الجمهورية الجزائرية الديموقراطية الشعبية
République Algérienne Démocratique et Populaire
وزارة التعليم العالي و البحث العلمي
Minstère de l'Enseignement Supérieur et de la Recherche Scientifique

CENTRE UNIVERSITAIRE DE MILA
INSTITUT DES SCIENCES ET DE LA TECHNOLOGIE

Réf.

Mémoire de fin d'étude
Présenté pour l'obtention du diplôme de

Licence Académique

Domaine : **Mathématiques et Informatique**
Filière : **Mathématiques**
Spécialité : **Mathématiques fondamentale**

Thème

Extensions de Groupes

Présenté par :

* **Zeghilet Fatiha**
* **Chouchi Seloua**
* **Cherafa Seloua**

Dirigé par :

-- Mr. Bouguebina mounir

Année universitaire 2012-2013

Extensions de Groupes

Zeghilet fatiha ,Chouchi seloua et Cherafa seloua

Table des matières

Remerciements

Avant tout nous remercions Dieu qui nous a donné la force pour terminer ce travail. Nous adressons nos remerciements à notre encadreur le professeur Bouguebina Mounir pour sa disponibilité et ses encouragements. Nous adressons aussi nos remerciements à tous les enseignants de l'institut des sciences et de la technologie. Enfin, merci a tous ceux qui ont contribué de prés ou de loin a l'élaboration de ce modeste travail.

Introduction

Les extensions de groupes constituent une partie d'une théorie trés riche et abondamment utilisée en Mathématiques : la théorie de l'homologie (et de la cohomologie). Le but de ce modeste travail est de donner la définition précise de ce qu'est une extension de groupes et d'étudier ses principales propriétés. En particulier le problème de la classification des extensions est posé et on en donne des solutions complètes pour certains types d'extensions, notamment les extensions scindées et centrales. La classification du premier type fait intervenir la notion de produit semidirect de groupes et celle du second type fait intervenir certaines classes de cohomologie, éléments du deuxième groupe de cohomologie d'un groupe à coefficients dans un groupe abélien.

Ce mémoire est organisé de la manière suivante : le premier chapitre est un rappel de quelques notions de théorie des groupes que nous utiliserons par la suite. Le second chapitre commence par la définition de la notion d'extension de groupes que l'on caractérise à isomorphisme prés et finit par l'introduction des extensions scindées et leur classification. Dans le dernier chapitre, aprés avoir défini les extensions centrales et quelques notions de cohomologie, on explique comment le H^2 permet de caractériser complètement cex extensions.

Chapitre 1

Groupes

Dans ce premier chapitre, nous rassemblons quelques éléments de la théorie des groupes en insistant notamment sur les notions de sous-groupe normal, de produit semidirect de groupes et d'opération d'un groupe sur un ensemble qui ne sont en général pas inclus dans un premier cours sur les groupes. Ces notions, importantes en elle mêmes, seront constamment utilisées dans les chapitres suivants.

1.1 Loi de composition interne

Soit G un ensemble. Une loi de composition interne sur G est une application $G \times G \longrightarrow G$ qui à deux éléments $x, y \in G$, associe un troisième élément $x * y$. On dit aussi que $*$ est une opération sur G et on parle du couple $(G, *)$.

Exemple

1) $*$ = addition dans $\mathbb{N}, \mathbb{Z}$ ou $\mathbb{Q}$.

2) $*$ = $\cup$ ou $\cap$ dans $E = P(A)$, l'ensemble des parties d'un ensemble quelconque A.

Propriétés

1) On dit que $*$ est associative si :

$$x * (y * z) = (x * y) * z$$

pour tous $x, y, z \in G$.

