenter pour chaque propriété ce "diagramme minimal".

<u>Dém.</u>: Les propriétés (i), (ii) et (iii) sont une conséquence de la proposition 1.6 et de la commutativité. Les diagrammes partielles sont

$$\begin{tikzcd} B \arrow[r, "\sigma"] \arrow[d, two heads, "\mu"'] & G \arrow[d, "\gamma"] & \\ \bar{B} \arrow[r, "\bar{\sigma}"'] & \bar{G} \arrow[r] & 1 \end{tikzcd} \qquad \text{(i)}$$

$$\begin{tikzcd} 1 \arrow[r] & A \arrow[r, "\kappa"] \arrow[d, "\lambda"'] & B \arrow[d, tail, "\mu"] \\ & \bar{A} \arrow[r, "\bar{\kappa}"'] & \bar{B} \end{tikzcd} \qquad \text{(ii)}$$

Remarquez que le diagramme (ii) est le dual du diagramme (i)

- évidemment aux lettres près que l'on utilise pour désigner les groupes et leurs homomorphismes.

$$\begin{tikzcd}
1 \arrow[r] & \overset{\bullet}{A} \arrow[r, "\kappa"] \arrow[d, "\lambda"'] & B \arrow[r, "\sigma"] \arrow[d, "\mu"] & G \arrow[d, "\gamma"] & \\
& \bar{A} \arrow[r, "\bar{\kappa}"'] & \bar{B} \arrow[r, "\bar{\sigma}"'] & \underset{\bullet}{\bar{G}} \arrow[r] & 1
\end{tikzcd} \qquad \text{(iii)}$$

Le point $\bullet$ dans ces diagrammes et dans ceux qui vont suivre désigne les endroits où les lignes horizontales sont supposées exactes.

(iv) Les conditions de (iii) sont remplies; nous supposons en plus que λ est surjectif (il est alors bijectif) et nous démontrerons que γ est injectif (il est alors aussi bijectif).

Le diagramme partiel est

$$\begin{tikzcd}
1 \arrow[r] & \overset{\bullet}{A} \arrow[r, "\kappa"] \arrow[d, "\lambda"'] & \overset{\circ}{B} \arrow[r, "\sigma"] \arrow[d, "\mu"] & \overset{\bullet}{G} \arrow[r] \arrow[d, "\gamma"] & 1 \\
& \bar{A} \arrow[r, "\bar{\kappa}"'] & \underset{\bullet}{\bar{B}} \arrow[r, "\bar{\sigma}"'] & \underset{\bullet}{\bar{G}} \arrow[r] & 1
\end{tikzcd} \qquad \text{(iv)}$$

Le signe o signifie que la ligne est différentielle à cet endroit (fait utilisé dans les dernières lignes de la démonstration).

Soit $\alpha \in G$ et

$$\gamma\alpha = 1 \in \bar{G} \quad .$$

Par hypothèse

$$\exists b \in B, \quad \sigma b = \alpha$$

et

$$\gamma\sigma b = \gamma\alpha = 1 = \bar{\sigma}\mu b \quad .$$

Donc

$$\exists \bar{a} \in \bar{A}, \quad \mu b = \bar{\kappa}\bar{a} \quad .$$

De plus

$$\exists a \in A, \quad \lambda a = \bar{a} \quad .$$

Ainsi

$$\mu b = \bar{\kappa}\lambda a = \mu\kappa a$$

et

$$b = \kappa a \quad .$$

Il s'ensuit que

$$\alpha = \sigma b = \sigma\kappa a = 1 \in G \quad . \quad //$$

(v) Les conditions de (iii) sont remplies; nous supposons en plus que γ est injectif (il est alors bijectif) et nous démontrerons que λ est surjectif (il est alors aussi bijectif). Le diagramme partiel est

$$\begin{tikzcd}
1 \arrow[r] & A \arrow[r, "\kappa"] \arrow[d, "\lambda"'] & B \arrow[r, "\sigma"] \arrow[d, "\mu"] & G \arrow[d, "\gamma"] & \\
1 \arrow[r] & \bar{A} \arrow[r, "\bar{\kappa}"'] & \bar{B} \arrow[r, "\bar{\sigma}"'] & \bar{G} \arrow[r] & 1
\end{tikzcd} \qquad \text{(v)}$$

Remarquez que le diagramme (v) est le dual du diagramme (iv).

Soit $\bar{a} \in \bar{A}$.

Alors

$$\exists b \in B, \quad \mu b = \bar{\kappa}\bar{a}$$

ainsi

$$\gamma\sigma b = \bar{\sigma}\mu b = \bar{\sigma}\bar{\kappa}\bar{a} = 1 \in \bar{G} \quad .$$

Alors, par hypothèse,

$$\sigma b = 1 \in G$$

et

$$\exists a \in A \quad b = \kappa a \quad ,$$

donc

$$\mu b = \mu\kappa a = \bar{\kappa}\lambda a = \bar{\kappa}\bar{a}$$

et

$$\lambda a = \bar{a} \qquad . \quad //$$

(vi) Le diagramme partiel est

$$\begin{tikzcd} A \arrow[r, "\kappa"] \arrow[d, two heads, "\lambda"'] & B \arrow[r, "\sigma"] \arrow[d, "\mu"] & G \arrow[r] \arrow[d, two heads, "\gamma"] & 1 \\ \bar{A} \arrow[r, "\bar{\kappa}"'] & \bar{B} \arrow[r, "\bar{\sigma}"'] & \bar{G} & \end{tikzcd} \qquad \text{(vi)}$$

Soit $\bar{b} \in \bar{B}$. Alors $\bar{\sigma}\bar{b} \in \bar{G}$ et, par hypothèse,

$$\exists \alpha \in G \qquad \gamma\alpha = \bar{\sigma}\bar{b} \qquad .$$

Aussi

$$\exists b \in B \qquad \alpha = \sigma b \qquad ;$$

ainsi

$$\gamma\alpha = \gamma\sigma b = \bar{\sigma}\mu b = \bar{\sigma}\bar{b}$$

et

$$\bar{b} \cdot \mu b^{-1} \in \operatorname{Ker} \bar{\sigma} = \operatorname{Im} \bar{\kappa} \qquad .$$

Donc

$$\exists \bar{a} \in \bar{A} \qquad \bar{b} \cdot \mu b^{-1} = \bar{\kappa}\bar{a} \qquad .$$

Mais, par hypothèse,

$$\exists a \in A \qquad \lambda a = \bar{a} \qquad ;$$

alors

$$\bar{b} \cdot \mu b^{-1} = \bar{\kappa}\lambda a = \mu\kappa a$$

$$\bar{b} = \mu\,(\kappa a \cdot b) \qquad . \quad //$$

(vii) Le diagramme partiel est dual au diagramme (vi)

$$\begin{tikzcd} & A \arrow[r, "\kappa"] \arrow[d, tail, "\lambda"'] & B \arrow[r, "\sigma"] \arrow[d, "\mu"] & G \arrow[d, tail, "\gamma"] \\ 1 \arrow[r] & \bar{A} \arrow[r, "\bar{\kappa}"'] & \bar{B} \arrow[r, "\bar{\sigma}"'] & \bar{G} \end{tikzcd} \qquad \text{(vii)}$$

Soit

$$\mu b = 1 \in \overline{B}$$

alors

$$\gamma\sigma b = \overline{\sigma}\mu b = \overline{\sigma}1 = 1 \in \overline{G}$$

et, par hypothèse,

$$\sigma b = 1 \in G \quad .$$

Ainsi

$$\exists a \in A, \quad b = \kappa a \quad .$$

De plus

$$\overline{\kappa}\lambda a = \mu\kappa a = \mu b = 1 \in \overline{B}$$

et

$$\lambda a = 1 \in \overline{A} \quad .$$

Alors, par hypothèse

$$a = 1$$

et

$$b = \kappa a = 1 \in B \quad . \quad //$$

(viii) Le diagramme partiel est

$$\begin{tikzcd} & A \arrow[r, "\kappa"] \arrow[d, two heads, "\lambda"'] & B \arrow[r, "\sigma"] \arrow[d, "\mu"] & G \arrow[r] \arrow[d, two heads, "\gamma"] & 1 \\ 1 \arrow[r] & \overline{A} \arrow[r, "\overline{\kappa}"'] & \overline{B} \arrow[r, "\overline{\sigma}"'] & \overline{G} & \end{tikzcd} \qquad \text{(viii)}$$

.

1.5 Automorphismes et endomorphismes

Soit ϕ un homomorphisme de groupe.

D Si Dom ϕ = Cod ϕ, ϕ est appelé endomorphisme. Les endomorphismes d'un groupe G forment un monoïde End(G). Un endo-

D morphisme qui est un isomorphisme s'appelle automorphisme. Les automorphismes d'un groupe G forment un groupe A(G).

Proposition 1.16 . A chaque $x \in G$ faisons correspondre une application, θx, de G dans G définie par

$$\forall g \in G \qquad (\theta x)g = xgx^{-1} \quad .$$

Alors θx est un automorphisme et l'application

$$\theta: \ G \longrightarrow A(G)$$

est un homomorphisme dont le noyau est le centre, C(G), de G.

D L'image de θ, appelé groupe des automorphismes intérieurs de G et noté I(G), est un sous-groupe normal de A(G):

$$I(G) = \mathrm{Im}\ \theta \triangleleft A(G) \quad .$$

Dém.: θx est un endomorphisme :

$$(\theta x)(gh) = xghx^{-1} = xgx^{-1}xhx^{-1} = [(\theta x)g][(\theta x)h] \quad .$$

θx est un automorphisme. En effet, θx a un inverse $(\theta x)^{-1}$ défini par

$$(\theta x)^{-1}: \ g \longmapsto x^{-1}gx \quad .$$

L'application θ: $G \longrightarrow A(G)$ est un homomorphisme :

$$[(\theta x)(\theta y)^{-1}]g = (\theta x)(y^{-1}gy) = xy^{-1}g(xy^{-1})^{-1} = [\theta(xy^{-1})]g$$

Im θ = I(G) est donc un sous-groupe de A(G). C'est même un sous-groupe normal :

$$\forall \alpha \in A(G), \ \ \forall(\theta x) \in I(G), \ \ \forall g \in G :$$

$$[\alpha(\theta x)\alpha^{-1}]g = \alpha[\theta x(\alpha^{-1}g)] = \alpha[x(\alpha^{-1}g)x^{-1}] =$$

$$= (\alpha x)g(\alpha x)^{-1} = [\theta(\alpha x)]g$$

i.e.

$$\alpha(\theta x)\alpha^{-1} = \theta(\alpha x) \quad .$$

Le noyau de θ est le centre de G :

$$\theta x = 1 \in A(G)$$

signifie en effet

$$\forall g \in G \quad xgx^{-1} = g$$

i.e. x commute avec n'importe quel élément de G. //

Je rappelle que l'ensemble C(G) des éléments d'un groupe G qui commutent avec chaque élément du groupe est

D appelé le centre du groupe

$$C(G) = \{x \in G \mid \forall g \in G \quad xg = gx\} \quad .$$

Nous venons de voir que C(G) est un sous-groupe normal (et abélien par sa définition) de G et qu'on a la suite exacte courte suivante :

$$1 \longrightarrow C(G) \longrightarrow G \xrightarrow{\Omega} I(G) \longrightarrow 1 \quad .$$

De plus, puisque $I(G) \triangleleft A(G)$, nous pouvons définir un groupe

D E(G) des automorphismes extérieurs de A par

$$E(G) = A(G)/I(G) \quad .$$

On a donc une deuxième suite exacte courte

$$1 \longrightarrow I(G) \longrightarrow A(G) \xrightarrow{\sigma} E(G) \longrightarrow 1 \quad .$$

On voit que la suite suivante

$$\begin{tikzcd} 1 \arrow[r] & C(G) \arrow[r] & G \arrow[r, "\theta"] \arrow[dr, "\Omega"'] & A(G) \arrow[r, "\sigma"] & E(G) \arrow[r] & 1 \\ & & & I(G) \arrow[u, "(\iota)"'] & & \end{tikzcd}$$

est aussi exacte.

D Soit G un groupe à opérateurs Ψ. Un sous-groupe H stable par rapport à Ψ (un sous-groupe Ψ-stable, un Ψ-sous-groupe) est un sous-groupe $H \subset G$ tel que

$\forall \alpha \in \Psi, \quad \forall h \in H \quad \alpha h \in H \quad .$

Un sous-module d'un R-module M est un R-sous-groupe d'un groupe abélien M. Un sous-groupe normal $N \lhd G$ est un I(G)-sous-groupe de G.

D Les A(G)-sous-groupes de G s'appellent <u>sous-groupes caractéristiques</u>, les End(G)-sous-groupes de G s'appellent

D <u>sous-groupes totalement invariants</u> ("fully invariant") ou

D <u>endostables</u>. Nous écrirons

$$H \lhd\!\mid G$$

pour dire que H est un sous-groupe caractéristique de G et

$$H \lhd\!\mid\mid G$$

pour dire que H est un sous-groupe endostable de G. Un sous-groupe endostable est évidemment caractéristique; un sous-groupe caractéristique est évidemment normal. Symboliquement

$$\lhd\!\mid\mid \Longrightarrow \lhd\!\mid \Longrightarrow \lhd \quad .$$

Si $H \lhd G$, les automorphismes intérieurs de G sont des automorphismes de H. Si $H \lhd\!\mid G$, les automorphismes de G sont des automorphismes de H. Si $H \lhd\!\mid\mid G$, les endomorphismes de G sont des endomorphismes de H.

Le centre d'un groupe est précisément l'exemple d'un sous-groupe caractéristique.

<u>Proposition 1.16</u> .

$$C(G) \lhd\!\mid G \quad .$$

<u>Dém.</u>:

$\forall \alpha \in A(G), \quad \forall c \in C(G), \quad \forall g \in G$

$\alpha c \cdot \alpha g = \alpha(cg) = \alpha(gc) = \alpha g \cdot \alpha c \quad .$

Puisque α est un automorphisme, chaque $g' \in G$ peut être écrit comme $g' = \alpha g$. //

Nous allons maintenant donner l'exemple d'un sous-groupe important qui est endostable. Soient x et y, deux éléments d'un groupe G. On appelle <u>commutateur de x et y</u> l'élément $[x,y] = xyx^{-1}y^{-1}$ de G. Le produit de deux commutateurs n'est pas nécessairement un commutateur, l'ensemble des commutateurs d'un groupe ne forment donc pas nécessairement un groupe. On appelle <u>groupe dérivé</u> de G (ou <u>groupe commutateur</u> de G) le groupe engendré par les commutateurs de G. On le note G' ou $[G,G]$.

<u>Proposition 1.17</u> .

$$[G,G] \lhd\!\!\mid\!\mid G \quad .$$

<u>Dém.</u>: En effet, un endomorphisme $\chi \in \mathrm{End}(G)$ envoie un commutateur donné dans un autre commutateur :

$$\chi[x,y] = \chi(xyx^{-1}y^{-1}) = \chi x \cdot \chi y \cdot \chi x^{-1} \cdot \chi x^{-1} = [\chi x, \chi y] \qquad //$$

Si G est abélien

$$C(G) = G, \quad [G,G] = 1 \quad .$$

Tandis que la propriété d'être normal n'est pas transitive, i.e.

$$F \lhd G, \quad G \lhd H \quad \not\Longrightarrow \quad F \lhd H \quad ,$$

la propriété d'être caractéristique ou endostable est transitive.

<u>Proposition 1.18</u> .

(i) $F \lhd\!\!\mid G, \quad G \lhd\!\!\mid H \Longrightarrow F \lhd\!\!\mid H$

(ii) $F \lhd\!\!\mid\!\mid G, \quad G \lhd\!\!\mid\!\mid H \Longrightarrow F \lhd\!\!\mid\!\mid H$.

<u>Dém.</u>: Chaque automorphisme (respectivement endomorphisme) de H est un automorphisme (respectivement endomorphisme) de G; il est donc aussi un automorphisme (respectivement endomorphisme) de F. //

<u>Proposition 1.19</u> .

$$F \lhd\!| \; G, \quad G \lhd H \Longrightarrow F \lhd H \quad .$$

<u>Dém.</u>: Chaque automorphisme intérieur de H est un automorphisme de G; il est donc un automorphisme de F. //

En revanche, on n'a pas de propriété analogue à la suivante :

$$\left.\begin{array}{l} F \subset G \subset H \\ F \lhd H \end{array}\right\} \Longrightarrow F \lhd G$$

qui soit valable pour les sous-groupes caractéristiques ou endostables.

Extensions de groupes

Donnons-nous une suite exacte courte de groupes

$$1 \longrightarrow A \xrightarrow{\kappa} X \xrightarrow{\sigma} G \longrightarrow 1 \quad ,$$

i.e. un groupe X avec les propriétés suivantes

$$A \simeq \kappa A \triangleleft X \qquad G \simeq X/A \quad .$$

D Un tel groupe X est appelé <u>extension de A par G</u>. (Attention, Bourbaki appelle cela une extension de G par A. Nous suivrons ici l'usage majoritaire établi par le fondateur de la théorie, Schreier). Nous avons alors le diagramme suivant:

$$\begin{tikzcd}
 & 1 \arrow[d] & & & \\
 & C(A) \arrow[d] & & & \\
1 \arrow[r] & A \arrow[r, "\kappa"] \arrow[d, "\Omega"'] & X \arrow[r, "\sigma"] & G \arrow[r] & 1 \\
1 \arrow[r] & I(A) \arrow[r, "\bar{\kappa}"'] \arrow[d] & A(A) \arrow[r, "\bar{\sigma}"'] & E(A) \arrow[r] & 1 \\
 & 1 & & &
\end{tikzcd}$$

Puisque A est normal dans X, la conjugaison par un élément de X est un automorphisme de A. Chaque élément x de X détermine ainsi un automorphisme de A.

(1) $$x + a - x =: (\phi x)a$$

où ϕ est une application de X dans le groupe A(A) des automorphismes de A. Il est facile de voir que ϕ est un homomorphisme

(2) $$\phi : X \longrightarrow A(A) \quad .$$

Le noyau de ϕ est le centralisateur $C_X(A)$ de A dans X.

D Rappellons que le centralisateur de A dans X est l'ensemble des éléments de X qui commutent avec A :

$$C_X(A) = \{x \in X \mid \forall a \in A,\ x + a = a + x\} \quad .$$

Le centre de A est certainement contenu dans $C_X(A)$.

$$C(A) \subset C_X(A) \quad .$$

Exercice 2.a. Soit $A \triangleleft X$ et $\phi : X \longrightarrow A(A)$. Montrer que

$$\operatorname{Ker} \phi = C_X(A)$$

et

$$C(A) \triangleleft C_X(A) \quad .$$

Dans ces conditions (voir Proposition 1.14), il existe un unique homomorphisme

(3) $$\psi : G \longrightarrow E(A)$$

tel que

(4) $$\bar{\sigma}\phi = \psi\sigma \quad .$$

L'extension X de A par G détermine donc d'une façon unique un groupe $\operatorname{Im} \psi \subset E(A)$ d'automorphismes extérieurs de A.

(5)
$$\begin{tikzcd}
 & 1 \arrow[d] & 1 \arrow[d] & & \\
1 \arrow[r] & C(A) \arrow[r] \arrow[d] & C_X(A) \arrow[d] & & \\
1 \arrow[r] & A \arrow[r, "\kappa"] \arrow[d, "\Omega"'] & X \arrow[r, "\sigma"] \arrow[d, "\phi"'] & G \arrow[r] \arrow[d, "\psi"] & 1 \\
1 \arrow[r] & I(A) \arrow[r, "\bar{\kappa}"'] \arrow[d] & A(A) \arrow[r, "\bar{\sigma}"'] & E(A) \arrow[r] & 1 \\
 & 1 & & &
\end{tikzcd}$$

2.1 Théorie de Schreier

L'idée qui a ouvert à Schreier la voie à l'étude de la structure des extensions était celle de l'utilisation d'abord de représentants des classes latérales de A dans X et de la formulation, ensuite, des propriétés indépendantes du choix particulier de ces représentants.

Pour simplifier l'écriture, nous identifierons le sous-groupe κA de X au groupe A. Ceci nous oblige d'utiliser la même notation pour la loi interne dans A et pour la loi interne dans X; ce sera la notation additive, de nouveau pour simplifier l'écriture. L'emploi de la notation additive ne signifie pas pour autant que les groupes A et X soient abéliens ! Nous dirons explicitement quand l'un de ces groupes est abélien. Dans la plus grande partie de ce cours, A sera abélien, mais X ne le sera pas nécessairement. Aussi faudra-t-il faire attention au fait que

$$-(x+y) = -y-x \quad .$$

Nous utiliserons le plus souvent les lettres suivantes pour désigner les éléments des groupes en question :

$$o,a,b,c,\ \ldots \in A$$

$$o,x,y,z,\ \ldots \in X$$

$$1,\alpha,\beta,\gamma,\ \ldots \in G \quad .$$

Le groupe X peut être partitionné en classes latérales suivant A (ou modulo A). Le groupe X est la réunion disjointe de ces classes. Comme G est isomorphe au groupe X/A dont les éléments sont les classes latérales, nous pouvons choisir dans chaque classe un représentant $r\alpha$, avec $\alpha \in G$.

Si nous choisissons des classes à gauche (attention, la gauche de l'un est la droite de l'autre), chaque élément $x \in X$ peut s'écrire alors

(6) $$x = a + r\alpha \qquad a \in A,\ \alpha \in G \quad .$$

Nous avons ainsi une application

(7) $$r : G \longrightarrow X \quad .$$

Composée avec la surjection $\sigma : X \longrightarrow G$, elle donne l'application identité de G :

(8) $$\sigma r = 1_G \quad .$$

D Nous appellerons r un <u>relèvement</u> et Im r un <u>choix de représentants</u>.

Remarquons que $r\sigma$ est une application de X dans X qui envoie chaque élément sur le représentant de la classe à gauche à laquelle il appartient.

En général, l'application r n'est pas un homomorphisme. A l'élément unité $1 \in G$ correspond un élément de A qui n'est pas nécessairement l'unité de A :

(9) $$r1 = a_o \in A \quad .$$

De plus,

(10) $$\sigma[r\alpha+r\beta-r(\alpha\beta)] = \sigma r\alpha\cdot\sigma r\beta\cdot\sigma r(\alpha\beta)^{-1} = \alpha\beta(\alpha\beta)^{-1} = 1 \quad ,$$

de sorte que

(11) $$\hat{\exists} m(\alpha,\beta) \in A \qquad r\alpha+r\beta-r(\alpha\beta) = m(\alpha,\beta) \quad .$$

Si dans (1) nous posons $x = r\alpha$, nous pouvons associer à chaque $\alpha \in G$ un automorphisme $\varphi\alpha$ de A :

(12) $$r\alpha + a - r\alpha = (\phi r\alpha)a =: (\varphi\alpha)a$$

où nous avons posé

(13) $$\phi r = \varphi \, .$$

Il s'ensuit que

(14) $$\bar{\sigma}\varphi = \bar{\sigma}\phi r = \psi\sigma r = \psi \quad ,$$

c'est pourquoi nous écrirons parfois

$$\forall\alpha \in G \qquad \varphi\alpha \in \psi\alpha \quad ,$$

pour dire que $\varphi\alpha$ appartient à la classe latérale $\psi\alpha$ -- de $I(A)$ dans $A(A)$.

Mais en général l'application

$$\varphi : G \longrightarrow A(A)$$

n'est pas un homomorphisme. On peut le voir en calculant $(\varphi\alpha)(\varphi\beta)a$ à l'aide de (11) et de (12) :

(15) $$(\varphi\alpha)(\varphi\beta)a = m(\alpha,\beta) + \varphi(\alpha\beta)a - m(\alpha,\beta) = \Omega m(\alpha,\beta)\varphi(\alpha\beta)a \quad .$$

De l'associativité (de la loi interne dans X) découle une propriété importante de l'application m. Nous avons d'une part

$$\begin{aligned} r\alpha + (r\beta+r\gamma) &= r\alpha + m(\beta,\gamma) + (-r\alpha+r\alpha) + r(\beta\gamma) \\ &= (\varphi\alpha)m(\beta,\gamma) + m(\alpha,\beta\gamma) + r(\alpha\beta\gamma) \end{aligned}$$

et d'autre part

$$(r\alpha+r\beta) + r\gamma = m(\alpha,\beta) + m(\alpha\beta,\gamma) + r(\alpha\beta\gamma) \quad .$$

Il en résulte

(16) $$(\varphi\alpha)m(\beta,\gamma) = m(\alpha,\beta) + m(\alpha\beta,\gamma) - m(\alpha,\beta\gamma) \quad .$$

D Nous appellerons <u>facteur</u> ("factor set" en anglais) une application

$$m : G\text{x}G \longrightarrow A$$

satisfaisant à la relation (16).

Nous pouvons maintenant expliciter la loi interne de X :

(17) $$(a+r\alpha) + (b+r\beta) = a + (\varphi\alpha)b + m(\alpha,\beta) + r(\alpha\beta) \quad .$$

Toutes ces constructions dépendent encore du relèvement r choisi. Il nous faut donc examiner ce qui se passe si nous chosissons un autre relèvement $\bar{r}$ pour la même extension X. Nécessairement

(18) $$\bar{r}\alpha = c\alpha + r\alpha$$

avec

(19) $c : G \longrightarrow A$.