2) On dit que $*$ est commutative si :

$$x * y = y * x$$

pour tous $x, y \in G$.
3) Soit $e \in G$. On dit que e est un élément neutre pour $*$ si :

$$x * e = e * x = x$$

pour tout $x \in G$. Si e existe, il est alors unique. En effet supposons que $e^{'}$ soit un autre élément neutre. On a alors : $e * e^{'} = e$ ($e^{'}$ est élément neutre) et $e * e^{'} = e^{'}$ (e est élément neutre) et donc $e = e^{'}$. Un couple $(G, *)$ ayant un élément neutre est appelé monoide.Par exemple $(\mathbb{N}, +)$ est un monoide d'élément neutre 0.
4) Soit e un élément neutre de $(G, *)$. Soient $x, x^{'}$ deux éléments de G. On dit que $x^{'}$ est le symétrique de x pour la loi $*$ si :

$$x * x^{'} = x^{'} * x = e.$$

Le symétrique , s'il existe, est unique si $*$ est associative. En effet si $x^{'}$ et $x^{''}$ sont deux symétriques de x, on a : $x^{''} = e * x^{''} = (x^{'} * x) * x^{''} = x^{'} * (x * x^{''}) = x^{'} * e = x^{'}$.
Exemple
1) Dans $(\mathbb{N}, +)$, aucun élément autre que 0 n'a de symétrique. Le symétrique de 0 est 0.
2) Dans $(\mathbb{Z}, +)$, tout élément a un symétrique : le symétrique de x est $-x$.
3) Dans $(\mathbb{Z}, \times)$, l'élément neutre est 1 et c'est le seul élément qui ait un symétrique.

1.2 Groupes

Soit G un ensemble muni d'une loi de composition interne $*$.

Definition 1 *: Le couple $(G, *)$ est un groupe si*
- *$*$ est associative.*
- *$*$ admet un élément neutre e.*
- *tout élément x de G admet un symétrique $x^{'}$ pour $*$.*

Si $*$ est commutative, on dit que $(G, *)$ est un groupe commutatif ou abélien.

Exemple
1) $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +)$ sont des groupes. L'élément neutre est 0 et le symétrique de x est $-x$. L'associativité est évidente.
2) $(\mathbb{N}, +)$ n'est pas un groupe car aucun élément autre que 0 n'a de symétrique.

3) $(\mathbb{Z}, \times)$ n'est pas un groupe. La multiplication est associative dans $\mathbb{Z}$ d'élément neutre 1, mais si $x \neq 1$, alors x n'a pas de symétrique.
4) $(\mathbb{Q}^* = \mathbb{Q} - \{0\}, \times)$ est un groupe ainsi que $(\mathbb{R}^* = \mathbb{R} - \{0\}, \times)$. L'élément neutre est 1 et le symétrique de x est $x^{-1} = \frac{1}{x}$

Definition 2 *: Soit $(G, *)$ un groupe et soit H une partie non vide de G. On dit que H est un sous-groupe de G si :*

- *H est stable pour la loi $*$: $x, y \in H \Rightarrow x * y \in H$.*
- *muni de la loi $*$, H est lui-même un groupe.*

Notation : $H < G$
Remarque : En pratique pour montrer que H est un sous-groupe de G, il suffit de vérifier que $x, y \in H \Rightarrow x * y^{'} \in H$. Remarquer aussi que G et H ont même élément neutre : $e_G = e_H$.
Exemple
1) Pour $* = +$, on a des inclusions de sous-groupes : $\mathbb{Z} < \mathbb{Q} < \mathbb{R} < \mathbb{C}$.
2) Pour $* = \times$, on aussi des inclusions : $\{1\} < \{-1, 1\} < \mathbb{Q}^* < \mathbb{R}^* < \mathbb{C}^*$.
3) Tout sous-groupe de $(\mathbb{Z}, +)$ est de la forme $n\mathbb{Z}$ pour $n \in \mathbb{N}$. En effet $n\mathbb{Z}$ est clairement un sous-groupe de $\mathbb{Z}$. Inversement soit H un sous-groupe de $\mathbb{Z}$. Soit n le plus petit élément positif non nul de H. Si $x \in H$, la division euclidienne de x par n donne $x = kn + r$ avec $k \in \mathbb{Z}$ et $0 \leq r < n$. Comme H est un sous-groupe, on doit avoir $x - kn = r \in H$. Par définition de n, on doit avoir $r = 0$ et $x = kn$. Donc $H = n\mathbb{Z}$.