Il vient alors

$$(\bar{\varphi}\alpha)a = \bar{r}\alpha + a - \bar{r}\alpha = c\alpha + r\alpha + a - r\alpha - c\alpha = c\alpha + (\varphi\alpha)a - c\alpha$$

ou

(20) $(\bar{\varphi}\alpha) = (\Omega c\alpha)(\varphi\alpha)$

et l'on vérifie qu'en effet

(21) $\bar{\sigma}\bar{\varphi} = \bar{\sigma}\varphi = \psi$.

Regardons ce qui advient aux facteurs. En partant de (11) et en utilisant (18) et (12) on trouve

$$\bar{m}(\alpha,\beta) =: \bar{r}\alpha + \bar{r}\beta - \bar{r}(\alpha\beta)$$

$$= c\alpha + r\alpha + c\beta + (-r\alpha + r\alpha) + r\beta - r(\alpha\beta) - c(\alpha\beta)$$

(22) $\bar{m}(\alpha,\beta) = c\alpha + (\varphi\alpha)(c\beta) + m(\alpha,\beta) - c(\alpha\beta)$.

D Des facteurs $\bar{m}$ et m reliés par (22) seront appelés <u>facteurs équivalents</u> et nous écrivons

$$\bar{m} \sim m \quad (c) \quad .$$

En effet, (22) est une relation d'équivalence : on vérifie que

$$m \sim m \quad (o) \quad ,$$

et, en tenant compte de (20) que

$$\bar{m} \sim m \quad (c) \quad \Longrightarrow \quad m \sim \bar{m} \quad (-c) \quad .$$

Enfin

$$m_2 \sim m_1 \quad (c_1) \quad \text{et} \quad m_3 \sim m_2 \quad (c_2)$$

impliquent

$$m_3 \sim m_1 \quad (c_2 + c_1) \quad .$$

Nous noterons par $[m]$ la classe d'équivalence d'un facteur m. Ainsi les formules qui précèdent disent que $m_2 \in [m_1]$ plus $m_3 \in [m_2]$ entraînent $m_3 \in [m_1]$.

Résumons maintenant les résultats acquis.

Proposition 2.1 . Une extension donnée X de A par G détermine

(i) un homomorphisme $\psi : G \longrightarrow E(A)$

(ii) une classe d'équivalence $[m]$ de facteurs,

et il existe un facteur $m \in [m]$ et un φ satisfaisant à $\bar{\sigma}\varphi = \psi$ reliés par les relations (15) et (16) :

$$(\varphi\alpha)(\varphi\beta) = \Omega m(\alpha,\beta)\varphi(\alpha\beta)$$

$$(\varphi\alpha)m(\beta,\gamma) = m(\alpha,\beta) + m(\alpha\beta,\gamma) - m(\alpha,\beta\gamma) \quad .$$

Exercice 2.b : Démontrer que φ détermine r seulement modulo C(A) et que m détermine r seulement modulo une application $c : G \longrightarrow A$ qui satisfait à

$$\Omega m(\alpha,\beta)^{-1} c(\alpha\beta) = c\alpha + (\varphi\alpha)(c\beta) \quad .$$

La réciproque de la Proposition 2.1 est aussi vraie :

Proposition 2.2 . Soient donnés

(i) une application $\varphi : G \longrightarrow A(A)$

(ii) une application $m : G\mathrm{x}G \longrightarrow A$

satisfaisant à (15) et (16). Il existe alors une extension X de A par G qui détermine un groupe d'automorphismes extérieurs $\psi G \subset E(A)$ et une classe d'équivalence de facteurs $[m]$ tels que $\bar{\sigma}\varphi = \psi$ et $m \in [m]$.

Dém.: Soit X l'ensemble A x G. Définissons dans X une loi interne + (pas nécessairement abélienne) :

(23) $$(a,\alpha) + (b,\beta) = (a+(\varphi\alpha)b + m(\alpha,\beta), \alpha\beta) \quad .$$

Il faut d'abord vérifier que (X,+) est un groupe. On voit en effet que la loi associative est vérifiée, qu'il y a un élément unité

(24) $$(-m(1,1),1) = 1 \in X$$

et que chaque élément (a,α) a un inverse

(25) $$(-m(1,1) - m(\alpha^{-1},\alpha) - (\varphi\alpha^{-1})a,\alpha^{-1}) = -(a,\alpha) \quad .$$

L'ensemble X avec la loi de multiplication (23) sera noté $X[A,G,\varphi,m]$. C'est donc un groupe.

Le reste de la démonstration est laissé comme exercice (2.c).

Une propriété importante des morphismes de suites exactes courtes est donnée par la

<u>Proposition 2.3</u> . Soit X une extension de A par G déterminant une application φ et un facteur m, soit Y une extension de B par H déterminant une application $\overline{\varphi}$ et un facteur $\overline{m}$, soient enfin $\lambda : A \longrightarrow B$ et $\nu : G \longrightarrow H$ deux homomorphismes. Alors un homomorphisme $\mu : X \longrightarrow Y$ qui rend le diagramme ci-dessous commutatif

(26) $$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \xrightarrow{(\kappa)} & X & \xrightarrow{\sigma} & G & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle\lambda} & & \downarrow{\scriptstyle\mu} & & \downarrow{\scriptstyle\nu} & & \\ 0 & \longrightarrow & B & \xrightarrow[(\overline{\kappa})]{} & Y & \xrightarrow[\overline{\sigma}]{} & H & \longrightarrow & 1 \end{array}$$

existe ssi on peut trouver une application

(27) $$u : G \longrightarrow B$$

(soumise à une condition de normalisation à spécifier) telle que pour tout $\alpha,\ \beta \in G$

(28) $$\lambda[(\varphi\alpha)a] = (\Omega u\alpha)(\overline{\varphi}\nu\alpha)(\lambda a)$$

(29) $$\lambda m(\alpha,\beta) = u\alpha + (\overline{\varphi}\nu\alpha)(u\beta) + \overline{m}(\nu\alpha,\nu\beta) - u(\alpha\beta) \quad .$$

<u>Dém.</u>: Supposons d'abord l'existence de l'homomorphisme μ. Soient alors $r : G \longrightarrow X$ et $\overline{r} : H \longrightarrow Y$ deux relèvements. Alors la commutativité nous donne

$$\overline{\sigma}\overline{r}\nu = \overline{\sigma}\overline{r}(\nu\sigma)r = (\overline{\sigma}\mu)r$$

de sorte que

(30) $\exists u\alpha \in B \quad \mu r\alpha = \bar{\kappa} u\alpha + \bar{r}\nu\alpha$,

et en particulier

(31) $\mu r1 = \bar{\kappa} u1 + \bar{r}1$.

L'utilisation de la définition (12) de $\varphi\alpha$ et de $\bar{\varphi}\alpha$, ainsi que de (30) permet d'établir (28) :

$$\bar{\kappa}\lambda[(\varphi\alpha)a] = \mu[r\alpha+\kappa a-r\alpha] = \mu r\alpha + \mu\kappa a - \mu r\alpha$$
$$= \bar{\kappa}u\alpha + \bar{r}\nu\alpha + \bar{\kappa}\lambda a - \bar{r}\nu\alpha - \bar{\kappa}u\alpha$$
$$= \bar{\kappa}[(\Omega u a)(\bar{\varphi}\nu\alpha)(\lambda a)] \quad .$$

De façon semblable, on calcule à partir de (11)

$$\bar{\kappa}\lambda m(\alpha,\beta) = \mu\kappa m(\alpha,\beta)$$
$$= \bar{\kappa}u\alpha + \bar{r}\nu\alpha + \bar{\kappa}u\beta + (-\bar{r}\nu\alpha+\bar{r}\nu\alpha) + \bar{r}\nu\beta - \bar{r}\nu(\alpha\beta) - \bar{\kappa}u(\alpha\beta)$$
$$= \bar{\kappa}[u\alpha + (\bar{\varphi}\nu\alpha)(u\beta) + \bar{m}(\nu\alpha,\nu\beta) - u(\alpha\beta)] \quad .$$

(Dans ces calculs nous avons utilisé les insertions (κ) et ($\bar{\kappa}$) que d'habitude nous omettons.) L'homomorphisme μ peut être explicité :

(32) $\mu(a+r\alpha) = (\lambda a+u\alpha) + \bar{r}\nu\alpha$.

Réciproquement, si l'on définit une application $\mu: X \longrightarrow Y$ par (32), on montre qu'elle rend le diagramme commutatif, si la condition de normalisation (31) est remplie. Alors les relations (28) et (29) permettent de montrer que μ est en fait un homomorphisme. Notons qu'à chaque choix de $u: G \longrightarrow B$ correspond un homomorphisme $\mu: X \longrightarrow Y$. //

Les relations (20) et (22) sont un cas spécial de (28) et (29) que l'on obtient en posant $B = A$, $\lambda = 1_A$, $H = G$, $\nu = 1_G$:

(33)
$$\begin{tikzcd}
0 \arrow[r] & A \arrow[r] \arrow[d, equal, "1_A"'] & X \arrow[r] \arrow[d, "\mu"] & G \arrow[r] \arrow[l, bend right, "r"'] \arrow[d, equal, "1_G"] & 1 \\
0 \arrow[r] & A \arrow[r] & Y \arrow[r] & G \arrow[r] \arrow[l, bend left, "r"] & 1
\end{tikzcd}$$

D L'homomorphisme μ est alors bijectif. Des extensions X et Y satisfaisant à un tel diagramme sont appelées isomorphes. Le choix de relèvements différents (r et $\bar{r}$) pour un groupe abstrait donné donne lieu à des extensions isomorphes. Des extensions isomorphes correspondent à un seul groupe abstrait. Mais, attention, étant donné deux extensions, X et Y, de A par G, les deux groupes abstraits peuvent être isomorphes sans que les deux extensions X et Y le soient. L'isomorphisme d'extensions est une relation d'équivalence entre les extensions d'un groupe donné, A, par un autre groupe donné, G. C'est pourquoi des extensions isomorphes sont souvent appelées

D extensions équivalentes. Deux groupes X et Y qui sont les deux des extensions de A par G peuvent être des groupes isomorphes sans qu'ils soient des extensions équivalentes.

$$\begin{tikzcd} 0 \arrow[r] & A \arrow[r] & X \arrow[r] \arrow[d, "\mu"'] & G \arrow[r] & 1 \\ 0 \arrow[r] & A \arrow[r] & Y \arrow[r] & G \arrow[r] & 1 \end{tikzcd}$$

On ne peut donc pas compléter le diagramme ci-dessus par 1_A et 1_B pour obtenir le diagramme commutatif (33).

Soit X une extension de A par G telle que la classe de facteurs [m] qu'elle détermine contient le facteur trivial m_o :

(34) $\forall\alpha,\beta \in G \quad m_o(\alpha,\beta) = 0 \in A$.

D Une telle extension s'appelle <u>extension triviale</u>, la suite exacte courte qui lui correspond est une <u>suite exacte courte</u>

D <u>scindée</u>. Le groupe $X[A,G,\varphi,m_o]$ est appelé un <u>produit semi-direct</u> de A par G; on le notera $A\times_\varphi G$. La loi interne dans $A\times_\varphi G$ est

(35) $(a,\alpha) + (b,\beta) = (a+(\varphi\alpha)b,\ \alpha\beta)$.

Notez que l'on ne peut pas parler en général <u>du</u> produit semi-direct de deux groupes A et B; il y en a un pour chaque $\varphi : B \longrightarrow A(A)$. Chaque extension triviale est équivalente à un produit semi-direct, le facteur $m \in [m_o]$ associé à une extension triviale est donc de la forme

(36) $m(\alpha,\beta) = c\alpha+(\varphi\alpha)(c\beta) - c(\alpha\beta)$.

Et maintenant la propriété la plus importante :

<u>Proposition 2.4</u> . Une suite exacte courte

$$0 \longrightarrow A \xrightarrow[\kappa]{} X \xrightarrow[\sigma]{} G \longrightarrow 1$$

est scindée ssi σ est une rétraction.

<u>Dém.</u>: C'est évident puisque, en vertu de (34) :

$$r_o\alpha + r_o\beta - r_o(\alpha\beta) = m_o(\alpha,\beta) = 0 \quad .$$

On voit que r_o est un homomorphisme (injectif d'ailleurs) tel que $\sigma r_o = 1_G$. //

Dans une extension triviale X de A par G (non seulement $A \simeq \kappa A \lhd X$ mais aussi)

(37) $G \simeq rG \subset X$.

Revenons maintenant à nos discussions du premier chapitre. Nous avons vu qu'un épimorphisme de groupes n'est pas nécessairement une rétraction. On voit maintenant que dire qu'un épimorphisme de groupes $\sigma : X \longrightarrow G$ est une rétraction équivaut à dire que X est isomorphe à un produit semi-direct de Ker σ par G. Or tous les groupes n'ont pas cette structure.

Si dans un produit semi-direct $A \times_{\varphi} G$ l'application φ est

D l'application triviale $o : G \longrightarrow A(A)$ on obtient <u>le produit direct</u> de A par G que l'on écrit $A \times G$. La loi interne dans $A \times G$ s'écrit simplement

(38) $$(a,\alpha) + (b,\beta) = (a+b, \alpha\beta) \quad .$$

Evidemment un relèvement pour un produit direct est un monomorphisme de groupes, mais si l'on tient compte de (12) on voit

$$r\alpha + a - r\alpha = (\varphi\alpha)a = a$$

i.e. Imr est un sous-groupe du centralisateur $C_X(A)$ de A dans X

(39) $$\operatorname{Im} r \subset C_X(A) \quad .$$

En d'autres termes pour chaque représentation (6) des éléments de X on a la propriété suivante

$$x = a + r\alpha = r\alpha + a \quad .$$

Mais maintenant (non seulement σ est une rétraction, mais aussi) κ est une corétraction. En effet, définissons une application

$$s : X \longrightarrow A$$

$$s : (a+r\alpha) \longmapsto a$$

Cette application s est un homomorphisme qui satisfait à

(40) $$s\kappa = 1_A$$

elle est donc surjective. Quel est le noyau de cette surjection ?

$$\mathrm{Ker}\ s = \mathrm{Im}\ r \simeq G \quad .$$

On a donc

(41) $$G \simeq rG \triangleleft X$$

i.e. X est aussi une extension (triviale) de G par A. On dira donc que c'est le produit direct de A <u>et</u> G.

<u>Proposition 2.5</u> . Un groupe X figurant dans une suite exacte courte

$$0 \longrightarrow A \xrightarrow{\kappa} X \xrightarrow{\sigma} G \longrightarrow 1$$

est un produit direct ssi κ est une corétraction et σ une rétraction.

On voit donc que le dual de la suite exacte scindée ci-dessus, i.e.

$$0 \longrightarrow G \xrightarrow[r]{} X \xrightarrow[s]{} A \longrightarrow 1$$

est aussi une suite exacte courte scindée.

Un autre cas spécial important est celui des extensions

D centrales. Une extension X de A par G est <u>centrale</u> si $A \subset C(X)$. Alors, nécessairement, A est un groupe abélien. La réciproque n'est pas vraie. De plus, le groupe G opère nécessairement trivialement sur A, i.e. on a toujours

$$\forall \alpha \in G \quad \varphi\alpha = 1 \in A(A) \quad .$$

La réciproque n'est pas vraie : ainsi un produit direct n'est pas nécessairement une extension centrale.

Si A est un groupe abélien, le diagramme (5) se simplifie considérablement. En effet dans ce cas C(A) = A, donc I(A) = {1} et A(A) = E(A), de sorte que le diagramme se présente ainsi

(42)
$$\begin{tikzcd} 0 \arrow[r] & A \arrow[r, "\kappa"] & X \arrow[r, "\sigma"] \arrow[d, "\phi"'] & G \arrow[r] \arrow[dl, "\varphi"] & 1 \\ & & A(A) & & \end{tikzcd}$$

Remarquons que A est un G-module puisque, par l'intermédiaire de φ, G opère sur A comme automorphisme de groupes abéliens. De plus, on a $(\varphi 1)a = a$. Ainsi A est un G-module.

Pour M. Hall une extension centrale est quelque chose de plus général que ce que nous avons appelé ainsi. Chez Hall c'est une extension telle que le facteur m est une application dans le centre C(A) de A

(43) $$m : G \times G \longrightarrow C(A) \qquad .$$

Il s'ensuit que l'application

(44) $$\varphi : G \longrightarrow A(A)$$

est un homomorphisme. Et puisque $C(A) \triangleleft A$, les automorphismes de A sont aussi des automorphismes de C(A)

(45) $$A(A) \subset A(C(A)) \qquad .$$

Ainsi G opère sur le groupe abélien C(A), C(A) est donc un G-module. Mais cette notion de centrale n'est pas invariante parce qu'elle n'est pas basée sur le groupe A mais sur l'application m. En d'autres termes si m est une application dans C(A) un facteur équivalent $\bar{m}$ n'est pas nécessairement une application dans C(A). La relation (22), qui maintenant peut s'écrire

(46) $$\bar{m}(\alpha,\beta) = m(\alpha,\beta) + c\alpha + (\varphi\alpha)(c\beta) - c(\alpha\beta) \qquad ,$$

montre qu'il faut imposer la condition

(47) $$c : G \longrightarrow C(A)$$

si l'on veut qu'une extension équivalente à une extension centrale soit elle aussi centrale. Cette condition à son tour entraîne qu'un seul homomorphisme

$$\varphi : G \longrightarrow A(A)$$

est associé à une classe d'extensions équivalentes. Nous appellerons des extensions remplissant les conditions (43) et (47) extensions centrales au sens de Hall ou, plus brièvement,

D extensions de Hall. Ce sont les seules extensions de groupes non-abéliens relativement faciles à étudier. Elles jouent aussi un rôle dans l'étude des extensions générales.

Les relations entre ces différentes notions sont résumées dans le tableau suivant :

$$\underbrace{\text{extension centrale} \Longrightarrow \text{A abélien}}_{\varphi = 0} \Longrightarrow \text{extension de Hall}$$

$\varphi = 0$ — φ est le même homomorphisme pour une classe d'extensions équivalentes

Soit $\varphi : G \longrightarrow A(A)$ un homomorphisme fixe. L'ensemble $Ext(A,G,\varphi)$ des classes d'équivalence des extensions de Hall de A par G pour ce φ choisi a une structure très simple. Si m_1 et m_2 sont deux facteurs nous introduisons une loi interne + en définissant $m_1 + m_2$ par

(48) $$\forall(\alpha,\beta) \in G \quad (m_1 + m_2)(\alpha,\beta) = m_1(\alpha,\beta) + m_2(\alpha,\beta) \quad .$$

Posons $m_3 = m_1 + m_2$. Si l'on calcule $(\varphi\gamma)m_3(\alpha,\beta)$ on voit que m_3 vérifie la relation (16), m_3 est donc aussi un facteur. La loi + est associative et abélienne. L'élément unité pour cette loi est le facteur trivial m_o défini par (34) :

$$\forall\alpha,\beta \qquad m_o(\alpha,\beta) = 0 \in C(A)$$

et l'inverse (-m) de m est défini par

$$\forall\alpha,\beta \qquad (-m)(\alpha,\beta) = -m(\alpha,\beta) \quad .$$

Ainsi les facteurs déterminés par les extensions de A par G pour φ fixe forment un groupe abélien $F_\varphi(A,G)$. La différence entre deux facteurs équivalents

$$c\alpha + \alpha(c\beta) - c(\alpha\beta)$$

satisfait encore à la condition (16) et est donc aussi un

D facteur - parfois appelé <u>facteur principal</u>. (Puisque φ est fixé, nous pouvons écrire αa au lieu de $(\varphi\alpha)a$.) La somme de deux facteurs principaux est encore un facteur principal. L'inverse d'un facteur principal est encore un facteur principal. Ces facteurs principaux $P_\varphi(A,G)$ forment donc un sous-groupe de $F_\varphi(A,G)$:

$$P_\varphi(A,G) \subset F_\varphi(A,G) \quad .$$

On voit donc que $\mathrm{Ext}(A,G,\varphi)$ a la structure d'un groupe abélien :

(49) $$\mathrm{Ext}(A,G,\varphi) = F_\varphi(A,G)/P_\varphi(A,G) \quad .$$

Les éléments de $\mathrm{Ext}(A,G,\varphi)$ sont les classes d'équivalence des extensions de A par G pour ce φ donné. L'élément unité dans ce groupe est la classe des extensions triviales. Je laisse la démonstration immédiate de toutes ces affirmations comme Exercices 2.d.

Un autre exercice, plus amusant, est le suivant :

Exercice 2.e. Déterminer toutes les extensions du groupe cyclique $\mathbb{Z}_n$ (n = 1,2,3,4,5,6) par le groupe cyclique $\mathbb{Z}_2$. Il faut d'abord déterminer tous les homomorphismes $\varphi\colon \mathbb{Z}_n \longrightarrow \mathbb{Z}_2$, puis pour chaque φ les facteurs inéquivalents.

2.2 Obstructions

Nous avons vu que chaque extension, X, de A par G détermine d'une façon univoque un homomorphisme $\psi : G \longrightarrow E(A)$. Mais, étant donné un tel homomorphisme ψ, il ne lui correspond pas nécessairement une extension de A par G. Nous allons déterminer des conditions nécessaires et suffisantes pour l'existence d'une extension.

Nous travaillons dans A(A) au lieu de X et nous aimerions obtenir les analogues des formules (15) et (16). Choisissons donc un représentant, $\varphi\alpha$, de la classe latérale $\psi\alpha$,

$$\varphi\alpha \in \psi\alpha \quad .$$

En procédant comme dans (10) nous trouvons

$$\bar{\sigma}[\varphi\alpha\cdot\varphi\beta\cdot\varphi(\alpha\beta)^{-1}] = \psi\alpha\cdot\psi\beta\cdot\psi(\alpha\beta)^{-1} = \psi 1 = 1$$

de sorte que

(50) $$\exists m(\alpha,\beta) \in A \qquad \varphi\alpha\cdot\varphi\beta = \Omega m(\alpha,\beta)\varphi(\alpha\beta) \quad .$$

(Evidemment $m(\alpha,\beta)$ est déterminé seulement modulo le centre C(A) de A.) Nous avons ainsi obtenu une relation tout à fait semblable à (15).

Utilisons maintenant l'associativité (de la loi interne dans A(A). Nous trouvons :

$$\begin{aligned}
\varphi\alpha\cdot(\varphi\beta\cdot\varphi\gamma) &= \varphi\alpha\cdot\Omega m(\beta,\gamma)\cdot(\varphi\alpha^{-1}\cdot\varphi\alpha)\varphi(\beta\gamma) \\
&= \Omega[(\varphi\alpha)m(\beta,\gamma)]\cdot\Omega m(\alpha,\beta\gamma)\cdot\varphi(\alpha\beta\gamma) \\
(\varphi\alpha\cdot\varphi\beta)\varphi\gamma &= \Omega m(\alpha,\beta)\cdot\varphi(\alpha\beta)\cdot\varphi\gamma \\
&= \Omega m(\alpha,\beta)\cdot\Omega m(\alpha\beta,\gamma)\cdot\varphi(\alpha\beta\gamma) \quad .
\end{aligned}$$

Il s'ensuit que

$$\Omega[(\varphi\alpha)m(\beta,\gamma) + m(\alpha,\beta\gamma) - m(\alpha\beta,\gamma) - m(\alpha,\beta)] = 1 \in I(A) \quad .$$

L'élément $k(\alpha,\beta,\gamma)$ défini par

(51) $$k(\alpha,\beta,\gamma) = (\varphi\alpha)m(\beta,\gamma) + m(\alpha,\beta\gamma) - m(\alpha\beta,\gamma) - m(\alpha,\beta)$$

est donc un élément du centre $C(A)$. Nous avons ainsi trouvé une application

(52) $$k : G \times G \times G \longrightarrow C(A)$$

associé à l'homomorphisme $\psi : G \longrightarrow A$. Evidemment k dépend du choix de φ dans sa classe d'automorphismes et du choix de m et il faudrait examiner comment k varie en fonction de ces choix. C'est précisément cela que nous ne pouvons pas faire maintenant, faute de temps. Mais k a deux propriétés importantes que nous allons démontrer.

<u>Proposition 2.6</u> . Etant donné un homomorphisme $\psi : G \longrightarrow E(A)$, il existe une extension X de A par G, ssi on peut choisir $\varphi\alpha \in \psi\alpha$ et m satisfaisant à (50) tels que $k = 0$, i.e.

$$\forall\alpha,\beta,\gamma \in G \quad k(\alpha,\beta,\gamma) = 0 \quad .$$

D <u>Remarque</u> : Nous appellerons k une <u>obstruction</u> à ψ.

<u>Dém.</u>: Supposons que X existe. Alors nous pouvons choisir un relèvement r qui détermine des applications φ et m satisfaisant à (16) :

$$(\varphi\alpha)m(\beta,\gamma) = m(\alpha,\beta) + m(\alpha\beta,\gamma) - m(\alpha,\beta\gamma) \quad .$$

L'obstruction k correspondant à ce φ et ce m est nulle. Supposons réciproquement que l'obstruction k est nulle. Alors m est un facteur et il existe une extension de A par G correspondant à φ et m (en vertu de la Proposition 2.2). //

Proposition 2.7 . L'application

$$k : G \times G \times G \longrightarrow C(A)$$

satisfait à la relation

(53) $$(\varphi\delta)k(\alpha,\beta,\gamma) - k(\delta\alpha,\beta,\gamma) + k(\delta,\alpha\beta,\gamma) - k(\delta,\alpha,\beta\gamma) + k(\delta,\alpha,\beta) = 0 \quad .$$

Dém.: Ecrivons (51) sous la forme

$$(\varphi\alpha)m(\beta,\gamma) + m(\alpha,\beta\gamma) = k(\alpha,\beta,\gamma) + m(\alpha,\beta) + m(\alpha\beta,\gamma) \quad ,$$

appliquons $(\varphi\delta)$ aux deux côtés, utilisons (50) et (51) et tenons compte du fait que k est une application dans le centre C(A).

$$\begin{aligned}
&(\varphi\delta)(\varphi\alpha)m(\beta,\gamma) + (\varphi\delta)m(\alpha,\beta\gamma) \\
&= m(\delta,\alpha) + \varphi(\delta\alpha)m(\beta,\gamma) - m(\delta,\alpha) + (\varphi\delta)m(\alpha,\beta\gamma) \\
&= m(\delta,\alpha) + k(\delta\alpha,\beta,\gamma) + m(\delta\alpha,\beta) + m(\delta\alpha\beta,\gamma) - m(\delta\alpha,\beta\gamma) \\
&\quad - m(\delta,\alpha) + k(\delta,\alpha,\beta\gamma) + m(\delta,\alpha) + m(\delta\alpha,\beta\gamma) - m(\delta,\alpha\beta\gamma)
\end{aligned}$$

$$\begin{aligned}
&(\varphi\delta)k(\alpha,\beta,\gamma) + (\varphi\delta)m(\alpha,\beta) + (\varphi\delta)m(\alpha\beta,\gamma) \\
&= (\varphi\delta)k(\alpha,\beta,\gamma) + k(\delta,\alpha,\beta) + m(\delta,\alpha) + m(\delta\alpha,\beta) - m(\delta,\alpha\beta) \\
&\quad + k(\delta,\alpha\beta,\gamma) + m(\delta,\alpha\beta) + m(\delta\alpha\beta,\gamma) - m(\delta,\alpha\beta\gamma) \quad .
\end{aligned}$$

Après réarrangement et comparaison de ces deux expressions on voit bien que la relation (53) est satisfaite. //

Si A est un groupe abélien, φ est un homomorphisme et (50) est satisfait par

$$m(\alpha,\beta) = 0 \qquad \forall \alpha,\beta \in G \quad .$$

Alors k = 0. Ainsi, pour un groupe abélien A et un φ donné, il existe toujours au moins une extension de A par G; c'est le produit semi-direct $A \times_\varphi G$.

3 Cohomologie des groupes

3.1 Définition des groupes de cohomologie

Dans tout ce qui suit A sera un groupe abélien.

La cohomologie non-abélienne est beaucoup moins développée: on peut définir les groupes de cohomologie en dimension zéro et un et trouver un petit morceau de la suite exacte de cohomologie. Nous n'aborderons pas cette théorie.

Soit donc A un G-module. Considérons des applications d'ensembles

(1) $$f^n : \underbrace{G \times \ldots \times G}_{n \text{ fois}} \longrightarrow A \qquad n \geqslant 1$$

$$f^n : (\alpha_1,\ldots,\alpha_n) \longmapsto f^n(\alpha_1,\ldots,\alpha_n) \in A \quad .$$

D Ces applications f^n s'appellent des n-cochaînes. Désignons par $C^n(G,A)$ l'ensemble des n-cochaînes. Pour $n = 0$ nous définissons

$$C^o(G,A) =: A \quad .$$

D'une façon naturelle nous pouvons transférer de A à $C^n(G,A)$ la structure de groupes abéliens. Nous définissons une addition de cochaînes en posant pour $f,g \in C^n(G,A)$

(2) $$(f+g)(\alpha_1,\ldots,\alpha_n) = f(\alpha_1,\ldots,\alpha_n) + g(\alpha_1,\ldots,\alpha_n) \quad .$$

A étant un G-module l'opération des éléments de G sur $f(\alpha_1,\ldots,\alpha_n)$ est aussi définie.

Avec les cochaînes nous allons construire une suite diffé-

D rentielle de groupes abéliens appelée aussi complexe de cochaînes. Définissons une application

$$d_n : C^n(G,A) \longrightarrow C^{n+1}(G,A)$$

de la manière suivante

(3) $$(d_n f^n)(\alpha_1,\dots,\alpha_{n+1}) = (-1)^{n+1}\sum_{i=0}^{n+1}(-1)^i(p^i_{n+1}f^n)(\alpha_1,\dots,\alpha_{n+1})$$

(3') $$(p^i_{n+1}f^n)(\alpha_1,\dots,\alpha_{n+1}) = \begin{cases} \alpha_1[f^n(\alpha_2,\dots,\alpha_{n+1})] & i=0 \\ f^n(\alpha_1,\dots,\alpha_i\alpha_{i+1},\dots,\alpha_{n+1}) & 0<i<n+1 \\ f^n(\alpha_1,\dots,\alpha_n) & i=n+1 \end{cases}$$

Illustrons cela en basse dimension :

$n = 0$, $a \in A$

$$(d_o a)(\alpha) = -[(p^o_1 a)(\alpha) - (p^1_1 a)(\alpha)] = -\alpha a + a$$

$n = 1$, $f \in C^1$

$$(d_1 f)(\alpha_1,\alpha_2) = (p^o_2 f)(\alpha_1,\alpha_2) - (p^1_2 f)(\alpha_1,\alpha_2) + (p^2_2 f)(\alpha_1,\alpha_2)$$
$$= \alpha_1 f(\alpha_2) - f(\alpha_1\alpha_2) + f(\alpha_1)$$

$n = 2$, $f \in C^2$

$$(d_2 f)(\alpha_1,\alpha_2,\alpha_3) = -\alpha_1 f(\alpha_2,\alpha_3) + f(\alpha_1\alpha_2,\alpha_3) - f(\alpha_1,\alpha_2\alpha_3) + f(\alpha_1,\alpha_2)$$

$n = 3$, $f \in C^3$

$$(d_3 f)(\alpha_1,\alpha_2,\alpha_3,\alpha_4) =$$
$$= \alpha_1 f(\alpha_2,\alpha_3,\alpha_4) - f(\alpha_1\alpha_2,\alpha_3,\alpha_4) + f(\alpha_1,\alpha_2\alpha_3,\alpha_4)$$
$$- f(\alpha_1,\alpha_2,\alpha_3\alpha_4) + f(\alpha_1,\alpha_2,\alpha_3) \quad .$$

D L'application d_n s'appelle <u>différentielle</u>.

Exercice 3.a . Montrer que p^i_n est un homomorphisme de groupes abéliens.

<u>Proposition 3.1</u> . La suite C(G,A) ci-dessous

$$C(G,A): \quad A \xrightarrow{d_o} C^1(G,A) \xrightarrow{d_1} C^2(G,A) \longrightarrow \dots$$

est une suite différentielle de groupes abéliens.

<u>Dém.</u>: Il nous faut montrer que

(4) $$d_n d_{n-1} = o \quad .$$

C'est un calcul un peu long.

$$d_n d_{n-1} = \left[(-1)^{n+1}\sum_{i=0}^{n+1}(-1)^i p_{n+1}^{\,i}\right]\left[(-1)^n\sum_{j=0}^{n}(-1)^j p_n^j\right]$$

$$= -\sum_{i=0}^{n+1}\sum_{j=0}^{n}(-1)^{i+j}p_{n+1}^i p_n^j$$

$$= -\sum_{0\leq i\leq j\leq n}(-1)^{i+j}p_{n+1}^i p_n^j - \sum_{0\leq j<i\leq n+1}(-1)^{i+j}p_{n+1}^i p_n^j$$

$$= -\sum_{0\leq i\leq j\leq n}(-1)^{i+j}p_{n+1}^i p_n^j - \sum_{0\leq j\leq i\leq n}(-1)^{i+1+j}p_{n+1}^{i+1} p_n^j$$

$$= -\sum_{0\leq i\leq j\leq n}(-1)^{i+j}p_{n+1}^i p_n^j - \sum_{0\leq i\leq j\leq n}(-1)^{i+j+1}p_{n+1}^{j+1} p_n^i$$

$$= \sum_{0\leq i\leq j\leq n}(-1)^{i+j}(p_{n+1}^{j+1}p_n^i - p_{n+1}^i p_n^j) \quad .$$

Evaluons cette somme. Nous devons montrer qu'elle est nulle.

Il y a 7 types de termes :

(i) $i = j = 0$

(ii) $i = 0,\ 0 < j < n$

(iii) $i = 0,\ j = n$

(iv) $0 < i < j < n$

(v) $0 < i = j < n$

(vi) $0 < i < j = n$

(vii) $i = j = n$

Examinons le cas (iv) :

$$\left[p_{n+1}^{j+1}(p_n^i f^{n-1})\right](\alpha_1,\ldots,\alpha_{n+1}) = (p_n^i f^{n-1})(\alpha_1,\ldots,\alpha_{j+1}\alpha_{j+2},\ldots,\alpha_{n+1})$$

$$= f^{n-1}(\alpha_1,\ldots,\alpha_i\alpha_{i+1},\ldots,\alpha_{j+1}\ \alpha_{j+2},\ldots,\alpha_{n+1})$$

$$\left[p_{n+1}^{i}(p_n^j f^{n-1})\right](\alpha_1,\ldots,\alpha_{n+1}) = (p_n^j f^{n-1})(\alpha_1,\ldots,\alpha_i\alpha_{i+1},\ldots,\alpha_{n+1})$$

$$= f^{n-1}(\alpha_1,\ldots,\alpha_i\alpha_{i+1},\ldots,\alpha_{j+1}\alpha_{j+2},\ldots,\alpha_{n+1}) \quad .$$

Exercice 3.b . Montrer que la somme donne zéro pour les autres types de termes.

Posons

(5) $$Z^n(G,A) =: \mathrm{Ker}\ d_n \subset C^n(G,A)$$

et

(6) $$B^n(G,A) =: \mathrm{Im}\ d_{n-1} \subset C^n(G,A) \quad .$$

D Les éléments de Z^n s'appellent n-cocycles, ceux de B^n

D s'appellent n-cobords. $B^n(G,A)$ et $Z^n(G,A)$ sont évidemment des sous-groupes de $C^n(G,A)$. Nous venons de démontrer que

$$B^n(G,A) \subset Z^n(G,A) \quad .$$

Nous pouvons donc former le quotient

(7) $$H^n(G,A) =: Z^n(G,A) \,/\, B^n(G,A) \quad .$$

D Le groupe abélien $H^n(G,A)$ est appelé n-ième groupe de cohomologie (de G avec coefficients dans A) ou n-ième groupe de cohomologie du complexe C(G,A). Ses éléments sont des classes de n-cohomologie, c'est-à-dire les n-cocycles pris modulo les n-cobords. Pour un $f \in Z^n(G,A)$ nous notons $[f] \in H^n(G,A)$ sa classe de cohomologie ;

$$[f_1] = [f_2] \in H^n(G,A)$$

signifie donc

$$f_1 \equiv f_2 \qquad (\mathrm{mod}\ B^n(G,A))$$

ou encore

$$\exists g \in C^{n-1}(G,A) \qquad f_1 = f_2 + dg \quad ;$$

On dit alors que f_1 et f_2 sont cohomologues.

Le groupe de cohomologie $H^n(G,A)$ révèle la non-exactitude du complexe C(G,A) à l'endroit $C^n(G,A)$. Le complexe est exact à cet endroit si chaque cocycle est un cobord, i.e. $H^n(G,A) = 0$.

3.2 Interprétations en dimensions 0, 1, 2 et 3

Maintenant passons en revue les basses dimensions. Les 0-cocycles sont des éléments $a \in A$, satisfaisant à la relation

$$\forall \alpha \in G \qquad \alpha a = a$$

Le groupe des 0-cocycles est donc le sous-groupe des éléments de A laissés invariants par G. Nous noterons

(8) $$A^G =: Z^o(G,A) =: H^o(G,A) \qquad .$$

(Les 0-cobords n'étant pas définis par (6), nous posons $B^o(G,A) = 0$.) Un 1-cocycle est une application $f: G \longrightarrow A$ qui satisfait à la relation

(9) $$f(\alpha_1\alpha_2) = f(\alpha_1) + \alpha_1 f(\alpha_2) \qquad .$$

D Une telle application est appelée <u>homomorphisme croisé</u>. Si A est un G-module trivial, un homomorphisme croisé est un homomorphisme. Un 1-cobord est une application $f_a: G \longrightarrow A$ qui (pour chaque élément $a \in A$ fixé) est défini de la façon suivante

(10) $$f_a(\alpha) = a - \alpha a \qquad .$$

D Une telle application est appelée <u>homomorphisme croisé principal</u>. Un 2-cocycle m est une application $m: G \times G \longrightarrow A$ satisfaisant à

(11) $$\alpha m(\beta,\gamma) = m(\alpha,\beta) + m(\alpha\beta,\gamma) - m(\alpha,\beta\gamma) \qquad .$$

C'est donc un facteur. Un 2-cobord est une application $f: G \times G \longrightarrow A$ construite à partir d'une application $c: G \longrightarrow A$ de la façon suivante

(12) $$f_c(\alpha,\beta) = c(\alpha) + \alpha c(\beta) - c(\alpha\beta) \qquad .$$

C'est donc un facteur principal.

Nous pouvons maintenant exprimer en langage cohomologique les propriétés des extensions d'un groupe abélien A par un groupe G. La Proposition 2.1 dit qu'une extension X d'un groupe abélien A par un groupe G détermine un homomorphisme $\varphi : G \longrightarrow A(A)$ et une classe de cohomologie $[m] \in H^2_\varphi(G,A)$. Nous avons ajouté l'indice inférieur φ à H pour rappeler que la structure de G-module de A est déterminée par φ. Des extensions équivalentes déterminent la même classe de cohomologie $[m] \in H^2_\varphi(G,A)$. Enfin, on peut identifier $F_\varphi(A,G)$ à $Z^2_\varphi(G,A)$, $P_\varphi(A,G)$ à $B^2_\varphi(G,A)$ et finalement le groupe $\mathrm{Ext}(A,G,\varphi)$ des classes d'équivalence d'extensions de A par G au deuxième groupe de cohomologie $H^2_\varphi(G,A)$. Si $H^2_\varphi(G,A) = 0$, alors pour ce φ donné il existe une seule classe d'équivalence d'extensions de A par G : la classe triviale qui contient le produit semi-direct $A \times_\varphi G$.

Examinons encore les 3-cocycles. Un 3-cocycle k est une application $k : G \times G \times G \longrightarrow A$ qui satisfait à

(13) $$\delta k(\alpha,\beta,\gamma) - k(\delta\alpha,\beta,\gamma) + k(\delta,\alpha\beta,\gamma) - k(\delta,\alpha,\beta\gamma) + k(\delta,\alpha,\beta) = 0$$

On voit donc qu'une obstruction à un homomorphisme $\psi : G \longrightarrow E(A)$ -- avec A non-abélien ! -- est un 3-cocycle avec coefficients dans C(A) :

(14) $$k \in Z^3_\psi(G,C(A)) \quad .$$

Nous avons ainsi donné des interprétations de la cohomologie en dimensions 0, 2 et 3. Le premier groupe de cohomologie est étroitement lié au théorème de Maschke et à celui de Bieberbach. Le théorème de Maschke dit que la représentation d'un groupe fini G par des automorphismes d'un K-module A (où K est un corps dont la caractéristique ne divise pas l'ordre du groupe) est une somme directe de représentations irréductibles. En d'autres termes, cette représentation est complètement réductible. Si A est un K-module et G opère sur A, alors A est aussi un K(G)-module. Ici K(G) est l'anneau du groupe avec coefficients dans K. (L'exercice 1.f avait pour but la démonstration que chaque G-module est un $\mathbb{Z}(G)$-module, avec $\mathbb{Z}(G)$ l'anneau du groupe G sur les entiers.) Exprimé en terme de modules le théorème de Maschke dit que, dans les conditions énoncées ci-dessus, le K(G)-module A est complètement réductible, en d'autres termes que chaque sous-module A' d'un K(G)-module A est membre d'une somme directe :

$$\forall A' \subset A \qquad \exists A'' \subset A \qquad A' \oplus A'' = A \qquad .$$

Or, on peut montrer que l'on est dans la situation de complète réductibilité chaque fois qu'un certain premier groupe de cohomologie est trivial. D'une façon plus précise on peut démontrer la proposition suivante :

Soit K un corps et G un groupe et soit

$$H^1(G,A) = 0$$

pour tout K(G)-module A. Alors tout K(G)-module A est complètement réductible. La démonstration de ce théorème serait un peu longue à cause de la préparation qu'elle exigerait. Nous devons donc renoncer à la faire. Nous pouvons cependant illustrer ce théorème. Pour ce faire, nous introduisons une différentielle $\underline{d}^n$ légèrement plus générale que celle que nous avons introduite précédemment. La seule différence est dans le terme $p_{n+1}^{n+1}f^n$ qui maintenant est défini ainsi

$$(p_{n+1}^{n+1}f^n)(\alpha_1,\ldots,\alpha_{n+1}) = f(\alpha_1,\ldots,\alpha_n)\alpha_{n+1}$$

i.e. le groupe G opère maintenant à gauche et à droite sur A. On peut vérifier facilement que la propriété $d_{n+1}d_n = 0$ reste vraie. On retrouve d'ailleurs la définition originale, en supposant que l'opération à droite de G est triviale. Un 1-cocycle $f \in Z^1(G,A)$ satisfait maintenant à

(16) $$f(\alpha\beta) = f(\alpha)\beta + \alpha f(\beta)$$

et un 1-cobord $f_a \in B^1(G,A)$ à

$$f_a(\alpha) = a\alpha - \alpha a \quad .$$

Soit maintenant G un groupe fini et M une représentation matricielle réduite et de dimension finie de G avec coefficients dans K.

$$M(\alpha)M(\beta) = M(\alpha\beta)$$

ou

$$\begin{pmatrix} D(\alpha) & 0 \\ U(\alpha) & L(\alpha) \end{pmatrix}\begin{pmatrix} D(\beta) & 0 \\ U(\beta) & L(\beta) \end{pmatrix} = \begin{pmatrix} D(\alpha)D(\beta) & 0 \\ U(\alpha)D(\beta)+L(\alpha)U(\beta) & L(\alpha)L(\beta) \end{pmatrix}$$
$$= \begin{pmatrix} D(\alpha\beta) & 0 \\ U(\alpha\beta) & L(\alpha\beta) \end{pmatrix} \quad .$$

Mais ceci implique que

$$D(\alpha\beta) = D(\alpha)D(\beta)$$

$$L(\alpha\beta) = L(\alpha)L(\beta)$$

et

(17) $$U(\alpha\beta) = U(\alpha)D(\beta) + L(\alpha)U(\beta) \quad .$$

La comparaison de (17) avec (16) montre que

$$U \in Z^1(G,\hat{A}) \quad .$$

Mais quel est le groupe abélien $\hat{A}$ dont il s'agit ici. Si d et l sont les dimensions de D et de L respectivement, $\hat{A}$ est le groupe abélien additif de matrices rectangulaires $d \times l$.

Supposons maintenant que $H^1(G,\hat{A}) = 0$, i.e. que chaque cocycle est un cobord. Alors

$$\forall\alpha \in G \qquad \exists V \in \hat{A} \qquad U(\alpha) = VD(\alpha) - L(\alpha)V$$

et

$$\begin{pmatrix} 1 & 0 \\ V & 1 \end{pmatrix}^{-1} \begin{pmatrix} D(\alpha) & 0 \\ U(\alpha) & L(\alpha) \end{pmatrix} \begin{pmatrix} 1 & 0 \\ V & 1 \end{pmatrix} = \begin{pmatrix} D(\alpha) & 0 \\ 0 & L(\alpha) \end{pmatrix} .$$

Ainsi $H^1(G,A) = 0$ entraîne la réductibilité complète. Mais il faut encore savoir dans quelles conditions un groupe de cohomologie est trivial. Plus tard, nous voulons examiner quelques-unes de ces conditions et nous nous servirons, entre autres, d'une généralisation de la méthode, très féconde, que Schur a introduite dans la démonstration du théorème de Maschke.

Le théorème de Bieberbach dit que dans un espace euclidien de dimension n, deux groupes crystallographiques isomorphes peuvent toujours être insérés comme sous-groupes conjugués dans le groupe affine. Nous avons pu montrer récemment que cela aussi dépend de la trivialité d'un certain premier groupe de cohomologie.

3.3 Changement de module - suite exacte de cohomologie

Soit

$$\lambda : A \longrightarrow \bar{A}$$

un homomorphisme de G-bimodules, i.e. un homomorphisme de groupes abéliens tel que

$$\forall \alpha,\beta \in G \qquad \lambda(\alpha a \beta) = \alpha(\lambda a)\beta \qquad .$$

Nous allons examiner maintenant ce que l'existence de cet homomorphisme implique pour les groupes de cohomologie $H^n(G,A)$ et $H^n(G,\bar{A})$. Pour ce faire, nous introduisons l'application

$$\lambda_*^n : C^n(G,A) \longrightarrow C^n(G,\bar{A})$$

définie par le diagramme commutatif suivant

(18)
$$\begin{tikzcd} G\times\ldots\times G \arrow[r, "f"] \arrow[dr, "\lambda_*^n f"'] & A \arrow[d, "\lambda"] \\ & \bar{A} \end{tikzcd}$$

On vérifie facilement que λ_*^n est un homomorphisme de groupes abéliens :

$$\begin{aligned} [\lambda_*^n(f+g)](\alpha_1,\ldots,\alpha_n) &= \lambda[(f+g)(\alpha_1,\ldots,\alpha_n)] \\ &= \lambda[f(\alpha_1,\ldots,\alpha_n) + g(\alpha_1,\ldots,\alpha_n)] \\ &= \lambda[f(\alpha_1,\ldots,\alpha_n)] + \lambda[g(\alpha_1,\ldots,\alpha_n)] \\ &= (\lambda_*^n f)(\alpha_1,\ldots,\alpha_n) + (\lambda_*^n g)(\alpha_1,\ldots,\alpha_n) \\ &= (\lambda_*^n f + \lambda_*^n g)(\alpha_1,\ldots,\alpha_n) \qquad . \end{aligned}$$

Soient

$$d_n : C^n(G,A) \longrightarrow C^{n+1}(G,A)$$

et

$$\bar{d}_n : C^n(G,\bar{A}) \longrightarrow C^{n+1}(G,\bar{A})$$

les différentielles des complexes construits respectivement avec A et $\bar{A}$.

Proposition 3.2.