Le nombre d'éléments d'un groupe G est appelé son ordre qui peut donc être fini ou infini. Un groupe fini est un groupe d'ordre fini. Soit S une partie de G. Le sous-groupe engendré par S est le plus petit sous-groupe de G contenant S. On le note $< S >$. C'est l'ensemble des produits finis $x_1 . . . . x_n$ avec $x_i \in S$ ou $x_i^{'} \in S$. Quand $S = \{a\}$ avec $a \in G$, le sous-groupe $< S >=< a >$ est appelé le groupe cyclique engendré par a. Ses éléments sont les puissances a^n de a. Le groupe G est de type fini si $G =< S >$ avec S une partie finie de G. En particulier tout groupe cyclique (engendré par un seul élément) est de type fini.
Remarque : De type fini ne veut pas dire fini. Par exemple $\mathbb{Z}$ muni de l'addition est un groupe de type fini et même cyclique engendré par 1. Mais il contient une infinité d'éléments.

Definition 3 *: Soient $(G, *)$ et $(H, \perp)$ deux groupes. Une application $f : G \longrightarrow H$ est un morphisme de groupes si :*

$$f(x * y) = f(x) \perp f(y)$$

$\forall x, y \in G.$

Autrement dit f préserve les structures de groupes de G et H. Si f est bijective, on dit que c'est un isomorphisme. Si $G = H$ et $* = \perp$, on parle d'endomorphisme et d'automorphisme. Noter que $f(e_G) = e_H$. Le noyau du morphisme f est :

$$Kerf = \{x \in G : f(x) = e_H\} = f^{-1}(e_H).$$

C'est un sous-groupe de G. Le noyau est utile pour detecter si f est injective ou non. En effet on a : f injective si et seulement si $Kerf = \{e_G\}$. Par exemple le morphisme $f : \mathbb{Z} \longrightarrow \mathbb{Z}$ donné par $f(x) = 3x$ est injectif puisque $Kerf = \{0\}$ (la loi de groupe est l'addition). De même l'image de f :

$$Im(f) = f(G)$$

est un sous-groupe de H et f est surjective si et seulement si $Im(f) = H$.

L'ensemble $Aut(G)$ de tous les automorphismes de G devient lui-même un groupe en prenant comme opération la composition des applications. L'élément neutre est l'identité Id_G.

Remarque : Si la loi $*$ est commutative, on la note additivement : $* = +, e = 0$ et $x^{'} = -x$. Dans le cas général elle est notée multiplicativement : $* = ., e = 1$ et $x^{'} = x^{-1}$. C'est ce que nous ferons dans toute la suite de ce travail.

1.3 Sous-groupes normaux

Soit G un groupe et soit H un sous-groupe de G. La relation modulo H à gauche est la relation sur G définie par

$$x \Re y \Leftrightarrow y = xh$$

pour un certain $h \in H$. On vérifie facilement que c'est une relation d'équivalence sur G. Les classes d'équivalence sont les

$$xH = \{xh, h \in H\}$$

De la même manière on définit les classes à droite

$$Hx = \{hx, h \in H\}$$

Remarquer que les classes à gauche et à droite sont en général distinctes.

Definition 4 *: Le sous-groupe H de G est dit normal si les classes à gauche modulo H sont égales aux classes à droite modulo H :*

$$xH = Hx$$

La condition $xH = Hx$ équivaut à $xHx^{-1} = H$ et si $i_x : G \to G$ est l'automorphisme de conjugaison intérieure de G vers lui-même donné par $i_x(y) = x^{-1}yx$, elle équivaut aussi à $i_x(H) = H$ pour tout $x \in G$. Mais dans la pratique pour montrer que H est normal, on utilise plutôt la condition équivalente suivante

$$xhx^{-1} \in H$$

pour tout $h \in H$.

Si $f : G \longrightarrow G^{'}$ est un morphisme de groupes, son noyau $Kerf$ est toujours un sous-groupe normal de G. En effet soit $h \in Kerf$. Donc $f(h) = 1_{G'}$. Pour tout $x \in G$, on a $f(xhx^{-1}) = f(x)f(h)f(x^{-1}) = f(x)f(x)^{-1} = 1_{G'}$ et donc $xhx^{-1} \in Kerf$.