(19) $$\lambda_*^{n+1}\, d_n = \bar{d}_n \lambda_*^n$$

Dém.:

$$[\lambda_*^{n+1}(p_{n+1}^o f^n)](\alpha_1,\ldots,\alpha_{n+1}) = \lambda\{\alpha_1[f^n(\alpha_2,\ldots,\alpha_{n+1})]\}$$

$$= \alpha_1\{\lambda[f^n(\alpha_2,\ldots,\alpha_{n+1})]\} = \alpha_1[(\lambda_*^n f^n)(\alpha_2,\ldots,\alpha_{n+1})]$$

$$= [\bar{p}_{n+1}^o(\lambda_* f^n)](\alpha_1,\ldots,\alpha_{n+1})$$

$$[\lambda_*^{n+1}(p_{n+1}^i f^n)](\alpha_1,\ldots,\alpha_{n+1}) = \lambda[f^n(\alpha_1,\ldots,\alpha_i\alpha_{i+1},\ldots,\alpha_{n+1})]$$

$$= (\lambda_*^n f^n)(\alpha_1,\ldots,\alpha_i\alpha_{i+1},\ldots,\alpha_{n+1})$$

$$= [\bar{p}_n^i(\lambda_*^n f^n)](\alpha_1,\ldots,\alpha_{n+1}) \quad , \quad i = 1,2,\ldots,n$$

$$[\lambda_*^{n+1}(p_{n+1}^{n+1} f^n)](\alpha_1,\ldots,\alpha_{n+1}) = \lambda[f^n(\alpha_1,\ldots,\alpha_n)\alpha_{n+1}]$$

$$= [(\lambda_*^n f^n)(\alpha_1,\ldots,\alpha_n)]\alpha_{n+1} = [\bar{p}_{n+1}^{n+1}(\lambda_*^n f^n)](\alpha_1,\ldots,\alpha_{n+1}) \quad //$$

On a ainsi montré que le diagramme ci-dessous est commutatif :

$$\begin{tikzcd}
C(G,A) \ \ldots \arrow[r, "d_{n-1}"] & C^n(G,A) \arrow[r, "d_n"] \arrow[d, "\lambda_*^n"] & C^{n+1}(G,A) \arrow[r, "d_{n+1}"] \arrow[d, "\lambda_*^{n+1}"] & \ldots \\
C(G,\bar{A}) \ \ldots \arrow[r, "\bar{d}_{n-1}"] & C^n(G,\bar{A}) \arrow[r, "\bar{d}_n"] & C^{n+1}(G,\bar{A}) \arrow[r, "\bar{d}_{n+1}"] & \ldots
\end{tikzcd} .$$

L'ensemble des homomorphismes λ_*^n est appelé un morphisme du complexe $C(G,A)$ au complexe $C(G,\bar{A})$. On note souvent

(20) $$\lambda_*^n =: C^n(G,\lambda)$$

et

$$C(G,\lambda) : \ C(G,A) \longrightarrow C(G,\bar{A}) \quad .$$

Soit $d_n f^n = 0$, alors

$$\lambda_*^{n+1}(d_n f^n) = \bar{d}_n(\lambda_*^n f^n) = 0 \quad ;$$

soit maintenant $f^n = d_{n-1}g^{n-1}$, alors

$$\lambda_*^n f^n = \bar{d}_{n-1}(\lambda_*^{n-1} g^{n-1}) \quad .$$

La commutativité (19) implique donc que λ_*^n envoie des cocycles sur des cocycles et des cobords sur des cobords. On a ainsi le diagramme suivant :

$$\begin{tikzcd} 0 \arrow[r] & B^n(G,A) \arrow[r] \arrow[d] & Z^n(G,A) \arrow[r, "{[\ ]}"] \arrow[d, "\lambda_*^n"] & H^n(G,A) \arrow[r] \arrow[d, dashed, "{[\lambda_*^n]}"] & 0 \\ 0 \arrow[r] & B^n(G,\bar{A}) \arrow[r] & Z^n(G,\bar{A}) \arrow[r, "{[\ ]}"'] & H^n(G,\bar{A}) \arrow[r] & 0 \end{tikzcd}$$

(Dans ce diagramme nous avons désigné par λ_*^n aussi la restriction à $Z^n(G,A)$ de λ_*^n).Il existe donc d'après la proposition 1.14 un unique homomorphisme

$$[\lambda_*^n] \ : \ H^n(G,A) \longrightarrow H^n(G,\bar{A})$$

qui rend le diagramme commutatif. La commutativité s'exprime par la relation

$$[\lambda_*^n f] = [\lambda_*^n][f] \quad :$$

la classe de cohomologie de l'image est l'image de la classe de cohomologie. On trouve souvent la notation

$$[\lambda_*^n] =: H^n(G,\lambda) \quad .$$

<u>Proposition 3.3</u>. Soient λ et μ deux homomorphismes de G-bimodules tels que $\lambda\mu$ soit défini. Alors

(21)
$$(\lambda\mu)_* = \lambda_*\mu_* \ , \qquad C^n(G,\lambda\mu) = C^n(G,\lambda)C^n(G,\mu)$$
$$[(\lambda\mu)_*] = [\lambda_*][\mu_*], \qquad H^n(G,\lambda\mu) = H^n(G,\lambda)H^n(G,\mu) \quad .$$

De plus, pour chaque G-bimodule A on a :

(22)
$$C^n(G,1_A) = 1_{C^n(G,A)}$$
$$H^n(G,1_A) = 1_{H^n(G,A)} \quad .$$

<u>Dém.</u>: Immédiate.

<u>Proposition 3.4</u>. Soit

$$\begin{tikzcd} A \arrow[r, "\lambda"] \arrow[d, "\mu"'] & B \arrow[d, "\nu"] \\ C \arrow[r, "\omega"'] & D \end{tikzcd}$$

un diagramme commutatif de G-bimodules, alors les deux diagrammes ci-dessous sont aussi commutatifs :

(23)
$$\begin{tikzcd} C^n(G,A) \arrow[r, "\lambda_*"] \arrow[d, "\mu_*"'] & C^n(G,B) \arrow[d, "\nu_*"] \\ C^n(G,C) \arrow[r, "\omega_*"'] & C^n(G,D) \end{tikzcd}$$

$$\begin{tikzcd} H^n(G,A) \arrow[r, "{[\lambda_*]}"] \arrow[d, "{[\mu_*]}"'] & H^n(G,B) \arrow[d, "{[\nu_*]}"] \\ H^n(G,C) \arrow[r, "{[\omega_*]}"'] & H^n(G,D) \end{tikzcd}$$

Dém.: Immédiate.

Proposition 3.5. Soit

$$0 \longrightarrow A \xrightarrow[i]{} B \xrightarrow[p]{} C \longrightarrow 0$$

une suite exacte de G-bimodules. Alors les deux suites ci-dessous sont exactes

$$0 \longrightarrow C^n(G,A) \xrightarrow[i_*]{} C^n(G,B) \xrightarrow[p_*]{} C^n(G,C) \longrightarrow 0$$

$$H^n(G,A) \xrightarrow[{[i_*]}]{} H^n(G,B) \xrightarrow[{[p_*]}]{} H^n(G,C) \quad .$$

Dém.: (i) i_* est injectif.

$$i_* f_A = 0 \in C^n(G,B) \quad .$$

Cela veut dire

$$\forall \alpha_1,\dots,\alpha_n \in G \quad (i_* f_A)(\alpha_1,\dots,\alpha_n) = i\,[f_A(\alpha_1,\dots,\alpha_n)] = 0 \quad .$$

Il s'ensuit

$$f_A(\alpha_1,\dots,\alpha_n) = 0$$

i.e.

$$f_A = 0 \quad .$$

(ii) p_* est surjectif. Soit $f_C \in C^n(G,C)$. Alors

$$\forall \alpha_1,\dots,\alpha_n \in G \quad f(\alpha_1,\dots,\alpha_n) \in C$$

et

$$\exists b \in B \qquad pb = f_C(\alpha_1,\ldots,\alpha_n) \qquad .$$

Posons

$$b = f_B(\alpha_1,\ldots,\alpha_n) \qquad .$$

Alors

$$(p_* f_B)(\alpha_1,\ldots,\alpha_n) = f_C(\alpha_1,\ldots,\alpha_n) \qquad .$$

(iii) Exactitude en $C^n(G,B)$. Nous savons que

$$pi = 0$$

entraîne

$$p_* i_* = 0 \qquad ,$$

i.e.

$$\mathrm{Im}\ i_* \subset \mathrm{Ker}\ p_* \qquad .$$

Supposons maintenant $f_B \in \mathrm{Ker}\ p_*$, i.e.

$$\forall \alpha_1,\ldots,\alpha_n \in G \qquad p[f_B(\alpha_1,\ldots,\alpha_n)] = 0 \in C$$

donc

$$\exists a \in A \qquad ia = f_B(\alpha_1,\ldots,\alpha_n) \qquad .$$

Posons

$$a = f_A(\alpha_1,\ldots,\alpha_n) \qquad .$$

Alors

$$i_* f_A = f_B \qquad .$$

(iv) Exactitude en $H^n(G,B)$. Nous savons que

$$p_* i_* = 0$$

entraîne

$$[p_*][i_*] = 0 \qquad ,$$

i.e.

$$\mathrm{Im}\ [i_*] \subset \mathrm{Ker}\ [p_*] \qquad .$$

Supposons maintenant $[f_B] \in \operatorname{Ker} [p_*] \subset H^n(G,B)$

i.e.

$$[p_*][f_B] = [p_* f_B] = 0 \in H^n(G,C) \quad .$$

Alors $p_* f_B$ est un n-cobord :

$$p_* f_B \in B^n(G,C)$$

et

$$\exists f_C \in C^{n-1}(G,C) \quad d_{n-1} f_C = p_* f_B \quad .$$

Mais, p_* étant surjectif,

$$\exists g_B \in C^{n-1}(G,B) \quad f_C = p_* g_B \quad .$$

Alors

$$p_* f_B = d_{n-1} p_* g_B = p_* d_{n-1} g_B$$

et

$$p_*(f_B - d_{n-1} g_B) = 0 \quad .$$

En vertu de (iii)

$$\exists f_A \in C^n(G,A) \quad f_B - d_{n-1} g_B = i_* f_A$$

et puisque $f_B - d_{n-1} g_B \in Z^n(G,B)$ nous trouvons

$$[f_B - d_{n-1} g_B] = [f_B] = [i_*][f_A] \quad . //$$

Dans ces calculs, nous avons utilisé le même symbole d_n pour désigner les homomorphismes différentiels dans chacun des trois complexes $C(G,A)$, $C(G,B)$ et $C(G,C)$. La proposition suivante est une conséquence immédiate.

<u>Proposition 3.6</u>. Si

$$0 \longrightarrow A \xrightarrow[i]{} B \xrightarrow[p]{} C \longrightarrow 0$$

est une suite exacte, alors

$$0 \longrightarrow C(G,A) \xrightarrow[C(G,i)]{} C(G,B) \xrightarrow[C(G,p)]{} C(G,C) \longrightarrow 0$$

est une suite exacte courte de complexes de cochaines. Dans cette suite le symbole 0 représente le complexe trivial

$C(G,0)$:

$$\longrightarrow C^{n-1}(G,0) \longrightarrow C^n(G,0) \longrightarrow C^{n+1}(G,0) \longrightarrow$$

dans lequel chaque cochaine est isomorphe au groupe trivial {0}.

Rappelons que la suite exacte courte de complexes ci-dessus n'est autre chose que le diagramme commutatif de cochaines suivant :

$$\begin{tikzcd}
 & {} \arrow[d] & {} \arrow[d] & {} \arrow[d] & \\
0 \arrow[r] & C^{n-1}(G,A) \arrow[r, "i_*"] \arrow[d, "d_{n-1}"] & C^{n-1}(G,B) \arrow[r, "p_*"] \arrow[d, "d_{n-1}"] & C^{n-1}(G,C) \arrow[r] \arrow[d, "d_{n-1}"] & 0 \\
0 \arrow[r] & C^{n}(G,A) \arrow[r] \arrow[d, "d_{n}"] & C^{n}(G,B) \arrow[r] \arrow[d, "d_{n}"] & C^{n}(G,C) \arrow[r] \arrow[d, "d_{n}"] & 0 \\
0 \arrow[r] & C^{n+1}(G,A) \arrow[r] \arrow[d, "d_{n+1}"] & C^{n+1}(G,B) \arrow[r] \arrow[d, "d_{n+1}"] & C^{n+1}(G,C) \arrow[r] \arrow[d, "d_{n+1}"] & 0 \\
0 \arrow[r] & C^{n+2}(G,A) \arrow[r] \arrow[d] & C^{n+2}(G,B) \arrow[r] \arrow[d] & C^{n+2}(G,C) \arrow[r] \arrow[d] & 0 \\
 & {} & {} & {} &
\end{tikzcd}$$

C'est le diagramme que nous allons utiliser pour faire le dernier pas dans la construction de la suite exacte de cohomologie.

<u>Proposition 3.7.</u> Soit

(24) $$0 \longrightarrow A \xrightarrow[i]{} B \xrightarrow[p]{} C \longrightarrow 0$$

une suite exacte courte de G-bimodules, alors il existe un homomorphisme ∂_n tel que la suite suivante est aussi exacte :

(25) $$\ldots \xrightarrow[{[i_*]}]{} H^n(G,B) \xrightarrow[{[p_*]}]{} H^n(G,C) \xrightarrow[\partial_n]{} H^{n+1}(G,A) \xrightarrow[{[i_*]}]{} H^{n+1}(G,B) \longrightarrow \ldots$$

Si nous désignons la suite exacte (24) par E, nous pouvons désigner la suite exacte (25) par H(E). Cette suite s'appelle

D <u>suite exacte de cohomologie</u>. L'homomorphisme ∂_n s'appelle

D <u>homomorphisme de connection</u>.

<u>Dém.</u>: Nous avons déjà démontré l'exactitude en $H^n(G,B)$. Il nous faut maintenant construire ∂_n et démontrer l'exactitude

des paires $([p_*], \partial_n)$ et $(\partial_n, [i_*])$.

Construction de ∂_n. A un élément

$$[c] \in H^n(G,C) \qquad n \geqslant 0$$

nous voulons faire correspondre un élément

$$\partial_n [c] \in H^{n+1}(G,A) \quad .$$

Choisissons un

$$c \in Z^n(G,C)$$

comme représentant de $[c]$. Alors

(26) $$\exists b \in C^n(G,B) \qquad \underline{p_* b = c} \quad .$$

Puisque

$$d_n c = 0$$

nous trouvons

$$d_n c = d_n p_* b = p_* d_n b = 0 \quad .$$

Donc

(27) $$\exists a \in C^{n+1}(G,A) \qquad \underline{i_* a = d_n b} \quad .$$

Mais alors

$$i_* d_{n+1} a = d_{n+1} i_* a = d_{n+1} d_n b = 0$$

donc

$$d_{n+1} a = 0$$

i.e.

(28) $$a \in Z^{n+1}(G,A) \quad .$$

Posons

(29) $$\underline{\partial_n [c] = [a]} \in H^{n+1}(G,A) \quad .$$

Trois choix interviennent dans notre construction: le choix de $c \in [c]$; le choix de b satisfaisant à (26) et le choix de a satisfaisant à (27). Il nous faut vérifier que l'élément $[a]$ ne dépend pas de ces choix.

Au lieu de c choisissons un autre élément $\bar{c} \in Z^n(G,C)$ dans la classe de cohomologie $[c]$. Ces deux éléments diffèrent par un cobord, i.e.

$$\exists g \in C^{n-1}(G,C) \qquad \bar{c} = c + d_{n-1}g \quad .$$

De plus,

$$\exists h \in C^{n-1}(G,B) \qquad p_*h = g$$

de sorte que

$$\bar{c} = p_*b + d_{n-1}p_*h = p_*(b+d_{n-1}h) =: p_*\bar{b} \quad .$$

Il s'ensuit que

$$d_n\bar{b} = d_n(b+d_{n-1}h) = d_nb \quad .$$

A la place de b choisissons un autre élément $\hat{b} \in C^n(G,B)$ satisfaisant à (26). Alors

$$p_*(\hat{b}-b) = 0$$

et

$$\exists k \in C^n(G,A) \qquad i_*k = \hat{b} - b \quad .$$

Alors

$$d_n\hat{b} = d_nb + d_ni_*k = i_*(a+d_nk) =: i_*\hat{a}$$

de sorte que

$$[\hat{a}] = [a+d_nk] = [a] \quad .$$

Au lieu de $a \in C^{n+1}(G,A)$ choisissons un autre élément $\tilde{a}$ satisfaisant à (27). Alors

$$i_*(\tilde{a}-a) = 0$$

et

$$\tilde{a} = a \quad .$$

La classe de cohomologie $[a]$ est donc déterminée de façon univoque.

Il faut encore vérifier que ∂_n est un homomorphisme de groupes abéliens. Puisque toutes les applications intervenant dans la construction sont de tels homomorphismes, il est facile de voir que c'est le cas. En résumé :

$$\partial_n[c] = [a]$$

si

$$\exists b \in C^n(G,B) \qquad c = p_* b \quad \text{et} \quad d_n b = i_* a \quad .$$

Exactitude en $H^n(G,C)$. Soit

$$[c] \in \mathrm{Im}\ [p_*]$$

i.e.

$$[c] = [p_*][b] \quad .$$

Alors pour $b \in [b]$ nous trouvons

$$i_* a = d_n b = 0$$

donc $a = 0$ et $[a] = 0$, de sorte que

$$\partial_n[p_*][b] = \partial_n[c] = 0$$

i.e.

$$\mathrm{Im}\ [p_*] \subset \mathrm{Ker}\ \partial_n \quad .$$

Soit maintenant

$$[c] \in \mathrm{Ker}\ \partial_n$$

i.e.

$$\partial_n[c] = 0 \quad .$$

Alors

$$\exists b \in C^n(G,B) \qquad d_n b = i_* a = 0 \quad \text{et} \quad p_* b = c$$

donc

$$b \in Z^n(G,B) \quad .$$

et

$$[c] = [p_*][b]$$

i.e.

$$\mathrm{Ker}\ \partial_n \subset \mathrm{Im}\ [p_*] \quad .$$

Exactitude en $H^{n+1}(G,A)$. Les relations (29) et (27) donnent

$$[i_*]\partial_n[c] = [i_*][a] = 0$$

i.e.

$$\mathrm{Im}\ \partial_n \subset \mathrm{Ker}\ [i_*] \quad .$$

Soit maintenant

$$[a] \in \mathrm{Ker}\ [i_*]$$

i.e.

$$[i_*][a] = 0 \quad .$$

Alors $i_* a$ est un cobord :

$$\exists b \in C^n(G,B) \qquad i_* a = d_n b \quad .$$

En posant

$$c = p_* b \quad C^n(G,C) \qquad \text{on trouve donc}$$

$$d_n c = d_n p_* b = p_* d_n b = p_* i_* a = 0 \quad ,$$

$$c \in Z^n(G,C) \qquad \text{et} \qquad \partial_n[c] = [a] \quad ,$$

i.e. $\mathrm{Ker}\ [i_*] \subset \mathrm{Im}\ \partial_n$. //

Remarque. La suite (25) commence par

$$0 \longrightarrow H^o(G/A) \xrightarrow{[i_*]} H^o(G,B) \longrightarrow \ldots$$

i.e., l'homomorphisme $[i_*]$: $H^o(G,A) \longrightarrow H^o(G,B)$ est injectif.

Proposition 3.8 . Soit $\Lambda : E \longrightarrow \bar{E}$

$$\begin{tikzcd}
0 \arrow[r] & A \arrow[r, "i"] \arrow[d, "\lambda"'] & B \arrow[r, "p"] \arrow[d, "\mu"'] & C \arrow[r] \arrow[d, "\nu"'] & 0 & & E \arrow[d, "\Lambda"] \\
0 \arrow[r] & \bar{A} \arrow[r, "\bar{i}"'] & \bar{B} \arrow[r, "\bar{p}"'] & \bar{C} \arrow[r] & 0 & & \bar{E}
\end{tikzcd}$$

un morphisme de suites exactes courtes de G-bimodules, alors on a un morphisme

$$H(\Lambda) : \quad H(E) \longrightarrow H(\bar{E})$$

de suites exactes (longues) de groupes abéliens :

$$\begin{tikzcd} H(E)\cdots \arrow[r] \arrow[d, "H(\Lambda)"'] & H^n(G,B) \arrow[r, "{[p_*]}"] \arrow[d, "{[\mu_*]}"'] & H^n(G,C) \arrow[r, "\partial_n"] \arrow[d, "{[\nu_*]}"'] & H^{n+1}(G,A) \arrow[r, "{[i_*]}"] \arrow[d, "{[\lambda_*]}"] & H^{n+1}(G,B) \arrow[r] \arrow[d, "{[\mu_*]}"] & \cdots \\ H(\bar{E})\cdots \arrow[r] & H^n(G,\bar{B}) \arrow[r, "{[\bar{p}_*]}"'] & H^n(G,\bar{C}) \arrow[r, "\bar{\partial}_n"'] & H^{n+1}(G,\bar{A}) \arrow[r, "{[\bar{I}_*]}"'] & H^{n+1}(G,\bar{B}) \arrow[r] & \cdots \end{tikzcd}$$

<u>Dém.</u>: Une partie de la démonstration est contenue dans la Proposition 3.4. Il nous reste à démontrer la commutativité du carré contenant les homomorphismes de connection.

<u>Dém.</u>: Soit $[c] \in H^n(G,C)$ et

$$\partial_n[c] = [a] \in H^{n+1}(G,A) \quad .$$

D'après la définition de ∂_n cela signifie

$$\exists b \in C^n(G,B) \quad c = p_*b \quad d_nb = i_*a \quad .$$

D'une part nous trouvons

$$[\lambda_*]\partial_n[c] = [\lambda_*a] \in H^{n+1}(G,\bar{A}) \quad ,$$

d'autre part nous avons

$$\bar{\partial}_n[\nu_*][c] = \bar{\partial}_n[\nu_*c] \quad .$$

Il faut montrer $\bar{\partial}_n[\nu_*c] = [\lambda_*a]$. Faisons deux petits calculs :

$$\nu_*c = \nu_*p_*b = \bar{p}_*\mu_*b$$

$$\bar{d}_n(\mu_*b) = \mu_*d_nb = \mu_*i_*a = \bar{I}_*\lambda_*a \quad .$$

Ces formules disent exactement

$$\bar{\partial}_n[\nu_*c] = [\lambda_*a] \quad . \ //$$

<u>Proposition 3.9</u>. Soit

$$\begin{tikzcd} E_1 \arrow[rr, "\Lambda_1"] \arrow[dr, "\Lambda_2\Lambda_1"'] & & E_2 \arrow[dl, "\Lambda_2"] \\ & E_3 & \end{tikzcd}$$

un diagramme de suites exactes courtes de G-modules. Alors on a un diagramme de suites exactes de groupes abéliens.

$$\begin{tikzcd} H(E_1) \arrow[rr, "H(\Lambda_1)"] \arrow[dr, "H(\Lambda_2\Lambda_1)"'] & & H(E_2) \arrow[dl, "H(\Lambda_2)"] \\ & H(E_3) & \end{tikzcd}$$

<u>Dém.</u>: C'est une combinaison des propositions 3.3 et 3.8.

3.4 Changement de groupe

Changeons maintenant le groupe G. Plus précisément, soit

$$\nu : \bar{G} \longrightarrow G$$

un homomorphisme de groupes. Par ν le G-module A devient aussi un $\bar{G}$-module :

$$\forall \bar{a} \in \bar{G} \qquad \bar{a}a =: (\nu\bar{a})a \qquad .$$

L'homomorphisme ν induit une application

(30) $$\nu_n^* : C^n(G,A) \longrightarrow C^n(\bar{G},A)$$

définie ainsi

(31) $$(\nu_n^* f)(\bar{a}_1,\ldots,\bar{a}_n) =: f(\nu\bar{a}_1,\ldots,\nu\bar{a}_n) \qquad .$$

En diagramme

$$\begin{tikzcd} G\times\ldots\times G \arrow[r, "f"] & A \\ \bar{G}\times\ldots\times\bar{G} \arrow[u, "\nu\times\ldots\times\nu"] \arrow[ur, "\nu_n^* f"'] & \end{tikzcd}$$

où évidemment $\nu\times\ldots\times\nu$ est défini par

$$\nu\times\ldots\times\nu : (\bar{a}_1,\ldots,\bar{a}_n) \longmapsto (\nu\bar{a}_1,\ldots,\nu\bar{a}_n) \qquad .$$

On vérifie que ν_n^* est un homomorphisme de groupes abéliens :

$$[\nu_n^*(f+g)](\bar{a}_1,\ldots,\bar{a}_n) = (f+g)(\nu\bar{a}_1,\ldots,\nu\bar{a}_n)$$
$$= f(\nu\bar{a}_1,\ldots,\nu\bar{a}_n) + g(\nu\bar{a}_1,\ldots,\nu\bar{a}_n)$$
$$= (\nu_n^* f)(\bar{a}_1,\ldots,\bar{a}_n) + (\nu_n^* g)(\bar{a}_1,\ldots,\bar{a}_n)$$
$$= (\nu_n^* f + \nu_n^* g)(\bar{a}_1,\ldots,\bar{a}_n) \qquad .$$

<u>Proposition 3.10</u>. Soit

$$d_n : C^n(G,A) \longrightarrow C^{n+1}(G,A)$$

et

$$\bar{d}_n : C^n(G,\bar{A}) \longrightarrow C^{n+1}(\bar{G},A)$$

les différentielles respectivement des complexes $C(G,A)$ et $C(\bar{G},A)$ et ν_n^* l'homomorphisme défini par (31). Alors pour $\forall n \geqslant 0$

(32) $$\nu^*_{n+1}\, d_n = \bar{d}_n\, \nu^*_n \quad ,$$

ou en diagramme

$$\begin{tikzcd}
{} \arrow[r] & C^n(G,A) \arrow[r, "d_n"] \arrow[d, "\nu^*_n"'] & C^{n+1}(G,A) \arrow[r] \arrow[d, "\nu^*_{n+1}"] & \ldots & C(G,A) \\
{} \arrow[r] & C^n(\bar{G},A) \arrow[r, "\bar{d}_n"'] & C^{n+1}(\bar{G},A) \arrow[r] & \ldots & C(\bar{G},A)
\end{tikzcd}$$

<u>Dém.</u>:

$$[\nu^*_{n+1}(p^0_{n+1}f^n)](\bar{a}_1,\ldots,\bar{a}_{n+1}) = (p^0_{n+1}f^n)(\nu\bar{a}_1,\ldots,\nu\bar{a}_{n+1})$$
$$= (\nu\bar{a}_1)[f^n(\nu\bar{a}_2,\ldots,\nu\bar{a}_{n+1})] = (\nu\bar{a}_1)[(\nu^*_n f^n)(\bar{a}_2,\ldots,\bar{a}_{n+1})]$$
$$= \bar{a}_1[(\nu^*_n f^n)(\bar{a}_2,\ldots,\bar{a}_{n+1})] = [\bar{p}^0_{n+1}(\nu^*_n f^n)](\bar{a}_1,\ldots,\bar{a}_{n+1})$$
$$[\nu^*_{n+1}(p^i_{n+1}f^n)](\bar{a}_1,\ldots,\bar{a}_{n+1}) = (p^i_{n+1}f^n)(\nu\bar{a}_1,\ldots,\nu\bar{a}_{n+1})$$
$$= f^n(\nu\bar{a}_1,\ldots,\nu(\bar{a}_i\bar{a}_{i+1}),\ldots,\nu\bar{a}_{n+1})$$
$$= (\nu^*_n f^n)(\bar{a}_1,\ldots,\bar{a}_i\bar{a}_{i+1},\ldots,\bar{a}_{n+1})$$
$$= [\bar{p}^i_{n+1}(\nu^*_n f^n)](\bar{a}_1,\ldots,\bar{a}_{n+1}) \qquad , i = 1,2,\ldots,n$$
$$[\nu^*_{n+1}(p^{n+1}_{n+1}f^n)](\bar{a}_1,\ldots,\bar{a}_{n+1}) = (p^{n+1}_{n+1}f^n)(\nu\bar{a}_1,\ldots,\nu\bar{a}_{n+1})$$
$$= f^n(\nu\bar{a}_1,\ldots,\nu\bar{a}_n) = (\nu^*_n f^n)(\bar{a}_1,\ldots,\bar{a}_n)$$
$$= [\bar{p}^{n+1}_{n+1}(\nu^*_n f^n)](\bar{a}_1,\ldots,\bar{a}_{n+1}) \qquad . //$$

On écrit souvent

$$C^n(\nu,A) =: \nu^*_n \qquad .$$

L'ensemble des ν^*_n ainsi construits est un homomorphisme du complexe $C(G,A)$ au complexe $C(\bar{G},A)$ et on écrit

(33) $$C(\nu,A) : \;\; C(G,A) \longrightarrow C(\bar{G},A) \qquad .$$

La propriété (32) implique que l'image par ν^* d'un cocycle est un cocycle et que l'image d'un cobord est un cobord.

L'homomorphisme ν^* induit donc un homomorphisme, $[\nu^*]$, entre les classes de cohomologie

$$[\nu^*] : H^n(G,A) \longrightarrow H^n(\overline{G},A)$$

et l'on a

$$[\nu^* f] = [\nu^*][f] \quad .$$

On trouve souvent la notation

$$[\nu^*] =: H^n(\nu,A) \quad .$$

Proposition 3.11. Soient $\nu : G \longrightarrow H$ et $\mu : H \longrightarrow K$ deux homomorphismes de groupes et A un K-module. Alors

$$(\mu\nu)^* = \nu^*\mu^* \;, \quad C^n(\mu\nu,A) = C^n(\nu,A)C^n(\mu,A)$$

et

$$[(\mu\nu)^*] = [\nu^*][\mu^*] \;, \quad H^n(\mu\nu,A) = H^n(\nu,A)H^n(\mu,A) \quad .$$

De plus

$$C^n(1_G,A) = 1_{C^n(G,A)}$$
$$H^n(1_G,A) = 1_{H^n(G,A)}$$

Dém.: Immédiate.

Proposition 3.12. Soit A un G-module et soit

(34) $$1 \longrightarrow H \xrightarrow[i]{} G \xrightarrow[p]{} K \longrightarrow 1$$

une suite exacte courte de groupes. Alors la suite suivante de groupes abéliens est exacte :

(35) $$0 \longrightarrow H^1(K,A^H) \xrightarrow[{[p^*]}]{} H^1(G,A) \xrightarrow[{[i^*]}]{} H^1(H,A) \quad .$$

Dém.: Pas tout à fait triviale, mais pas trop difficile. Voir peut-être Serre: Corps locaux, p.125.

Réexaminons maintenant la proposition 2.3 pour A et B abéliens :

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \longrightarrow & X & \longrightarrow & G & \longrightarrow & 1 \qquad \varphi, m \\ & & \downarrow \lambda & & \downarrow \mu & & \downarrow \nu & & \\ 0 & \longrightarrow & B & \longrightarrow & Y & \longrightarrow & H & \longrightarrow & 1 \qquad \bar{\varphi}, \bar{m} \end{array}$$

Les conditions (2.28),(2.29) et (2.31) donnent

$$\lambda[(\varphi\alpha)a] = (\bar{\varphi}\nu\alpha)(\lambda a)$$

$$\lambda m(\alpha,\beta) = \bar{m}(\nu\alpha,\nu\beta) + u\alpha + (\bar{\varphi}\nu\alpha)(u\beta) - u(\alpha\beta) \quad .$$

La première relation dit que λ est un homomorphisme de G-modules, G opérant sur B par l'intermédiaire de ν.

Dans la deuxième relation, il faut remarquer d'abord que

$$u\alpha + (\bar{\varphi}\nu\alpha)(u\beta) - u(\alpha\beta) = (d_1 u)(\alpha,\beta) \quad .$$

En utilisant les homomorphismes induits, on peut donc écrire

$$(\lambda_* m)(\alpha,\beta) = (\nu^* \bar{m})(\alpha,\beta) + (d_1 u)(\alpha,\beta)$$

ou

$$\lambda_* m = \nu^* \bar{m} + d_1 u \in Z^2(G,B) \quad .$$

Passant aux classes de cohomologie, on obtient

$$[\lambda_*][m] = [\nu^*][\bar{m}] \in H^2(G,B) \quad .$$

3.5 Modules à cohomologie nulle

Ces modules ont une grande importance tant du point de vue pratique que pour les fondements de la théorie. Nous allons étudier quelques cas intéressants.

3.5.1 Modules coinduits

Soit X un G-module. Considérons le groupe abélien $C^1(G,X)$. Nous lui donnons la structure d'un G-module en définissant

(36) $$\forall\alpha,\beta \in G,\ \forall f \in C^1(G,X) \quad (\beta f)(\alpha) = f(\alpha\beta) \quad .$$

En effet

$$[\beta(f+g)](\alpha) = (f+g)(\alpha\beta) = f(\alpha\beta) + g(\alpha\beta) = (\beta f)(\alpha) + (\beta g)(\alpha)$$

et

$$[(\beta\gamma)f](\alpha) = f(\alpha\beta\gamma) = (\gamma f)(\alpha\beta) = [\beta(\gamma f)](\alpha) \quad .$$

D Un G-module A est dit <u>coinduit</u> s'il existe un G-module X tel que

$$A \approx C^1(G,X) \quad .$$

Nous allons montrer que chaque G-module A est isomorphe à un G-sous-module d'un G-module coinduit et que $H^n(G,M) = 0$ pour $n > 0$ et M coinduit.

<u>Proposition 3.13</u>. Chaque G-module A est isomorphe à un sous-module d'un G-module coinduit M.

<u>Dém.</u>: Prenons

(37) $$M = C^1(G,A) =: \hat{A}$$

et considérons l'application

$$\chi : A \longrightarrow \hat{A}$$

définie par

(38) $$\forall a \in A,\ \forall\alpha \in G \qquad (\chi a)(\alpha) = \alpha a \quad .$$

C'est un homomorphisme de groupes abéliens, puisque

$$[\chi(a+b)](\alpha) = \alpha(a+b) = \alpha a+\alpha b = (\chi a)(\alpha) + (\chi b)(\alpha)$$
$$= (\chi a+\chi b)(\alpha) \quad .$$

C'est aussi un homomorphisme de G-modules :

$$[\chi(\beta a)](\alpha) = \alpha(\beta a) = (\alpha\beta)a = (\chi a)(\alpha\beta) = [\beta(\chi a)](\alpha) \quad ;$$

c'est même une injection

$$(\chi a)(1) = a = 0 \quad . //$$

Soit

$f \in C^n(G,M)$

où M est coinduit, i.e. tel qu'il existe un G-module X et un isomorphisme $j : M \rightarrowtail\!\!\twoheadrightarrow C^1(G,X)$. Alors

$jf(\alpha_1,\dots,\alpha_n) \in C^1(G,X)$

de sorte que

$[jf(\alpha_1,\dots,\alpha_n)](\alpha_o) \in X \quad .$

Nous écrivons

(39) $$[jf(\alpha_1,\dots,\alpha_n)](\alpha_o) = \bar{f}(\alpha_o,\dots,\alpha_n) \quad .$$

Ainsi $\bar{f}$ est une cochaine <u>particulière</u> de $C^{n+1}(G,X)$. On peut vérifier facilement que $\bar{f} + \bar{g} = \overline{f + g}$. Considérons maintenant la différentielle d_n: $C^n(G,M) \longrightarrow C^{n+1}(G,M)$; on a

$$(\overline{d_n f})(\alpha_o,\dots,\alpha_{n+1}) = [j(d_n f)(\alpha_1,\dots,\alpha_{n+1})](\alpha_o)$$
$$= [j\{(-1)^{n+1}\sum_{i=o}^{n+1}(-1)^i(p^i_{n+1}f)(\alpha_1,\dots,\alpha_{n+1})\}](\alpha_o)$$
$$= [(-1)^{n+1}\sum_{i=o}^{n+1}(-1)^i\{j(p^i_{n+1}f)(\alpha_1,\dots,\alpha_{n+1})\}](\alpha_o)$$
$$= (-1)^{n+1}\sum_{i=o}^{n+1}(-1)^i\{[j(p^i_{n+1}f)(\alpha_1,\dots,\alpha_{n+1})](\alpha_o)\} \quad .$$

Examinons cela terme par terme. Pour $i = 0$ on trouve

$$[j(p^{o}_{n+1}f)(\alpha_1,\dots,\alpha_{n+1})](\alpha_o) = [j\{\alpha_1 f(\alpha_2,\dots,\alpha_{n+1})\}](\alpha_o)$$

$$= [\alpha_1\{jf(\alpha_2,\dots,\alpha_{n+1})\}](\alpha_o) = \{jf(\alpha_2,\dots,\alpha_{n+1})\}(\alpha_o\alpha_1)$$

$$= \overline{f}(\alpha_o\alpha_1,\alpha_2,\dots,\alpha_{n+1}) \quad .$$

Pour $0<i<n+1$ on a :

$$[j(p^{i}_{n+1}f)(\alpha_1,\dots,\alpha_{n+1})](\alpha_o) = [jf(\alpha_1,\dots,\alpha_i\alpha_{i+1},\dots,\alpha_{n+1})](\alpha_o)$$

$$= \overline{f}(\alpha_o,\alpha_1,\dots,\alpha_i\alpha_{i+1},\dots,\alpha_{n+1}) \quad .$$

Enfin

$$[j(p^{n+1}_{n+1}f)(\alpha_1,\dots,\alpha_{n+1})](\alpha_o) = [jf(\alpha_1,\dots,\alpha_n)](\alpha_o)$$

$$= \overline{f}(\alpha_o,\alpha_1,\dots,\alpha_n) \quad .$$

Ainsi

$$(\overline{d_n f})(\alpha_o,\alpha_1,\dots,\alpha_{n+1}) = (-1)^{n+1}\sum_{i=o}^{n}(-1)^i\overline{f}(\alpha_o,\dots,\alpha_i\alpha_{i+1},\dots,\alpha_{n+1})$$

$$+ \overline{f}(\alpha_o,\alpha_1,\dots,\alpha_n) \quad .$$

<u>Proposition 3.14</u>. Soit M un G-module coinduit. Alors

$$H^n(G,M) = 0 \qquad (n>0) \quad .$$

<u>Dém.</u>: Introduisons les homomorphismes de groupes abéliens

(40) $$S_{n+1}: C^{n+1}(G,M) \longrightarrow C^n(G,M)$$

par la définition suivante

$$(\overline{S_{n+1}f})(\alpha_o,\dots,\alpha_n) = (-1)^{n+1}\overline{f}(1,\alpha_o,\dots,\alpha_n) \quad ;$$

en vertu de (39) cela équivaut à

$$[j(S_{n+1}f)(\alpha_1,\dots,\alpha_n)](\alpha_o) = (-1)^{n+1}\{j[f(\alpha_o,\dots,\alpha_n)](1)\}$$

Calculons d'abord

$$C^n(G,M) \xrightarrow{d_n} C^{n+1}(G,M) \xrightarrow{S_{n+1}} C^n(G,M) \qquad (n\geq 0) \quad .$$

Nous trouvons

$$[\overline{S_{n+1}(d_n f)}](\alpha_o,\ldots,\alpha_n) = (-1)^{n+1}\overline{(d_n f)}(1,\alpha_o,\ldots,\alpha_n)$$

$$= \bar{f}(\alpha_o,\ldots,\alpha_n) - \sum_{i=o}^{n-1}(-1)^i \bar{f}\,(1,\alpha_o,\ldots,\alpha_i\alpha_{i+1},\ldots,\alpha_n)$$

$$+ (-1)^{n+1}\bar{f}(1,\alpha_o,\ldots,\alpha_{n-1}) \quad .$$

Examinons

$$C^n(G,M) \xrightarrow{S_n} C^{n-1}(G,M) \xrightarrow{d_{n-1}} C^n(G,M) \qquad (n\geq 1) \quad .$$

Il vient

$$[\overline{d_{n-1}(S_n f)}](\alpha_o,\ldots,\alpha_n)$$

$$= (-1)^n \sum_{i=o}^{n-1}(-1)^i(\overline{S_n f})(\alpha_o,\ldots,\alpha_i\alpha_{i+1},\ldots,\alpha_n)$$

$$+ (\overline{S f})(\alpha_o,\alpha_1,\ldots,\alpha_{n-1})$$

$$= \sum_{i=o}^{n-1}(-1)^i\bar{f}(1,\alpha_o,\ldots,\alpha_i\alpha_{i+1},\ldots,\alpha_n)$$

$$+ (-1)^n\bar{f}(1,\alpha_o,\ldots,\alpha_{n-1}) \quad .$$

Ainsi, on obtient

$$[\overline{S_{n+1}(d_n f)} + \overline{d_{n-1}(S_n f)}](\alpha_o,\ldots,\alpha_n) = \bar{f}(\alpha_o,\ldots,\alpha_n)$$

ou

$$S_{n+1} d_n f + d_{n-1}S_n f = f \in C^n(G,M)$$

ou encore

(41) $$S_{n+1}d_n + d_{n-1}S_n = 1_{C^n(G,M)} \quad .$$

Ces formules impliquent que tout n-cocycle est un n-cobord. En effet, soit $f \in Z^n(G,M)$, i.e. $d_n f = 0$. Alors

$$d_{n-1}(S_n f) = f$$

i.e. $f \in B^n(G,M)$. Mais cela veut dire précisément

$$H^n(G,M) = 0 \quad . \; //$$

3.5.2 Autres cas de cohomologie nulle

Soit G un groupe et $H \triangleleft G$ un sous-groupe normal fini d'ordre h. Soit A un G-module. L'application

$$N_H : A \longrightarrow A$$

définie par

(42) $$N_H : a \longmapsto \sum_{\alpha\in H} \alpha a$$

est évidemment un homomorphisme de groupes abéliens. C'est aussi un homomorphisme de G-modules. En effet, pour tout $\beta \in G$

$$N_H(\beta a) = \sum_{\alpha\in H} \alpha(\beta a) = \sum_{\alpha\in H} \beta\beta^{-1}\alpha\beta a$$

$$= \beta \sum_{\alpha'\in H} \alpha' a = \beta(N_H a) \quad .$$

Une autre propriété dont nous aurons besoin est le fait que pour tout $a \in A$, l'élément $N_H a$ est un élément qui est fixe sous l'action de H :

$$\forall \chi \in H \qquad \chi N_H a = \sum_{\alpha\in H} \chi\alpha a = N_H a \quad .$$

Exprimé autrement

(43) $$N_H A \subset A^H \quad .$$

Considérons l'homomorphisme induit

(44) $$[N_H^n] : H^n(G,A) \longrightarrow H^n(G,A)$$

<u>Proposition 3.15</u>. Pour tout G-module A on a

(45) $$[N_H^n] = h1_{H^n(G,A)} \quad .$$

<u>Dém.</u>: La démonstration sera faite par induction sur n. Pour n=0, la propriété (45) est trivialement satisfaite puisque $H^o(G,A) = A^G$, le sous-module des éléments de H

laissés invariants par tout $\alpha \in G$. Supposons alors que (45) est vrai pour n-1 et insérons A dans un G-module coinduit M. Considérons le diagramme commutatif ci-dessous :

$$\begin{tikzcd}
0 \arrow[r] & A \arrow[r] \arrow[d, "N_H"'] & M \arrow[r] \arrow[d, "N_H"] & \bar{A} \arrow[r] \arrow[d, "N_H"] & 0 \\
0 \arrow[r] & A \arrow[r] & M \arrow[r] & \bar{A} \arrow[r] & 0
\end{tikzcd}$$

Il donne lieu au diagramme commutatif suivant

$$\begin{tikzcd}
{} \arrow[r] & H^{n-1}(G,M) \arrow[r] & H^{n-1}(G,\bar{A}) \arrow[r, "\partial_{n-1}"] \arrow[d, "{[N_H^{n-1}]}"'] & H^n(G,A) \arrow[r] \arrow[d, "{[N_H^n]}"'] & H^n(G,M) \arrow[r] \arrow[d, "{[N_H^n]}"] & {} \\
{} \arrow[r] & H^{n-1}(G,M) \arrow[r] & H^{n-1}(G,\bar{A}) \arrow[r, "\partial_{n-1}"'] & H^n(G,A) \arrow[r] & H^n(G,M) \arrow[r] & {}
\end{tikzcd}$$

Puisque M est coinduit les homomorphismes de connection sont des isomorphismes et la commutativité donne pour but $\bar{a} \in H^{n-1}(G,\bar{A})$

$$[N_H^n]\partial_{n-1}\bar{a} = \partial_{n-1}[N_H^{n-1}]\bar{a} = \partial_{n-1}h\bar{a} = h\partial_{n-1}\bar{a} \quad .$$

L'élément $\partial_{n-1}\bar{a} \in H^n(G,A)$ étant générique, (45) est démontré. //

<u>Proposition 3.16</u>. Si

(46) $\forall a \in A \qquad N_H a = 0$

alors l'ordre de chaque élément de $H^n(G,A)$ est un diviseur de l'ordre h de $H \triangleleft G$:

(47) $hH^n(G,A) = 0 \quad .$

<u>Dém.</u>: La condition (46) équivaut à

$$N_H = 0 \quad .$$

Alors, on a aussi

$$[N_H^n] = 0$$

et en vertu de (45)

(48) $h1_{H^n(G,A)} = 0$

ce qui équivaut à (47). //

Proposition 3.17. Si, en plus de la condition (46), A, comme groupe abélien, est divisible et sans torsion, alors

$$H^n(G,A) = 0 \quad .$$

Dém.: Par hypothèse

$$\forall [f] \in H^n(G,A) \qquad h[f] = 0 \quad ,$$

i.e.

$$hf = d_{n-1}k \in B^n(G,A) \quad .$$

Mais puisque A est divisible,

$$k(\alpha_1,\ldots,\alpha_{n-1}) = h[\bar{k}(\alpha_1,\ldots,\alpha_{n-1})] =: (h\bar{k})(\alpha_1,\ldots,\alpha_{n-1})$$

Ainsi

$$hf = d_{n-1}h\bar{k} = h(d_{n-1}\bar{k})$$

et puisque A est sans torsion (i.e. n'a pas d'éléments d'ordre fini) on conclut que

(49) $$f = d_{n-1}\bar{k} \quad ;$$

ainsi chaque cocycle est un cobord. //

Proposition 3.18. Soit G un groupe et A un G-module. Soit H un sous-groupe normal fini d'ordre h tel que le seul élément de A laissé invariant par H soit $0 \in A$. Alors

$$hH^n(G,A) = 0 \qquad n>0 \quad .$$

Dém.: L'hypothèse que le seul élément de A laissé invariant est l'élément zéro équivaut à

$$N_H A \subset A^H = 0 \quad .$$

Les conditions de la proposition 3.16 sont donc remplies. //

Considérons maintenant un groupe fini G.

Proposition 3.19. Soit G un groupe fini d'ordre g et A un G-module. Alors, pour n>0, l'ordre de chaque élément de

$H^n(G,A)$ divise g :

(50) $$gH^n(G,A) = 0 \qquad (n>0) \qquad .$$

<u>Dém.</u>: Comme dans la démonstration de la proposition 3.14, nous introduisons une application

$$s_{n+1} : C^{n+1}(G,A) \longrightarrow C^n(G,A)$$

que nous définissons ici par

(51) $$(s_{n+1}f)(\alpha_1,\ldots,\alpha_n) = (-1)^{n+1}\sum_{\alpha\in G} f(\alpha_1,\ldots,\alpha_n,\alpha) \qquad .$$

L'idée de sommation sur les éléments d'un groupe fini remonte à la preuve, par Schur (1905), du théorème de Maschke (1899). La même idée a été utilisée par Frobenius (1911) dans son travail sur les groupes d'espace. (Cette idée a donné lieu à plusieurs généralisations ultérieures.) Calculons maintenant $s_{n+1}(d_nf)$

$$[s_{n+1}(d_nf)](\alpha_1,\ldots,\alpha_n) = (-1)^{n+1}\sum_{\alpha}(d_nf)(\alpha_1,\ldots,\alpha_n,\alpha)$$

$$= \sum_{\alpha}\Big[\alpha_1 f(\alpha_2,\ldots,\alpha_n,\alpha) + \sum_{i=1}^{n-1}(-1)^i f(\alpha_1,\ldots,\alpha_i\alpha_{i+1},\ldots,\alpha_n,\alpha)$$

$$+ (-1)^n f(\alpha_1,\ldots,\alpha_{n-1},\alpha_n\alpha) + (-1)^{n+1} f(\alpha_1,\ldots,\alpha_n)\Big]$$

$$= \alpha_1\sum_{\alpha} f(\alpha_2,\ldots,\alpha_n,\alpha) + \sum_{i=1}^{n-1}(-1)^i\sum_{\alpha} f(\alpha_1,\ldots,\alpha_i\alpha_{i+1},\ldots,\alpha_n\alpha)$$

$$+ (-1)^n\sum_{\alpha} f(\alpha_1,\ldots,\alpha_{n-1},\alpha_n\alpha) + (-1)^{n+1} g f(\alpha_1,\ldots,\alpha_n)$$

$$= (-1)^n\alpha_1(s_nf)(\alpha_2,\ldots,\alpha_n) + (-1)^n\sum_{i=1}^{n-1}(-1)^i(s_nf)(\alpha_1,\ldots,\alpha_i\alpha_{i+1},\ldots,\alpha_n)$$

$$+ (s_nf)(\alpha_1,\ldots,\alpha_{n-1}) + (-1)^{n+1} g f(\alpha_1,\ldots,\alpha_n)$$

$$= d_{n-1}(s_nf)(\alpha_1,\ldots,\alpha_n) + (-1)^{n+1} g f(\alpha_1,\ldots,\alpha_n) \qquad .$$

Ainsi

(52) $$\forall f \in C^n(G,A) \quad (s_{n+1}d_n - d_{n-1}s_n)f = (-1)^{n+1}gf \quad .$$

Supposons

$$f \in Z^n(G,A) \quad .$$

Alors (52) donne

$$(d_{n-1}s_n)f = (-1)^n gf$$

ou

(53) $$gf = d_{n-1}((-1)^n s_n f)$$

ce qui équivaut à (50).//

<u>Proposition 3.20</u>. Si G est un groupe fini et A, comme groupe abélien, est divisible et sans torsion, alors

$$H^n(G,A) = 0 \quad .$$

<u>Dém.</u>: On procède comme dans la démonstration de la proposition 3.17.

L'idée de sommation sur un groupe fini peut être étendue à l'intégration sur un groupe compact. Soit donc G un groupe topologique compact et A un bimodule: un espace vectoriel fini sur les réels R (ou les complexes C) et aussi un G-module. Alors

$$\forall \alpha \in G, \quad \forall r \in R, \quad \forall a \in A, \quad \alpha(ra) = r(\alpha a)$$

i.e. les éléments de G agissent comme transformations linéaires de A et sont donc des transformations continues. Considérons maintenant des <u>cochaînes continues</u> $f \in C^n_c(G,A)$ et des applications

$$s_{n+1} : \quad C_c^{n+1}(G,A) \longrightarrow C_c^n(G,A)$$

par l'intégrale de Haar

(54) $$(s_{n+1}f)(\alpha_1,\ldots,\alpha_n) = (-1)^{n+1}\int f(\alpha_1,\ldots,\alpha_n,\alpha)d\alpha \quad .$$

(L'intégrale se calcule par composantes, après le choix d'une base pour A.) Remarquons que les $d_n f$ aussi sont maintenant des fonctions continues. En procédant maintenant comme dans la démonstration de la proposition 3.19 et en utilisant la linéarité et invariance (à gauche) de l'intégrale de Haar, on démontre d'abord

(55) $$s_{n+1}d_n - d_{n-1}s_n = (-1)^{n+1} 1_{C_c^n(G,A)} \quad .$$

En appliquant cela à un $f \in Z_c^n(G,A)$ on trouve

(56) $$d_{n-1}((-1)^n s_n f) = f \quad .$$

On a ainsi démontré la proposition suivante.

<u>Proposition 3.21</u>. Soit G un groupe topologique compact et A un espace vectoriel fini, réel ou complexe, sur lequel G opère linéairement. Alors

(57) $$H_c^n(G,A) = 0 \qquad n>0 \quad .$$

4 Le foncteur cohomologique

Nous avons introduit les groupes de cohomologie; nous avons étudié plusieurs de leurs propriétés et donné quelques interprétations pour ces groupes en dimensions 0, 1, 2 et 3. Il s'agit de savoir maintenant ce qui est essentiel et ce qui est accidentel dans tout ce que nous avons fait. La construction des cochaînes que nous avons utilisés est très adaptée à la discussion de la théorie des extensions de groupes abéliens. On pourrait imaginer d'autres constructions, inspirées par d'autres préoccupations mathématiques permettant de définir des groupes de cohomologie. Dans quelle mesure ces groupes dépendent-ils des constructions utilisées ? Dans quelles conditions le résultat est-il indépendant des pas intermédiaires ?

La discussion sur ces questions sera pour nous aussi l'occasion de faire un pas de plus dans la théorie des catégories. Nous avons déjà défini la notion de catégorie et nous avons donné des exemples de catégories. Le pas suivant est d'introduire une sorte d'application entre catégories.

4.1 Foncteurs

D Soient C et $\overline{C}$ deux catégories. Un <u>foncteur covariant</u>

$F : C \longrightarrow \overline{C}$

consiste en deux applications (que nous désignerons par la même lettre F), une application qui à chaque objet $A \in \mathrm{Ob}C$ fait correspondre un objet $F(A) \in \mathrm{Ob}\overline{C}$ et une application qui à chaque morphisme $f \in \mathrm{Mor}(A,B)$ entre deux objets de C fait correspondre un morphisme $F(f) \in \mathrm{Mor}(F(A),F(B))$ entre les objets correspondants de la catégorie $\overline{C}$. Ces applications doivent satisfaire aux deux conditions suivantes :

FON 1 :

$\forall A \in Ob(C) \qquad F(1_A) = 1_{F(A)}$.

FON 2_*: Pour tout morphisme composé gf défini dans la catégorie C

$F(gf) = F(g)F(f)$.

A l'aide de diagrammes un foncteur covariant peut être caractérisé ainsi

$$\begin{tikzcd} A \arrow[loop left, "1_A"] \arrow[rr, "f"] \arrow[dr, "gf"'] & & B \arrow[dl, "g"] \\ & C & \end{tikzcd} \xrightarrow{\quad F \quad} \begin{tikzcd} F(A) \arrow[loop left, "1_{F(A)}"] \arrow[rr, "F(f)"] \arrow[dr, "F(gf)"'] & & F(B) \arrow[dl, "F(g)"] \\ & F(C) & \end{tikzcd}$$

D Un <u>foncteur contravariant</u> F est caractérisé par les diagrammes suivants

$$\begin{tikzcd} A \arrow[rr, "f"] \arrow[dr, "gf"'] & & B \arrow[dl, "g"] \\ & C & \end{tikzcd} \xrightarrow{\quad F \quad} \begin{tikzcd} F(A) & & F(B) \arrow[ll, "F(f)"'] \\ & F(C) \arrow[ul, "F(gf)"] \arrow[ur, "F(g)"'] & \end{tikzcd}$$

i.e. la condition FON 2_* est remplacée par

FON 2^* : $F(gf) = F(f)F(g)$.

Nous avons déjà rencontré des foncteurs. Considérons en effet $H^n(G,A)$ avec G fixe et A variable. Notons cela par $H^n(G,-)$. Nous avons vu que $H^n(G,-)$ fait correspondre à chaque G-module A un groupe abélien $H^n(G,A)$ et à chaque homomorphisme

$f : A \longrightarrow B$

de G-modules un homomorphisme

$H^n(G,f) : H^n(G,A) \longrightarrow H^n(G,B)$

de groupes abéliens. De plus, pour tout homomorphisme composé, fg, de G-modules on a

$$H^n(G,fg) = H^n(G,f)H^n(G,g)$$

et pour chaque G-module A on trouve

$$H^n(G,1_A) = 1_{H^n(G,A)} \quad .$$

Ainsi, pour $n \geq 0$, $H^n(G,-)$ est un foncteur covariant de la catégorie $\mathcal{M}_G$ des G-modules à la catégorie $\mathcal{A}$ des groupes abéliens.

Si, en revanche, on fixe d'une part un G_o-module A et l'on considère d'autre part la catégorie $\mathcal{G}_o$ des groupes G dont l'image homomorphe est dans G_o, alors $H^n(-,A)$ est un <u>foncteur</u>
D <u>contravariant</u> de la catégorie $\mathcal{G}_o$ dans la catégorie des groupes abéliens $\mathcal{A}$. Les éléments de $\mathcal{G}_o$ sont les homomorphismes de groupe avec codomaine G_o

$$G \longrightarrow G_o \quad .$$

Les morphismes sont des homomorphismes de groupe $\mu: G \longrightarrow H$ tels que le diagramme

$$\begin{tikzcd} G \arrow[dr] \arrow[dd, "\mu"'] & \\ & G_o \\ H \arrow[ur] & \end{tikzcd}$$

est commutatif. A un tel homomorphisme correspond

$$H^n(\lambda,A) : \quad H^n(H,A) \longrightarrow H^n(G,A)$$

et pour tout homomorphisme de groupes $\mu\lambda$ on a

$$H^n(\mu\lambda,A) = H^n(\lambda,A)H^n(\mu,A) \quad .$$

Cela suggère l'introduction des notions de

D **catégorie produit** et de **bifoncteur**. Au lieu de définir ces notions formellement, décrivons le foncteur $H^n(-,-)$. On dira que $H^n(-,-)$ est un bifoncteur de la catégorie produit $\mathbf{G}_o \times \mathbf{A}$ à la catégorie $\mathbf{A}$; ce foncteur est contravariant dans la première variable et covariant dans la deuxième. Les objets de $\mathbf{G}_o \times \mathbf{A}$ sont des paires (G,A) avec $G \in Ob(\mathbf{G}_o)$ et $A \in Ob(\mathbf{A})$. Les morphismes de $\mathbf{G}_o \times \mathbf{A}$ sont des paires (λ,f) où λ est un morphisme de $\mathbf{G}_o$ et f un morphisme de $\mathbf{A}$. Si l'on a les deux diagrammes respectivement dans $\mathbf{G}_o$ et $\mathbf{A}$

$$\begin{tikzcd} K \arrow[rr, "\mu"] \arrow[dr] & & H \arrow[dl, "\lambda"] \\ & G & \end{tikzcd} \qquad\qquad \begin{tikzcd} A \arrow[rr, "f"] \arrow[dr] & & B \arrow[dl, "g"] \\ & C & \end{tikzcd} ,$$

dans $\mathbf{G}_o$ dans $\mathbf{A}$

il leur correspond le diagramme suivant dans $\underset{\circ}{G}\times A$

$$\begin{tikzcd}
(K,A) \arrow[rr, "{(\mu,f)}"] \arrow[dr, "{(\mu\lambda,gf)}"'] & & (H,B) \arrow[dl, "{(\lambda,g)}"] \\
& (G,C) &
\end{tikzcd} \quad .$$

Le foncteur $H^n(-,-)$ fait correspondre à chaque objet (G,H) de $\underset{\circ}{G}\times A$ un objet de A: le groupe abélien $H^n(G,A)$. A chaque morphisme (μ,f) de $\underset{\circ}{G}\times A$ il fait correspondre le morphisme $H^n(\mu,f)$ de A. Ces morphismes de A correspondent à la règle

$$H^n(\mu\lambda,gf) = H^n(\lambda,g)H^n(\mu,f)$$

illustrée par le diagramme suivant

$$\begin{tikzcd}
H^n(K,A) \arrow[rr, "{H^n(\mu,f)}"] \arrow[dr, "{H^n(\mu\lambda,gf)}"'] & & H^n(H,B) \arrow[dl, "{H^n(\lambda,g)}"] \\
& H^n(G,C) &
\end{tikzcd}$$

De plus, on trouve

$$H^n(\mu,f) = H^n(\mu,1_B)H^n(1_K,f) = H^n(1_H,f)H^n(\mu,1_A)$$

i.e. le diagramme ci-dessous est commutatif :

$$\begin{tikzcd}
H^n(K,A) \arrow[r, "{H^n(1_K,f)}"] \arrow[d, "{H^n(\mu,1_A)}"'] \arrow[dr, "{H^n(\mu,f)}"] & H^n(K,B) \arrow[d, "{H^n(\mu,1_B)}"] \\
H^n(H,A) \arrow[r, "{H^n(1_H,f)}"'] & H^n(H,B)
\end{tikzcd}$$

On remarque aussi que l'on peut identifier le morphisme $H^n(1_K,f)$ de A correspondant au morphisme $(1_K,f)$ de $\underset{\circ}{G}\times A$ et le morphisme $H^n(K,f)$ de A correspondant au morphisme f de $\mathcal{M}_G$

$$H^n(K,f) = H^n(1_K,f) \quad .$$

De même

$$H^n(\mu,B) = H^n(\mu,1_B) \quad .$$

<u>Exercice 4.a.</u> Donner la définition de catégorie produit et de bifoncteur deux fois covariant .

Un autre exemple de bifoncteur est le foncteur Hom. Soient A et B deux G-modules. Désignons par $\mathrm{Hom}_G(A,B)$ l'ensemble des homomorphismes du G-module A dans le G-module B. D'une façon naturelle on peut lui donner la structure d'un groupe abélien et on peut voir alors que $\mathrm{Hom}_G(-,-)$ est un bifoncteur (contravariant dans la première variable et covariant dans la seconde variable) de la catégorie produit $\mathcal{M}_G \times \mathcal{M}_G$ (des paires de G-modules) à la catégorie $\mathcal{A}$ des groupes abéliens.

<u>Proposition 4.1.</u> Soient

$$0 \longrightarrow A \xrightarrow[\alpha]{} B \xrightarrow[\beta]{} C \longrightarrow 0$$

et

$$0 \longrightarrow L \xrightarrow[\lambda]{} M \xrightarrow[\mu]{} N \longrightarrow 0$$

deux suites exactes de G-modules. Alors les deux suites ci-dessous sont exactes

(1) $$0 \longrightarrow \mathrm{Hom}(M,A) \xrightarrow[\mathrm{Hom}(M,\alpha)]{} \mathrm{Hom}(M,B) \xrightarrow[\mathrm{Hom}(M,\beta)]{} \mathrm{Hom}(M,C)$$

(2) $$0 \longrightarrow \mathrm{Hom}(N,B) \xrightarrow[\mathrm{Hom}(\mu,B)]{} \mathrm{Hom}(M,B) \xrightarrow[\mathrm{Hom}(\lambda,B)]{} \mathrm{Hom}(L,B)$$

Remarque: Nous avons partout écrit Hom au lieu de Hom_G.

<u>Dém.</u>: Rappelons d'abord la définition des applications qui interviennent. Soit

$$\alpha : A \longrightarrow B \quad ,$$

alors

$$\mathrm{Hom}(M,\alpha) : \mathrm{Hom}(M,A) \longrightarrow \mathrm{Hom}(M,B)$$

est défini par

$$\mathrm{Hom}(M,\alpha) : f \longmapsto \alpha f \qquad \begin{tikzcd} A \arrow[rr, "\alpha"] & & B \\ & M \arrow[ul, "f"] \arrow[ur, "\mathrm{Hom}(M,\alpha)f"'] & \end{tikzcd}$$

soit

$$\mu : M \longrightarrow N$$

alors

$$\mathrm{Hom}(\mu,A) : \mathrm{Hom}(N,A) \longrightarrow \mathrm{Hom}(M,A)$$

est défini par

$$\mathrm{Hom}(\mu,A) : g \longmapsto g\mu \qquad \begin{tikzcd} M \arrow[rr, "\mu"] \arrow[dr, "\mathrm{Hom}(\mu,A)g"'] & & N \arrow[dl, "g"] \\ & A & \end{tikzcd}$$

Enfin

$$\mathrm{Hom}(\mu,\alpha) : \mathrm{Hom}(N,A) \longrightarrow \mathrm{Hom}(M,B)$$

est défini par

$$\mathrm{Hom}(\mu,\alpha) : g \longmapsto \alpha g \mu \qquad \begin{tikzcd} & A \arrow[r, "\alpha"] & B \\ N \arrow[ur, "g"] & M \arrow[l, "\mu"] \arrow[ur, "\mathrm{Hom}(\mu,\alpha)g"'] & \end{tikzcd}$$

On voit que

$$\mathrm{Hom}(\mu,\alpha) = \mathrm{Hom}(M,\alpha)\mathrm{Hom}(\mu,A) = \mathrm{Hom}(\mu,B)\mathrm{Hom}(N,\alpha) \quad .$$

<u>Lemme</u>. Soient

$$0 \longrightarrow A \xrightarrow{\alpha} B$$

et

$$M \xrightarrow{\mu} N \longrightarrow 0$$

exactes, alors

$$0 \longrightarrow \mathrm{Hom}(N,A) \xrightarrow{\mathrm{Hom}(\mu,\alpha)} \mathrm{Hom}(M,B)$$

est exacte.

<u>Démonstration du lemme</u>. Prenons

$$g \in \mathrm{Hom}(N,A)$$

et supposons

$$\mathrm{Hom}(\mu,\alpha)g = \alpha g\mu = 0 \in \mathrm{Hom}(M,B)$$

i.e.

$$\forall m \in M \qquad \alpha g\mu m = 0 \in B \quad .$$

Puisque α est injectif,

$$g\mu m = 0 \in A \quad .$$

Mais, μ étant surjectif, μm est un élément général de N; ainsi

$$g = 0 \in \mathrm{Hom}(N,A) \quad . //$$

<u>Démonstration de la proposition</u> :

(i) Nous avons les relations

$$\mathrm{Hom}(M,\alpha) = \mathrm{Hom}(1_M,\alpha)$$

$$\mathrm{Hom}(\mu,B) = \mathrm{Hom}(\mu,1_B) \quad .$$

Puisque 1_M et μ sont des surjections, α et 1_B des injections, $\mathrm{Hom}(M,\alpha)$ et $\mathrm{Hom}(\mu,B)$ sont -- d'après le lemme -- des injections.

(ii) $\mathrm{Hom}(M,\beta)\mathrm{Hom}(M,\alpha) = \mathrm{Hom}(M,0) = 0$

$$\mathrm{Hom}(\lambda,B)\mathrm{Hom}(\mu,B) = \mathrm{Hom}(0,B) = 0 \quad .$$

Donc

$$\mathrm{Im}\ \mathrm{Hom}(M,\alpha) \subset \mathrm{Ker}\ \mathrm{Hom}(M,\beta)$$

$$\mathrm{Im}\ \mathrm{Hom}(\mu,B) \subset \mathrm{Ker}\ \mathrm{Hom}(\lambda,B) \quad .$$

(iii) Supposons

$$g \in \mathrm{Ker}\ \mathrm{Hom}(M,\beta) \subset \mathrm{Hom}(M,B) \quad .$$

Alors

$$\mathrm{Hom}(M,\beta)g = \beta g = 0 \in \mathrm{Hom}(M,C)$$

c'est-à-dire

$$\mathrm{Im} g \subset \mathrm{Ker}\ \beta = \mathrm{Im}\ \alpha, \subset B \quad .$$

Donc

$$\forall m \in M \qquad \exists a \in A \qquad gm = \alpha a \in B \qquad .$$

L'élément a est unique puisque α est injectif.

En restreignant le codomaine de g à Im α, on voit que g détermine un homomorphisme

$$h : M \longrightarrow A$$

$$h : m \longmapsto \alpha^{-1} gm$$

$$\begin{tikzcd} M \arrow[r, "g"] \arrow[dr, "h"'] & \operatorname{Im}\alpha \arrow[d, "\alpha^{-1}"] \\ & A \end{tikzcd}$$

Ainsi

$$g = \alpha h = \operatorname{Hom}(M,\alpha)h$$

ou

$$g \in \operatorname{Im} \operatorname{Hom}(M,\alpha) \qquad .$$

(iv) Soit

$$f \in \operatorname{Ker} \operatorname{Hom}(\lambda,B) \subset \operatorname{Hom}(M,B) \qquad .$$

Alors

$$\operatorname{Hom}(\lambda,B)f = f\lambda = 0 \in \operatorname{Hom}(L,B)$$

c'est-à-dire

$$f(\operatorname{Im} \lambda) = f(\operatorname{Ker} \mu) = 0$$

ou

$$\operatorname{Ker} \mu \subset \operatorname{Ker} f \subset M \qquad .$$

On a donc le diagramme

$$\begin{tikzcd} 0 \arrow[r] & \operatorname{Ker}\mu \arrow[r] \arrow[d, tail] & M \arrow[r] \arrow[d, equal] & M/\operatorname{Ker}\mu \arrow[r] \arrow[d, dashed, "f'"] & 0 \\ 0 \arrow[r] & \operatorname{Ker} f \arrow[r] & M \arrow[r, "f"'] & B & \end{tikzcd}$$

et il existe un unique

$$f' : M/\operatorname{Ker} \mu \longrightarrow B$$

qui rend le diagramme commutatif. Puisque μ est une surjection, nous avons un isomorphisme

$$s : N \twoheadrightarrow M/\mathrm{Ker}\,\mu$$

et le diagramme

$$\begin{tikzcd} N \arrow[r, two heads, "s"] & M/\mathrm{Ker}\,\mu \arrow[d, "f'"] \\ M \arrow[u, two heads, "\mu"] \arrow[r, "f"'] & B \end{tikzcd}$$

de sorte que

$$\mathrm{Hom}(\mu,B)f's = f's\mu = f$$

i.e.

$$f \in \mathrm{Im}\,\mathrm{Hom}(\mu,B) \qquad . //$$

Revenons à la cohomologie. Nous avons vu que $H^n(G,-)$ est un foncteur covariant de la catégorie $\mathcal{M}_G$ des G-modules dans la catégorie $\mathcal{A}$ des groupes abéliens. Les propositions 3.7, 3.8 et 3.9 nous montrent qu'à chaque suite exacte courte E de G-modules on peut faire correspondre une suite exacte H(E) de groupes abéliens, à chaque morphisme $\Lambda_1 : E_1 \longrightarrow E_2$ de suites exactes courtes de G-modules un morphisme $H(\Lambda_1)$ de suites exactes de groupes abéliens. Si, de plus, on a un deuxième morphisme $\Lambda_2 : E_2 \longrightarrow E_3$ on trouve $H(\Lambda_2\Lambda_1) = H(\Lambda_2)H(\Lambda_1)$. On a donc un foncteur H de la catégorie $\mathcal{K}_G$ des suites exactes courtes de G-modules dans la catégorie $\mathcal{L}$ des suites exactes (longues) de groupes abéliens

$$H : \mathcal{K}_G \longrightarrow \mathcal{L} \qquad .$$

On peut décrire la cohomologie d'une façon légèrement différente. D'abord, on a un foncteur $H^n(G,-)$ comme ci-dessus. Ensuite, on fait correspondre à chaque suite exacte courte de G-modules $0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$ un homomorphisme de groupes abéliens

$$\partial_n(E)\ :\quad H^n(G,C) \longrightarrow H^{n+1}(G,A)\quad .$$

Considérons $\partial_n(E)$ comme objet de la catégorie A^2 de morphismes de groupes abéliens. On peut voir que ∂_n est un foncteur de K à A^2. En effet, à chaque morphisme $\Lambda_1\ :\ E_1 \longrightarrow E_2$ dans K, i.e. à chaque diagramme commutatif

$$\begin{tikzcd} 0 \arrow[r] & A_1 \arrow[r] \arrow[d, "\alpha"] & B_1 \arrow[r] \arrow[d, "\beta"] & C_1 \arrow[r] \arrow[d, "\gamma"] & 0 & & E_1 \arrow[d, "\Lambda_1"] \\ 0 \arrow[r] & A_2 \arrow[r] & B_2 \arrow[r] & C_2 \arrow[r] & 0 & & E_2 \end{tikzcd}$$

correspond un morphisme $\partial_n(\Lambda_1)\ :\ \partial_n(E_1) \longrightarrow \partial_n(E_2)$, i.e. un diagramme commutatif

$$\begin{tikzcd} H^n(G,C_1) \arrow[r, "\partial_n(E_1)"] \arrow[d, "H^n(G,\gamma)"'] & H^{n+1}(G,A_1) \arrow[d, "H^n(G,\alpha)"] \\ H^n(G,C_2) \arrow[r, "\partial_n(E_2)"'] & H^{n+1}(G,A_2) \end{tikzcd}$$

(C'est le contenu de la Proposition 3.8). On peut aussi vérifier les autres propriétés fonctionnelles :

$$\partial_n(\Lambda_2\Lambda_1) = \partial_n(\Lambda_2)\partial_n(\Lambda_1)$$

et

$$\partial_n(1_E) = 1_{\partial_n(E)}\quad .$$

Pour caractériser complètement la cohomologie, il faut encore qu'à chaque suite exacte courte E_1 dans K corresponde une suite exacte longue de groupes abéliens $H(E_1)$:

$$\longrightarrow H^{n-1}(G,B) \longrightarrow H^{n-1}(G,C) \xrightarrow{\partial_n(E_1)} H^n(G,H) \longrightarrow H^n(G,B) \longrightarrow\quad .$$

Il nous reste encore à introduire une notion importante, celle de transformation naturelle entre deux foncteurs. Soient donc C et $\mathcal{D}$ deux catégories, S et T deux foncteurs de C à $\mathcal{D}$:

$$S,T\ :\ C \longrightarrow \mathcal{D}\quad .$$

D **Une transformation naturelle**

$$\eta : S \longrightarrow T$$

est une application qui associe à chaque $X \in Ob(C)$ un morphisme de $\mathcal{D}$

$$\eta_X : S(X) \longrightarrow T(X)$$

et cela de telle façon que, pour chaque morphisme

$$\lambda : X \longrightarrow Y$$

de C, le diagramme ci-dessous soit commutatif

(3)
$$\begin{array}{ccc} S(X) & \xrightarrow{\eta_X} & T(X) \\ {\scriptstyle S(\lambda)}\downarrow & & \downarrow{\scriptstyle T(\lambda)} \\ S(Y) & \xrightarrow[\eta_Y]{} & T(Y) \end{array}$$

Si pour tout $X \in Ob(C)$ le morphisme η_X est un isomorphisme,

D alors la transformation naturelle η est un <u>isomorphisme naturel.</u>

L'insertion χ d'un module A dans un module coinduit $\hat{A} = C^1(G,A)$, défini par la relation (3.38), peut être considérée comme transformation naturelle. Montrons d'abord la commutativité du diagramme

(4)
$$\begin{array}{ccc} A & \xrightarrow{\chi_A} & \hat{A} \\ {\scriptstyle \lambda}\downarrow & & \downarrow{\scriptstyle \lambda_*} \\ B & \xrightarrow[\chi_B]{} & \hat{B} \end{array}$$

où λ_* est défini par (3.18). On trouve

$$[(\lambda_*\chi_A)a](\alpha) = [\lambda_*(\chi_A a)](\alpha) = \lambda[(\chi_A a)\alpha] = \lambda[\alpha a]$$
$$= \alpha[\lambda a] = [\chi_B(\lambda a)](\alpha) \qquad .$$

Mais, d'après (3.20), nous avons $\lambda \in C^0(G,-)$ et $\lambda_* \in C^1(G,-)$.

Or $C^o(G,-)$ et $C^1(G,-)$ sont des foncteurs covariants de la catégorie des G-modules dans la catégorie des G-modules et on a

(4') $$\begin{tikzcd} C^o(G,A) \arrow[r, "\chi_A"] \arrow[d, "C^o(G,\lambda)"'] & C^1(G,A) \arrow[d, "C^1(G,\lambda)"] \\ C^o(G,B) \arrow[r, "\chi_B"'] & C^1(G,B) \end{tikzcd} .$$

Nous allons utiliser plus tard cette propriété.

4.2 L'unicité du foncteur cohomologique

Soit (pour $n \geqslant 0$) F^n un foncteur covariant de la catégorie $\mathcal{M}_G$ des G-modules à la catégorie $\mathcal{A}$ des groupes abéliens et soit ϕ_n un foncteur covariant de la catégorie $\mathcal{K}_G$ des suites exactes courtes de G-modules à la catégorie $\mathcal{A}^2$ des morphismes de groupes abéliens. Désignons par F la famille des F^n et par ϕ la famille des ϕ_n. La paire

D (F,ϕ) est appelée <u>foncteur cohomologique</u> si à chaque $E \in \mathrm{Ob}(\mathcal{K}_G)$

(5) $$E : \quad 0 \longrightarrow A \xrightarrow{i} B \xrightarrow{p} C \longrightarrow 0$$

correspond la suite exacte F(E) de G-modules

(6) $$F(E) : \longrightarrow F^n(B) \xrightarrow[F^n(p)]{} F^n(C) \xrightarrow[\phi_n(E)]{} F^{n+1}(A) \xrightarrow[F^{n+1}(i)]{} F^{n+1}(B) \longrightarrow$$

<u>Proposition 4.2</u>. Soit (F,ϕ) un foncteur cohomologique. Alors pour tout n il existe un et un seul foncteur F^n, satisfaisant aux deux conditions suivantes :

(7) (i) $\forall A \in \mathcal{M}_G \qquad F^o(A) = A^G$

(8) (ii) Pour tout $n > 0$ et tout <u>M coinduit</u> $F^n(M) = 0$.

<u>Dém.</u> : <u>Existence</u>. La paire (H,∂), avec $H^n = H^n(G,-)$, et $\partial_n = \partial_n(E)$ l'homomorphisme de connexion, est un tel foncteur. <u>Unicité</u>. Supposons maintenant que (D,Δ) et (F,ϕ) sont deux foncteurs cohomologiques qui satisfont à (7) et (8). Nous allons montrer d'abord que pour tout $n > 0$ et

(9) $$\forall A \in \mathcal{M}_G \qquad D^n(A) \approx F^n(A) \quad .$$

Pour $n = 0$ l'affirmation (7) est vraie par hypothèse puisque

$$\forall A \in \mathcal{M}_G \qquad D^o(A) = F^o(A) = A^G \quad .$$

Nous procédons maintenant par induction sur n. Considérons la suite exacte courte $E_A \in Ob(\mathcal{K}_G)$, où M est un G-module coinduit

$$E_A \qquad 0 \longrightarrow A \xrightarrow[\chi_A]{} M \longrightarrow \tilde{A} \longrightarrow 0 \quad .$$

Nous avons alors deux suites exactes $D(E_A)$ et $F(E_A)$

$$D(E_A) \qquad \longrightarrow D^n(M) \longrightarrow D^n(\tilde{A}) \longrightarrow D^{n+1}(A) \longrightarrow D^{n+1}(M) \longrightarrow$$

$$F(E_A) \qquad \longrightarrow F^n(M) \longrightarrow F^n(\tilde{A}) \longrightarrow F^{n+1}(A) \longrightarrow F^{n+1}(M) \longrightarrow .$$

Par hypothèse d'induction et la condition (8), nous pouvons construire le diagramme

(10)
$$\begin{tikzcd}
0 = D^n(M) \arrow[r] \arrow[d, equal, "\eta_n(M)"'] & D^n(\tilde{A}) \arrow[r, "\Delta_n(E_A)"] \arrow[d, "\eta_n(\tilde{A})"] & D^{n+1}(A) \arrow[r, "D^{n+1}(\chi_A)"] \arrow[d, dashed, "\eta_{n+1}(A)"] & D^{n+1}(M) = 0 \arrow[d, equal, "\eta_{n+1}(M)"] \\
0 = F^n(M) \arrow[r] & F^n(\tilde{A}) \arrow[r, "\phi_n(E_A)"'] & F^{n+1}(A) \arrow[r, "F^{n+1}(\chi_A)"'] & F^{n+1}(M) = 0
\end{tikzcd}$$

Ce diagramme définit un (unique) isomorphisme,

$$\eta_{n+1}(A) : \qquad D^{n+1}(A) \rightarrowtail\twoheadrightarrow F^{n+1}(A) \quad ,$$

précisément celui qui rend le diagramme commutatif.
Ainsi (9) est démontré et il reste à montrer que η_n est une transformation naturelle

$$\eta_n : \quad D^n \longrightarrow F^n$$

i.e. que pour $n \geq 0$ et pour chaque homomorphisme de

G-modules $\lambda : A \longrightarrow B$ le diagramme suivant est commutatif

$$\begin{tikzcd} D^n(A) \arrow[r, "\eta_n(A)"] \arrow[d, "D^n(\lambda)"'] & F^n(A) \arrow[d, "F^n(\lambda)"] \\ D^n(B) \arrow[r, "\eta_n(B)"'] & F^n(B) \end{tikzcd}$$

Pour n = 0 le diagramme est évidemment commutatif. Maintenant nous pouvons procéder de nouveau par induction sur n. Mais remarquons auparavant que la naturalité de l'insertion χ_A de A dans $\hat{A}$ (exprimée par la commutativité du diagramme (4)) nous permet de construire le diagramme commutatif suivant

$$(11)\qquad \begin{tikzcd} E_A & 0 \arrow[r] & A \arrow[r] \arrow[d, "\lambda"] & \hat{A} \arrow[r] \arrow[d, "\lambda_*"] & \tilde{A} \arrow[r] \arrow[d, "\tilde{\lambda}"] & 0 \\ E_B & 0 \arrow[r] & B \arrow[r] & \hat{B} \arrow[r] & \tilde{B} \arrow[r] & 0 \end{tikzcd} .$$

Alors, le fait que Δ_n et ϕ_n sont des foncteurs nous permet de conclure que le diagramme

$$(12)\qquad \begin{tikzcd} D^n(\tilde{A}) \arrow[r, tail, two heads, "\Delta_n(E_A)"] \arrow[d, "D^n(\tilde{\lambda})"'] & D^{n+1}(A) \arrow[d, "D^{n+1}(\lambda)"] \\ D^n(\tilde{B}) \arrow[r, tail, two heads, "\Delta_n(E_B)"'] & D^{n+1}(B) \end{tikzcd}$$

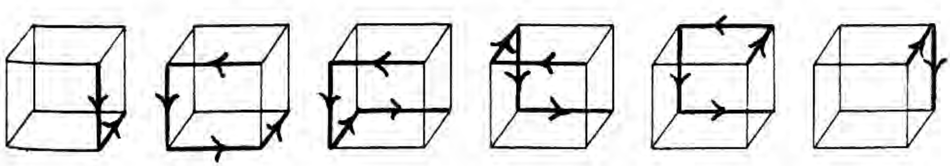
et le diagramme correspondant pour (F,ϕ) sont commutatifs. En vertu du diagramme (10) $\Delta_n(E_A)$ et $\Delta_n(E_B)$ sont des isomorphismes. Construisons alors le cube suivant

(13)

$$\begin{tikzcd}
 & F^n(\tilde{A}) \arrow[rr, tail, two heads, "\phi_n"] \arrow[dd, "F^n(\tilde{\lambda})"] & & F^{n+1}(A) \arrow[dd, "F^{n+1}(\lambda)"] \\
D^n(\tilde{A}) \arrow[ur, tail, "\eta_n"] \arrow[rr, tail, two heads, "\Delta_n"'] \arrow[dd, "D^n(\tilde{\lambda})"'] & & D^{n+1}(A) \arrow[ur, tail, "\eta_{n+1}"] \arrow[dd, "D^{n+1}(\lambda)"] & \\
 & F^n(\tilde{B}) \arrow[rr, tail, two heads, "\phi_n"] & & F^{n+1}(B) \\
D^n(\tilde{B}) \arrow[ur, tail, "\eta_n"] \arrow[rr, tail, two heads, "\Delta_n"'] & & D^{n+1}(B) \arrow[ur, tail, "\eta_{n+1}"'] &
\end{tikzcd}$$

Toutes les faces sont commutatives sauf peut-être celle qui nous intéresse, la face droite. On verra qu'alors cette face aussi doit être commutative. La face gauche (face D^n, F^n) est commutative par l'hypothèse d'induction. La commutativité des faces antérieures (D^n, D^{n+1}) et postérieures (F^n, F^{n+1}) exprime que Δ_n et ϕ_n sont des foncteurs, les faces supérieures ($\tilde{A}$,A) et inférieures sont commutatives en vertu de la définition des isomorphismes η. Notez que toutes les arêtes horizontales représentent des homomorphismes bijectifs et peuvent donc être parcourus dans les deux sens. On arrive à la conclusion que la face droite est commutative de la façon illustrée par la figure qui suit

4)



Ainsi l'unicité des F^n, à un isomorphisme naturel près, est démontrée. Mais un foncteur cohomologique (F,ϕ) consiste en deux familles de foncteurs: F et ϕ. Les foncteurs ϕ_n sont-ils aussi uniques modulo l'isomorphisme naturel (η_n,η_{n+1}) ? Soit $\Lambda\colon E \longrightarrow E'$ un morphisme de la catégorie $\mathcal{K}_G$:

$$\begin{tikzcd} E \arrow[d, "\Lambda"] \\ E' \end{tikzcd} \qquad \begin{tikzcd} 0 \arrow[r] & A \arrow[r] \arrow[d] & B \arrow[r] \arrow[d] & C \arrow[r] \arrow[d] & 0 \\ 0 \arrow[r] & A' \arrow[r] & B' \arrow[r] & C' \arrow[r] & 0 \end{tikzcd}$$

L'isomorphisme entre $\Delta_n(E)$ et $\phi_n(E)$ s'exprime par le diagramme commutatif

(15) $$\begin{tikzcd} D^n(C) \arrow[r, "\Delta_n(E)"] \arrow[d, "\eta_n(C)"'] & D^{n+1}(A) \arrow[d, "\eta_{n+1}(A)"] \\ F^n(C) \arrow[r, "\phi_n(E)"'] & F^{n+1}(A) \end{tikzcd}$$

La naturalité de l'isomorphisme s'exprime par la commutativité du cube ci-dessous dans lequel on trouve le diagramme (15) comme face devant et son analogue pour la suite exacte courte E' comme face derrière.

(16) $$\begin{tikzcd} & D^n(C') \arrow[rr, "\Delta_n(E')"] \arrow[dd] & & D^{n+1}(A') \arrow[dd, "\eta^{n+1}(A')"] \\ D^n(C) \arrow[ur] \arrow[rr, "\Delta^n(E)"] \arrow[dd, "\eta_n(C)"'] & & D^{n+1}(A) \arrow[ur] \arrow[dd] & \\ & F^n(C') \arrow[rr] & & F^{n+1}(A') \\ F^n(C) \arrow[ur] \arrow[rr, "\phi_n(E)"'] & & F^{n+1}(A) \arrow[ur] & \end{tikzcd}$$

Les faces dessous et dessus expriment que Δ_n et ϕ_n sont des foncteurs, tandis que les faces gauche et droite expriment la naturalité des isomorphismes η_n et η_{n+1}. Ainsi il suffit de démontrer l'existence d'un isomorphisme entre Δ_n et ϕ_n, la naturalité de cet isomorphisme suit alors automatiquement.

Pour démontrer cette existence, il nous faut utiliser

D la notion de module injectif. Un module J est <u>injectif</u> si chaque homomorphisme avec codomaine J peut être étendu, plus précisément chaque diagramme

$$\begin{tikzcd} 0 \arrow[r] & A \arrow[r, "\kappa"] \arrow[d] & B \\ & J & \end{tikzcd}$$

avec ligne horizontale exacte peut être complété en un diagramme commutatif :

(17)
$$\begin{tikzcd} 0 \arrow[r] & A \arrow[r, "\kappa"] \arrow[d] & B \arrow[dl] \\ & J & \end{tikzcd}$$

Il s'ensuit que chaque morphisme injectif $\kappa: J \rightarrowtail A$ de G-modules est une corétraction. En effet, on a le cas spécial de (17)

(18)
$$\begin{tikzcd} 0 \arrow[r] & J \arrow[r, "\kappa"] \arrow[d, equal, "1_J"'] & A \arrow[dl, "s"] \\ & J & \end{tikzcd} \qquad s\kappa = 1_J$$

Choisissons maintenant A coinduit (voir proposition 3.13) et appliquons le foncteur F^n. On trouve le diagramme

$$\begin{tikzcd} F^n(J) \arrow[r, "F^n(\kappa)"] \arrow[d, equal, "F^n(1_J)"'] & F^n(A)=0 \arrow[dl, "F^n(s)"] \\ F^n(J) & \end{tikzcd}$$

qui montre que

$$F^n(J) = 0$$

pour tout J injectif. Il nous faut connaître une autre propriété des modules injectifs.

<u>Proposition 4.3</u>. Chaque module est isomorphe à un sous-module d'un module injectif.

Soit maintenant une suite exacte de G-modules

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0 \quad .$$

Nous pouvons construire une autre suite

$$0 \longrightarrow A \longrightarrow J \longrightarrow A' \longrightarrow 0$$

avec J injectif. Ensuite, nous pouvons construire un diagramme commutatif

$$\begin{tikzcd}
0 \arrow[r] & A \arrow[r] \arrow[d, equal] & B \arrow[r] \arrow[d, "\beta"] & C \arrow[r] \arrow[d, "\gamma"] & 0 & & E \arrow[d, "A"] \\
0 \arrow[r] & A \arrow[r] & J \arrow[r] & A' \arrow[r] & 0 & & \bar{E}
\end{tikzcd} \tag{19}$$

ou $\beta : B \longrightarrow J$ est une conséquence de l'injectivité de J et on obtient γ en complétant le diagramme. Maintenant nous pouvons construire le cube suivant :

$$\begin{tikzcd}
& D^{n+1}(A) \arrow[rr, equal] \arrow[dd, "\eta_{n+1}(A)"] & & D^{n+1}(A) \arrow[dd, "\eta_{n+1}(A)"] \\
D^n(A') \arrow[ur, "\Delta_n(\bar{E})"] \arrow[dd, "\eta_n(A')"] & & D^n(C) \arrow[ll, "D^n(\gamma)"'] \arrow[ur, "\Delta_n(E)"'] \arrow[dd, "\eta_n(C)"] & \\
& F^{n+1}(A) \arrow[rr, equal] & & F^{n+1}(A) \\
F^n(A') \arrow[ur, "\Gamma_n(\bar{E})"] & & F^n(C) \arrow[ll, "F^n(\gamma)"] \arrow[ur, "\Gamma_n(E)"'] &
\end{tikzcd}$$

La face postérieure est commutative d'une façon triviale, la commutativité de la face antérieure exprime la naturalité de la transformation $\eta : D \longrightarrow F$. La commutativité des faces supérieures et inférieures exprime une propriété des foncteurs Δ_n et Γ_n, enfin la face gauche est commutative en vertu de la définition (10) de η. Ainsi, toutes les faces sauf peut-être la face droite sont commutatives et -- comme précédemment -- on peut montrer qu'elle aussi est alors commutative.

Nous avons ainsi démontré la proposition suivante - qui englobe la proposition 4.2.

<u>Proposition 4.4</u>. A un isomorphisme naturel près, il existe un et un seul foncteur cohomologique (F,ϕ) satisfaisant aux deux conditions suivantes :

(i) $\forall A \in M_G \qquad F^o(A) = A^G$

(ii) Pour tout $n>0$ et tout <u>M coinduit</u> $F^n(M) = 0$.

Remarquons que de notre définition du foncteur cohomologique, il suit qu'au lieu de (F,ϕ) on peut considérer un foncteur $\hat{F}$ de la catégorie K_G des suites exactes courtes de G-modules à la catégorie L des suites exactes de groupes abéliens. La question qui vient alors à l'esprit est la suivante: les deux suites exactes $\hat{F}(E)$ et $\hat{D}(E)$ -- qui correspondent à deux foncteurs cohomologiques satisfaisant à (7) et (8) -- sont-elles isomorphes ? i.e. le diagramme ci-dessous est-il commutatif ?

(20)
$$\begin{array}{ccccccccc}
\hat{D}(E) & & \longrightarrow D^n(C) & \xrightarrow{\Delta_n(E)} & D^{n+1}(A) & \longrightarrow & D^{n+1}(B) & \longrightarrow \\
\downarrow{\scriptstyle\eta} & & \downarrow{\scriptstyle\eta_n(C)} & & \downarrow{\scriptstyle\eta_{n+1}(A)} & & \downarrow & \\
\hat{F}(E) & & \longrightarrow F^n(C) & \xrightarrow[\phi_n(E)]{} & F^{n+1}(A) & \longrightarrow & F^{n+1}(B) & \longrightarrow
\end{array}$$

Autre question, la transformation

$$\eta : \hat{D} \longrightarrow \hat{F}$$

est-elle naturelle ? i.e. est-ce que pour chaque morphisme $\Lambda : E \longrightarrow E'$ de K_G on trouve que le diagramme

$$(21)\qquad \begin{tikzcd} \hat{D}(E) \arrow[r, "\eta_E"] \arrow[d, "\hat{D}(\Lambda)"'] & \hat{F}(E) \arrow[d, "\hat{F}(\Lambda)"] \\ \hat{D}(E') \arrow[r, "\eta_{E'}"'] & \hat{F}(E') \end{tikzcd}$$

est commutatif ? Mais démontrer la commutativité de (21) revient à démontrer la commutativité des cubes (10) et (16). Ainsi la réponse aux deux questions est affirmative.

Pour finir, une remarque d'une importance pratique. On se facilite certains calculs en normalisant les cochaînes.

D Une cochaîne $f^n \in C^n(G,A)$ est appelée normalisée si

$$f^n(\alpha_1,\ldots,\alpha_n) = 0$$

dès que l'un des arguments est l'élément unité de G. On voit facilement que le foncteur (H,∂) défini avec des cochaînes normalisées est un foncteur cohomologique satisfaisant aux deux conditions concernant H^0 et la valeur de H^n pour des modules coinduits. En théorie d'extensions, on aboutit aux cochaînes normalisées en prenant comme représentant du sous-groupe normal A toujours l'élément unité $0 \in A$:

$$r1 = 0 \in A \quad .$$

5 Sous-groupe des groupes d'isométries

5.1 Espace affine, espaces pseudo-euclidiens

Soit S un ensemble non vide et T un espace vectoriel réel de n-dimensions, i.e.

(1) $T = \mathbb{R}^n$.

Si T opère transitivement et fidèlement sur S, alors la

D paire (S,T) s'appelle <u>espace affine</u> réel de n-dimensions.

Que T opère sur S s'exprime par les formules

$T \times S \longrightarrow S$

(2) $(a,x) \longrightarrow a+x = x+a$

(3) $(a+b)+p = a+(b+p)$,

tandis que la transitivité et la fidélité de l'opération s'expriment par

(4) $\forall x,y \in S \quad \hat{\exists} a \in T \quad y = x+a$.

La transitivité correspond à l'existence, la fidélité à l'unicité. Ce vecteur unique a sera souvent noté

(5) $a = y-x$

et on dira que c'est un vecteur d'origine x et de but y.

D Les éléments de T s'appellent les <u>translations</u> de (S,T)

D ceux de S s'appellent les <u>points</u> de (S,T). Par commodité nous parlerons souvent de l'espace affine S. L'espace affine S n'est pas un espace vectoriel mais on peut facilement lui donner une telle structure "en choisissant une origine p". En effet, pour chaque $p \in S$, l'application

$\phi_p : S \longrightarrow T$

définie par

(6) $\phi_p : x \longmapsto x-p =: a \in T$

est une bijection et

(7) $$\phi_p^{-1} a = a+p = x \in S \quad .$$

Mais cette structure d'espace vectoriel n'est pas canonique, i.e. elle dépend du choix de l'origine.

Soit $(x_i)_{i \in I}$ une famille de points de S et $(k_i)_{i \in I}$ une famille de nombres réels tels que

(8) $$\sum_{i \in I} k_i = 1 \quad .$$

Alors, pour tout $z \in S$, l'expression

(9) $$[\sum_{i \in I} k_i(x_i - z)] + z = x \in S$$

D définit le même point x de S qu'on appelle le <u>barycentre</u> des points x_i et que l'on dénotera par

(10) $$x = \sum_{i \in I} k_i x_i \quad .$$

Une bijection

$$f: S \longrightarrow S$$

qui conserve les barycentres, i.e, telle que

(11) $$f(\sum_{i \in I} k_i x_i) = \sum_{i \in I} k_i (f x_i)$$

D s'appelle <u>bijection affine</u>. Les bijections affines forment

D un groupe, le <u>groupe affine A</u>.

Désignons par GL(T) le groupe des applications linéaires de T. Si T^+ est le groupe abélien sous-jacent à T on a

(12) $$GL(T) =: A_{\mathbb{R}}(T^+) \subset A(T^+)$$

et

(13) $$GL(T) \simeq GL(n, \mathbb{R}) \quad .$$

On peut vérifier qu'à chaque $g \in A(S)$ il correspond un unique élément $\partial g \in GL(T)$ défini par

(14) $\forall p \in S, \quad \forall a \in T \quad (\partial g)a = g(p+a) - gp$

et que l'application

(15) $\partial: \quad A(S) \longrightarrow GL(T)$

ainsi défini est un homomorphisme de groupes. En posant $p+a = y$ on trouve

(16) $(\partial g)(y-p) = gy-gp$.

Le noyau de ∂ est constitué par les translations :

(17) $\mathrm{Ker}\ \partial = T$.

On a ainsi une suite exacte courte de groupes

(18) $0 \longrightarrow T^+ \xrightarrow{(\kappa)} A \xrightarrow{\partial} GL(T) \longrightarrow 1$

et en vertu de la proposition 3.17, nous savons que $H^2(GL(T),T) = 0$ et l'extension est triviale. On peut donc écrire le groupe A comme produit semi-direct. Nous désigne-

D rons par <u>JGL(T)</u> le produit semi-direct de T^+ par GL(T) (ce dernier groupe étant considéré comme sous-groupe de $A(T^+)$).

Tous les relèvements $r: GL(T) \longrightarrow JGL(T)$ sont donc des homomorphismes. Il est utile d'examiner de près ces relèvements.

Considérons, pour un $x \in S$ donné, l'ensemble

(19) $G_p = \{g \in JGL(T) \mid gp = p\} \subset JGL(T)$.

D C'est un sous-groupe de JGL(T) appelé <u>sous-groupe fixateur</u> de p.

Pour tout $p \in S$ et tout $g \in JGL(T)$ il y a des éléments uniques $a \in T$ et $\alpha_p \in G_p$ tels que

(20) $g = a + \alpha_p \in JGL(T)$.

Le conjugué par $t \in T$ d'un sous-groupe fixateur G_p est encore un sous-groupe fixateur :

(21) $t + G_p - t = G_{p+t}$.

La bijection ϕ_p, définie par (6), induit un isomorphisme

(22) $\varphi_p: \ G_p \longrightarrow GL(T)$.

Posons en effet $g = \alpha_p \in G_p$ dans (16) et désignons par φ_p la restriction de ∂ à $G_p \subset JGL(T)$. Il vient :

(23) $$(\varphi_p \alpha_p)(\phi_p y) = \phi_p(\alpha_p y)$$

et on voit facilement que φ_p est un homomorphisme, donc un isomorphisme. Nous avons donc le diagramme suivant

(24) $$\begin{tikzcd} & & & G_p \arrow[dl, "(i_p)"'] \arrow[dr, "\varphi_p"] & & \\ 0 \arrow[r] & T^+ \arrow[r] & JGL(T) \arrow[rr, "\hat{\partial}"'] & & GL(T) \arrow[r] & 1 \end{tikzcd} .$$

L'application

(25) $$r_p =: i_p \, \varphi_p^{-1} : \quad GL(T) \longrightarrow G_p$$

est un monomorphisme. C'est aussi un relèvement :

(26) $$\partial r_p = 1_{GL(T)}$$

et

(27) $$\mathrm{Im}\, r_p = G_p \quad .$$

Ainsi un homomorphisme injectif r_p correspond au choix d'une origine p. Nous allons voir que la réciproque est vraie aussi.

<u>Proposition 5.1</u>. Un relèvement

$$r: \quad GL(T) \longrightarrow JGL(T)$$

est un homomorphisme injectif ssi

$$\exists p \in S \qquad \mathrm{Im}\, r = G_p \quad .$$

<u>Dém.</u>: Soit r un homomorphisme injectif $r: GL(T) \rightarrowtail JGL(T)$. Choisissons un $p \in S$; d'après (20)

(28) $$\forall \alpha \in GL(T) \qquad \hat{\exists} t(\alpha) \in T \qquad r\alpha = t(\alpha) + \alpha_p \quad .$$

De plus

(29) $$\hat{\exists} \alpha \in GL(T) \qquad \alpha_p = r_p \alpha$$

avec la section déterminée par le choix de p comme origine.

Ainsi

(30) $$r\alpha = t(\alpha) + r_p \alpha \quad .$$

Mais la différence de deux relèvements r et r_p qui sont des homomorphismes est un 1-cocycle :

(31) $$\begin{aligned} t(\alpha\beta) &= r(\alpha\beta) - r_p(\alpha\beta) \\ &= r\alpha + (-r_p\alpha + r_p\alpha) + r\beta - r_p\beta - r_p\alpha \\ &= t(\alpha) + \alpha(t(\beta)) \quad . \end{aligned}$$

Mais $H^1(GL(T),T) = 0$, en vertu de la proposition 3.17. Ainsi

(32) $$\exists a \in T \quad t(\alpha) = (d_o a)(\alpha) = a - \alpha a \quad .$$

En utilisant (21) on trouve alors

(33) $$\begin{aligned} r\alpha &= t(\alpha) + r_p\alpha = a - \alpha a + r_p\alpha = a + r_p\alpha - a - r_p\alpha + r_p\alpha \\ &= a + r_p\alpha - a = r_{p+a}(\alpha) \in G_{p+a} \quad . \end{aligned}$$

Ainsi le choix d'une origine correspond au choix d'un relèvement r qui est un homomorphisme injectif. //

La formule précédente montre d'ailleurs aussi qu'un changement d'origine de p en p+a correspond à une conjugaison par un élément a de T.

La relation (12) dit que l'homomorphisme $\varphi: GL(T) \longrightarrow A(T^+)$ déterminé par l'extension de T^+ par GL(T) est injectif. Nous allons montrer qu'alors T^+ est un sous-groupe abélien maximal de JGL(T).

<u>Proposition 5.2</u>. Soit X une extension d'un groupe abélien A par un groupe G et soit $\varphi: G \longrightarrow A(A)$ l'homomorphisme déterminé par l'extension,

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \longrightarrow & X & \xrightarrow{\sigma} & G & \longrightarrow & 1 \\ & & & & & & \downarrow{\scriptstyle \varphi} & & \\ & & & & & & A(A) & & \end{array}$$

A est un sous-groupe abélien maximal ssi φ est injectif.

<u>Lemme</u>. A est abélien maximal dans X ssi

(34) $$C_X(A) = A \quad .$$

Démonstration du lemme. Abélien maximal veut dire que A n'est contenu dans aucun autre sous-groupe abélien de X. Supposons que A est abélien maximal et prenons $x \in C_X(A)$. Le groupe engendré par A et x est alors abélien et contient A. Il doit donc être le groupe A lui-même, i.e. $x \in A$. Supposons maintenant $C_X(A) = A$. Soit A' un sous-groupe abélien de X contenant A et a' un élément quelconque de A'. Alors a' commute avec A donc $a' \in A$.

Démonstration de la proposition. Supposons que A est maximal abélien et soit

$$\alpha \in \operatorname{Ker} \varphi$$

et r un relèvement compatible avec φ. Alors

$$r\alpha \in C_X(A) = A$$

et

$$\alpha = 1 \in G \quad .$$

Supposons maintenant que φ est injectif et soit $x \in C_X(A)$. Alors

$$a = x + a - x = (\varphi\sigma x)a$$

et

$$\varphi\sigma x = 1_A \quad .$$

Donc

$$\sigma x = 1 \in G$$

et

$$x \in A \quad . //$$

Nous allons maintenant passer des espaces affines aux espaces pseudo-euclidiens. Considérons une application

(35) $$b\colon T\times T \longrightarrow \mathbb{R}$$

avec les propriétés suivantes ($\forall u,v,w \in T$, $\forall k \in \mathbb{R}$)

(36) $b(u,v) = b(v,u)$

(37) $b(u,v+w) = b(u,v) + b(u,w)$

(38) $b(kv) = kb(v)$.

D Une telle application s'appelle <u>forme bilinéaire</u> sur T. Posons

(39) $b(v,v) = q(v)$;

cela nous définit une application

$$q\colon T \longrightarrow K$$

ayant les propriétés suivantes

(40) $q(kv) = k^2 q(v)$

(41) $q(u+v) = q(u) + q(v) + 2b(u,v)$.

D Une telle application s'appelle <u>forme quadratique</u> sur T.

D La paire (T,q) s'appelle <u>espace (vectoriel) quadratique</u>. Un ensemble non vide S sur lequel un espace quadratique opère

D transitivement et fidèlement s'appelle <u>espace pseudo-euclidien</u>.

C'est donc un triplet (S,T,q); souvent nous parlerons simplement de l'espace pseudo-euclidien S.

Le groupe orthogonal $O(q)$ de l'espace quadratique (T,q) consiste des éléments de GL(T) qui laissent invariante la forme quadratique q. Plus précisément :

(42) $O(q) = \{\alpha \in GL(T) \mid \forall a \in T \quad q(\alpha a) = q(a)\}$.

Il s'ensuit que

(43) $\forall \alpha \in O(q), \quad \forall a,b \in T \qquad b(\alpha a,\alpha b) = b(a,b)$.

Puisque $O(q)$ contient le sous-groupe engendré par l'inversion, nous avons

(44) $H^n(O(q),T) = 0 \qquad n>0$.

D Deux <u>éléments</u> $a,b \in T$ sont <u>orthogonaux</u> si

$$b(a,b) = 0 \quad .$$

Soit U un sous-espace vectoriel de T: $U \subset T$. Le

D complément orthogonal $U^\perp$ de U est défini comme suit

(45) $$U^\perp = \{a \in T \mid b(a,U) = 0\} \quad .$$

D Un espace quadratique T est régulier si

$$T^\perp = 0 \quad .$$

On dit alors aussi que la forme quadratique est régulière ($T^\perp$

D est appelé le radical de T). Tous les espaces quadratiques que nous considérons dans la suite seront réguliers. (Je ne parlerai donc pas du groupe de Galilée.)

D Un élément $a \in T$ est dit isotrope si

$$q(a) = 0 \quad .$$

D Un espace quadratique $T \neq \{0\}$ est appelé totalement isotrope si

(46) $$\forall a \in T \quad q(a) = 0 \ ;$$

alors aussi

(47) $$\forall a,b \in T \quad b(a,b) = 0 \quad .$$

Nous utiliserons la proposition suivante que nous n'avons pas le temps de démontrer.

Proposition 5.3. Tous les sous-espaces totalement isotropes d'un espace quadratique T ont la même dimension.

D Cette dimension est appelée l'indice, ind T, de T. On parle aussi de l'indice de la forme quadratique q. On a pour l'indice l'inégalité suivante

(48) $$0 \leqslant 2 \text{ ind } T \leqslant \dim T \quad .$$

Si

(49) $$\text{ind } T = 0$$

D l'espace quadratique est dit défini (et la forme quadratique aussi). Si ce n'est pas le cas, l'espace (et la forme) quadra-

D tique sont indéfinis; de tels espaces contiennent toujours des vecteurs isotropes. Un espace quadratique T tel que pour tout $0 \neq a \in T$

$$q(a) > 0 \qquad\qquad [q(a) < 0]$$

D est appelé <u>défini positif</u> [défini négatif]. Tous les sous-espaces définis positifs maximaux [définis négatifs maximaux] d'un espace quadratique T ont la même dimension que l'on désignera par

$$\mathrm{ind}^{+}T \qquad\qquad [\mathrm{ind}^{-}T] \quad .$$

On peut voir que

$$\mathrm{ind}\, T = \text{minimum}\,(\mathrm{ind}^{+}T,\ \mathrm{ind}^{-}T) \quad .$$

Notre convention est

$$\mathrm{ind}\, T = \mathrm{ind}^{-}T \quad .$$

Soit S un espace pseudoeuclidien; en posant

(50) $$\forall x,y \in S \qquad \rho(x,y) = q(x-y) \quad ,$$

on peut introduire une distance ρ sur S, (mais en général cette distance n'a évidemment pas les propriétés de la fonction de distance introduite en topologie).

Une transformation $f \in A$ telle que

(51) $$\forall x,y \in S \qquad \rho(fx,fy) = \rho(x,y)$$

D est appelée <u>isométrie</u>. Les isométries forment un groupe,

D le <u>groupe des mouvements rigides</u> $M(q)$, qui est un sous-groupe de A. Les translations sont évidemment des isométries. On a donc la situation suivante

$$\begin{tikzcd}
0 \arrow[r] & T^{+} \arrow[r] \arrow[d, equal] & M(q) \arrow[r, dashed, "\bar{\sigma}"] \arrow[d] & \bar{M} \arrow[r, dashed] \arrow[d, dashed, "\nu"] & 1 \\
0 \arrow[r] & T^{+} \arrow[r] & JGL(T) \arrow[r] & GL(T) \arrow[r] & 1
\end{tikzcd}$$

Posons $(M(q)/T) = \overline{M}$ et $\overline{\sigma}$: $M(q) \longrightarrow\!\!\!\!\to \overline{M}$. Nous pouvons alors compléter le diagramme par un homomorphisme ν: $\overline{M} \longrightarrow GL(T)$ qui le rend commutatif; alors ν est une injection. Mais les éléments de $\overline{M}$ laissent la forme quadratique q invariante. En effet, en utilisant (16) avec $g \in M(q)$ on trouve pour tout $y,p \in S$

$$q[(\overline{\varphi}\overline{\sigma}g)(y-p)] = q(gy-gp) = q(y-p) \quad .$$

Ainsi

(52) $$\overline{M} = O(q) \subset GL(T) \quad .$$

Le groupe T est encore un sous-groupe maximal abélien de $M(q)$. Puisque $H^2(O(q),T) = 0$, le groupe des mouvements rigides $M(q)$ est une extension triviale de T par un sous-groupe $O(q)$ de $A(T^+)$. Nous noterons dorénavant par $JO(q)$ le produit semi-direct de T^+ par $O(q)$. Nous considérons $JO(q)$ comme sous-groupe donné de $JGL(T)$ et nous prendrons toujours les mêmes relèvements. Plus exactement

$$\overline{r}: \quad O(q) \longrightarrow JO(q)$$

sera la restriction de

$$\hat{r}: \quad GL(T) \longrightarrow JGL(T) \quad .$$

5.2. Sous-groupes des groupes des mouvements rigides

Soit $JO(q)$ le groupe des isométries d'un espace pseudo-euclidien (S,T,q), i.e. le produit semi-direct de T^+ par $O(q)$. (T est un espace vectoriel réel de dimension n, et le groupe abélien sous-jacent T^+ est un groupe abélien libre et un sous-groupe abélien maximal de $JO(q)$.) Pour un relèvement donné, les éléments de $JO(q)$ sont des paires (a,α) avec $a \in T$ et $\alpha \in O(q)$ et la loi interne est donnée par

(53) $$(a,\alpha) + (b,\beta) = (a+\alpha b,\alpha\beta) \quad .$$

Soit X un sous-groupe de $JO(q)$. Définissons le sous-

D groupe $U \subset X$ des <u>translations primitives de X</u> par

(54) $$U = T \cap X = \{a \in T \mid (a,1) \in X\} \quad .$$

D. Définissons le <u>groupe ponctuel</u> G de X par

(55) $$G = \{\alpha \in O(q) \mid (a,\alpha) \in X\} \quad .$$

Nous allons établir plusieurs propriétés des groupes U, X et G.

<u>Propriété 1</u>. Le groupe U est un groupe abélien libre. (Si U est discret, il est de rang $m \leqslant n$.)

<u>Propriété 2</u>.

(56) $$U \triangleleft X \quad \text{et} \quad G = X/U \quad .$$

En effet, $\forall x \in X$

$$xUx^{-1} = x(T\cap X)x^{-1} = xTx^{-1} \cap xXx^{-1} = T\cap X = U \quad .$$

<u>Propriété 3</u>. On a un morphisme d'extensions

(57)
$$\begin{tikzcd}
0 \arrow[r] & U \arrow[r, "\kappa"] \arrow[d, "(\lambda)"'] & X \arrow[r, "\sigma"] \arrow[d, "(\mu)"'] & G \arrow[r] \arrow[d, "\nu"] & 1 & {[m]} \\
0 \arrow[r] & T \arrow[r, "\bar\kappa"'] & JO(q) \arrow[r, "\bar\sigma"'] & O(q) \arrow[r] & 1 & \bar{m}=0
\end{tikzcd}$$

C'est une conséquence des propriétés 1 et 2 et de la proposition 1.14.

Propriété 4. Après le choix d'un relèvement

$r: G \longrightarrow X$ nous pouvons écrire

$$\forall x \in X \qquad x = \langle a,\alpha \rangle$$

avec $a \in U$, $\alpha \in G$. Soit $[m] \in H^2(G,U)$ la classe de cohomologie déterminée par l'extension X de A par G. Alors

(58) $$\exists u \in C^1(G,T) \qquad \mu\langle a,\alpha\rangle = (\lambda a + u\alpha, \nu\alpha)$$

et

(59) $$[\lambda_*][m] = 0 \in H^2(G,T) \qquad .$$

C'est une conséquence de la proposition 2.3. Nous avons vu que la relation (2.32) équivaut aux relations

$$\lambda_* m = \nu^* \bar{m} + d_1 u \in Z^2(G,T)$$

$$[\lambda_*][m] = [\nu^*][\bar{m}] \in H^2(G,T) \qquad .$$

Mais $JO(q)$ est un produit semi-direct, i.e.

$$\bar{m} = 0 \qquad .$$

Donc

(60) $$\lambda_* m = d_1 u \in B^2(G,T)$$

et

$$[\lambda_*][m] = 0 \qquad .$$

Tandis que la classe de 2-cohomologie $[m]$ caractérise le groupe X en tant qu'extension de U par G, la 1-cochaîne u décrit X comme sous-groupe du groupe des mouvements $JO(q)$ de l'espace pseudo-euclidien (S,T,q) et de ce fait comme groupe d'opérateurs sur cet espace. Car en effet en se donnant X comme extension de U par G, i.e. comme groupe d'éléments du type (a,α) on ne sait pas encore comment X opère sur l'espace S. Pour le savoir il faut plonger X dans le groupe des mouvements de S et alors on voit apparaître des éléments $u\alpha \in T$, donc des translations qui ne sont pas des éléments de U, donc pas des translations primitives. Pour cette raison la cochaîne u est appelée

D système de translations non-primitives du groupe X.

Il se pourrait cependant que pour tout $\alpha \in G$ l'élément $u\alpha$ soit une translation primitive, i.e. dans λU. Alors l'équation (60) montre que m est un 2-cobord :

$$\lambda_* m = \lambda_* d_1 \bar{u} \qquad \bar{u} \in C^1(G,A)$$

$$m = d_1 \bar{u}$$

(61) $$[m] = 0 \quad .$$

Par conséquent l'extension X de U par G est triviale. On a donc la propriété suivante :

Propriété 5. Un groupe sans translations non-primitives est une extension triviale et (π est défini par (63) ci-dessous)

(62) $$\pi_* u = 0 \in Z^1(G,T/U) \quad .$$

Nous verrons qu'en général la réciproque n'est pas vraie : un groupe peut avoir des translations non-primitives et être une extension triviale.

Explorons maintenant les propriétés des systèmes de translations non-primitives. Considérons pour cela la suite exacte courte de G-modules.

(63) $$0 \longrightarrow U \xrightarrow{\lambda} T \xrightarrow{\pi} T/U \longrightarrow 0 \quad .$$

Propriété 6.

(64) $$\pi_* u \in Z^1(G,T/U)$$

(65) $$[m] = \partial_1 [\pi_* u] \quad .$$

Ces deux relations sont des conséquences de (60). En effet

(66) $$d_1 \pi_* u = \pi_* d_1 u = \pi_* \lambda_* m = 0$$

et alors -- d'après la définition de l'homomorphisme de connection -- (60) veut dire exactement la même chose que (65).

Il est assez clair que la réciproque est aussi vraie, i.e. si $u \in C^1(G,T)$ est tel que $\pi_* u \in Z^1(G,T/U)$ alors il existe un 2-cocycle $m \in Z^2(G,U)$ et une extension X de U par G correspondant à ce m, tel que u est un système de translations non-primitives de X. Nous avons donc la propriété suivante :

<u>Propriété 7</u>. L'élément $u \in C^1(G,T)$ est un système de translations non-primitives du groupe X du diagramme (57) ssi $\pi_* u \in Z^1(G,T/U)$.

Maintenant nous voudrions savoir encore comment $\pi_* u$ dépend du choix de l'origine pour $JO(q)$. Nous savons que c'est équivalent à un changement du relèvement $O(q) \longrightarrow JO(q)$ et que cela revient à ajouter à u un 1-cobord (voir (32)) :

(67) $$u \rightsquigarrow u + d_o a \quad .$$

Si on change le relèvement $G \longrightarrow X$ le résultat est le suivant

$$\mu r'\alpha = \mu(c\alpha + r\alpha) = \lambda(c\alpha) + u\alpha + \bar{r}v\alpha$$
$$= (\lambda_* c + u)(\alpha) + \bar{r}v\alpha =: u'\alpha + \bar{r}v\alpha$$

avec $c \in C^1(G,U)$. Le résultat de tous ces changements est

(69) $$u \rightsquigarrow u + \lambda_* c + d_o a$$

et on voit que la classe de cohomologie dans $H^1(G,T/U)$ n'est pas affectée. Des <u>systèmes de translations non-primitives</u> qui diffèrent par un changement des relèvements sont appelés

D <u>équivalents</u>. Des systèmes équivalents déterminent le même élément de $H^1(G,T/U)$. On peut voir que réciproquement un élément de ce groupe de cohomologie détermine des translations non-primitives qui diffèrent uniquement par le choix des deux relèvements. Nous avons ainsi démontré la proposition suivante.

<u>Proposition 5.4.</u> Les systèmes inéquivalents de translations non-primitives sont en correspondance biunivoque avec les éléments du premier groupe de cohomologie $H^1(G,T/U)$.

Revenons au diagramme (57) :

$$\begin{tikzcd} 0 \arrow[r] & U \arrow[r] \arrow[d, "\lambda"] & X \arrow[r, "\sigma"] \arrow[d, "\mu"] & G \arrow[r] \arrow[d, "\nu"] & 1 & {[m]}\ \varphi \\ 0 \arrow[r] & T \arrow[r] & JO(q) \arrow[r, "\bar{\sigma}"'] & O(q) \arrow[r] & 1 & {[0]}\ \bar{\varphi} \end{tikzcd} \quad .$$

Nous pouvons résumer la situation ainsi : $H^2(G,U)$ classifie les extensions de U par G. $H^1(G,T/U)$ classifie les inclusions μ de X dans $JO(q)$; on peut donc dire que $H^1(G,T/U)$ classifie les groupes X comme groupes de transformations de l'espace pseudo-euclidien. Il y a deux points à retenir: (i) la classification par H^1 est beaucoup plus fine, (ii) chaque extension X de U par G n'est pas nécessairement un sous-groupe de $JO(q)$; c'est le cas seulement si

(70) $$\lambda_*[m] = 0 \quad .$$

Cela se voit d'ailleurs en examinant la suite exacte de cohomologie

(71) $$\longrightarrow H^1(G,T) \xrightarrow{[\pi_*]} H^1(G,T/U) \xrightarrow{\partial_1} H^2(G,U) \xrightarrow{[\lambda_*]} H^2(G,T) \longrightarrow$$

La propriété (i) reflète le fait que ∂_1 n'est pas injectif : plusieurs éléments de $H^1(G,T/U)$ correspondent à un seul élément de $H^2(G,U)$. La propriété (ii) est une conséquence du fait que ∂_1 n'est pas surjectif : il y a des éléments de $H^2(G,U)$ qui ne correspondent à aucun élément de $H^1(G,T/U)$ donc à aucun sous-groupe de $JO(q)$.

Jusqu'à maintenant nous n'avons pas supposé que X est un sous-groupe crystallographique. Il nous faut expliquer encore ce que nous entendons par crystallographique.

D Le groupe X est un sous-groupe crystallographique de $JO(q)$ si le groupe $U = T \cap X$ (rappelons $T = \mathbb{R}^n$) est (i) un groupe

D abélien libre de rang n et (ii) si λU engendre l'espace

D vectoriel réel T. On dit alors que U est un réseau sur T. La condition (i) signifie $U \cong Z^n$, la condition (ii) peut s'exprimer par $T = \mathbb{R}U$. Cette dernière condition est tout à fait essentielle parce que l'on peut trouver un groupe abélien libre de rang n et le plonger dans $\mathbb{R}^n$ sans qu'il n'engendre $\mathbb{R}^n$ tout entier. Voici un exemple en dimension 2. Les éléments a et πa ($\pi = 3.14 \ldots$) engendrent un groupe libre de rang 2, parce que π est irrationnel, mais n'engendrent pas $\mathbb{R}^2$, un espace vectoriel réel de dimension 2.

Proposition 5.5. Si X est crystallographique, alors U est abélien maximal dans X.

Dém.: Nous devons montrer que $C_X(U) = U$. Soit donc

$$g \in C_X(U) \quad ,$$

alors

$$\sigma g \in \operatorname{Ker} \varphi$$

et puisque U est un réseau sur T on a aussi

$$\nu\sigma g = \bar{\sigma}\mu g \in \operatorname{Ker} \bar{\varphi} = 1 \in O(q)$$

de sorte que

$$\mu g \in T \quad .$$

Mais alors

$$g \in T \cap X = U \quad . //$$

Proposition 5.6. Un groupe ponctuel crystallographique G est isomorphe à un sous-groupe de $GL(n,\mathbb{Z})$.

Dém.: Puisque U est abélien maximal, φ est un homomorphisme injectif; $GL(n,\mathbb{Z})$ est le groupe des automorphismes de $\mathbb{Z}^n$. //

D'après un théorème de Siegel sur les formes quadratiques indéfinies régulières, on peut conclure que la plupart des groupes ponctuels crystallographiques ont une présentation finie, i.e. ils peuvent être définis par un nombre fini de générateurs et un nombre fini de relations entre ces générateurs.

Proposition 5.7. Soit X un sous-groupe crystallographique de $JO(q)$ et $U = X \cap T$. Si l'indice de T est 0 ou 1, alors tout sous-groupe abélien normal, V, de X est contenu dans U (et donc abélien libre).

Dém.: Soit

(72) $$v = (a,\alpha) \in V \subset X \qquad a \in U,\ \alpha \in G$$

alors

$$\forall c \in U \quad w =: (c,1)(a,\alpha)(c,1)^{-1} = (a+c-\alpha c,\alpha) \in V$$

parce que $V \triangleleft U$. Mais on trouve aussi

(73) $$\begin{aligned} v^{-1}wv &= (-m(\alpha^{-1},\alpha) - \alpha^{-1}a,\alpha^{-1})(a+c-\alpha c,\alpha)(a,\alpha) \\ &= (a-c+\alpha^{-1}c,\alpha) = w \end{aligned}$$

parce que V est abélien. Ainsi

$$\forall c \in U \qquad 2c = \alpha c + \alpha^{-1}c \quad .$$

Considérons maintenant $q(c)$. Nous avons

$$\begin{aligned} 2q(c) = b(c,2c) &= b(c,\alpha c+\alpha^{-1}c) = b(c,\alpha c) + b(c,\alpha^{-1}c) \\ &= b(c,\alpha c) + b(\alpha c,\alpha\alpha^{-1}c) = 2b(c,\alpha c) \quad . \end{aligned}$$

Ainsi

(74) $$b(c,c) - b(c,\alpha c) = b(c,c-\alpha c) = 0$$

(75) $$b(\alpha c,c) - b(\alpha c,\alpha c) = b(\alpha c,c-\alpha c) = 0$$

et

(76) $$q(c-\alpha c) = 0 \quad .$$

Si ind $T = 0$, alors

$$\forall c \in U \qquad c = \alpha c \quad ,$$

donc $\alpha = 1 \in G$ et $v \in U$. Si ind $T = 1$, choisissons un $c \in T$ tel que

(77) $$q(c) < 0 \quad .$$

Alors (74) implique

(78) $$c = \alpha c$$

pour tout c satisfaisant à (77). Mais il y a dans c n éléments linéairement indépendants $c_1,\ldots,c_i,\ldots,c_n$ tels que $q(c_i) < 0$. La relation (78) est donc valable pour tout $c \in U$ et de nouveau $\alpha = 1$. //

Remarquons que la démonstration ci-dessus n'est plus valable si ind $T > 1$, car alors il est possible d'avoir deux vecteurs $c,d \in T$ tels que

$$q(c) < 0 \qquad q(d) = 0 \qquad b(c,d) = 0 \quad .$$

Proposition 5.8. Un sous-groupe normal, abélien libre et abélien maximal de X est unique.

Dém.: Soient U et V deux sous-groupes satisfaisant à ces conditions. De la proposition précédente il suit que $U \subset V$ et que $V \subset U$. //

Mais supposons maintenant que l'indice de la forme quadratique est zéro (dans ce cas on dit qu'elle est définie). Le groupe $JO(q)$ est alors le groupe d'Euclide. Bieberbach a montré qu'alors les groupes ponctuels crystallographiques sont finis. En vertu de la proposition 3.20 on a alors

(79) $$H^1(G,T) = H^2(G,T) = 0$$

et la suite exacte de cohomologie (71) donne alors <u>l'isomorphisme fondamental de la crystallographie définie</u> :

(80) $$H^1(G,T/U) \cong H^2(G,U) \quad .$$

Cela veut dire (i) que chaque extension X d'un groupe abélien libre U de rang n par un groupe fini G isomorphe à un sous-groupe de $GL(n,\mathbb{Z})$ est un sous-groupe crystallographique du groupe d'Euclide à n-dimensions E^n, donc un groupe d'espace. (ii) Les classifications des sous-groupes X de E^n par $H^1(G,T/U)$ en tant que groupes de transformations de l'espace d'Euclide et par $H^2(G,U)$ en tant qu'extensions de U par G coïncident. Historiquement la description de la structure algébrique des groupes d'espace via $H^1(G,T/U)$, donc par translations non-primitives, précède (Zassenhaus 1948); la description par les extensions et l'isomorphisme entre les deux ont suivi seulement plus tard (Janner et Ascher, Physica <u>54</u>, 77 (1971)).