Comme on va le voir tout sous-groupe normal est le noyau d'un certain morphisme de groupes. L'égalité des classes à gauche et à droite permet de multiplier deux classes entre elles :

$$xHyH = xyHH = xyH$$

et définit donc une multiplication sur l'ensemble des classes :

$$\frac{G}{H} = \{xH, x \in G\}$$

qui devient ainsi un groupe pour cette opération, appelé le groupe quotient de G par H. Son élément neutre est la classe de 1_G i.e H. On a automatiquement un morphisme de groupes

$$\phi : G \longrightarrow \frac{G}{H}$$

qui envoie $x \in G$ vers sa classe xH. Ce morphisme est par défintion surjectif et son noyau est

$$Ker\phi = H$$

En effet $\phi(x) = 1_{\frac{G}{H}} = H$ si et seulement si $xH = H$ et donc $xh = h^{'}$ pour $h, h^{'} \in H$. ce qui donne $x = h^{'}h^{-1} \in H$.

Ainsi tout morphisme de groupes $f : G \longrightarrow G^{'}$ induit un isomorphisme :

$$\frac{G}{Kerf} \longrightarrow Im(f)$$

1.4 Produit direct et semidirect

Soient G_1 et G_2 deux groupes. Sur l'ensemble produit :

$$G_1 \times G_2 = \{(x, y), x \in G_1, y \in G_2\}$$

on definit une multiplication

$$(x, y)(x^{'}, y^{'}) = (xx^{'}, yy^{'})$$

qui fait de $G_1 \times G_2$ un groupe. Par exemple son élément neutre est $(1_{G_1}, 1_{G_2})$ et l'inverse de (x, y) est (x^{-1}, y^{-1}).

Definition 5 *: Le groupe $G_1 \times G_2$ ainsi construit est appelé le produit direct de G_1 et G_2*

Soient H et N deux groupes avec un morphisme $g : H \longrightarrow Aut(N)$. Soit $G = H \times N$ muni de la multiplication :

$$(h, n)(h^{'}, n^{'}) = (hh^{'}, n^{g(h^{'})}n^{'})$$

avec $y^x = x^{-1}yx$. Cette opération fait de G un groupe. L'élément neutre est $(1_H, 1_N)$ et l'inverse de (h, n) est $(h^{-1}, (n^{-1})^{g(h)^{-1}})$.

Definition 6 *: Le groupe G ainsi défini est appelé le produit semidirect extérieur de H et N.*

Les morphismes $H \longrightarrow G$ et $N \longrightarrow G$ donnés par $h \mapsto (h, 1_N)$ et $n \mapsto (1_H, n)$ sont clairement injectifs et permettent d'identifier H et N à leurs images H^* et N^* dans G. Comme $(h, 1_N)(1_H, n) = (h, n)$, on obtient que

$$G = H^*N^*$$

De plus $H^* \cap N^* = 1_G$ et N^* est normal dans G.

Definition 7 *: Si $G = H^*N^*$ avec N^* normal dans G et $H^* \cap N^* = 1_G$, on dit que G est le produit semidirect intérieur de H^* et N^*.*

La conjugaison dans N^* par $(h, 1_N)$ est l'automorphisme $g(h)$ (en identifiant N et N^*) et on a donc aussi un morphisme $H^* \longrightarrow Aut(N^*)$ avec lequel on peut voir G comme le produit semidirect extérieur de H^* et N^*. Ceci montre que les deux notions coincident et on parlera tout simplement de produit semidirect. Enfin remarquons que le produit semidirect est un produit direct si et seulement si le morphisme g est trivial ($g(h) = Id_N$, pour tout $h \in H$).

1.5 Opération d'un groupe sur un ensemble

Soient G un groupe et E un ensemble. Une opération de G sur E est une application :

$$G \times E \longrightarrow E$$

qui à un élément $x \in G$ et à un élément $a \in E$ associe lélément $xa \in E$ et telle que $x(ya) = (xy)a$ et $1_G a = a$ pour tous $x, y \in G$ et tout $a \in E$. L'application $a \mapsto xa$ est alors une bijection de S pour tout $x \in G$. On obtient donc une application :

$$G \longrightarrow Bij(E)$$

de G vers l'ensemble des bijections de E qui est une autre manière de définir l'opération.

Tout groupe G opère sur lui-même par conjugaison intérieure. En effet soit $x \in G$. Alors i_x est un automorphisme de G et on obtient donc un morphisme :

$$G \longrightarrow Aut(G)$$

qui à x associe i_x. Le noyau de ce morphisme est constitué des éléments $x \in G$ tels que $x^{-1}yx = y$ pour tout $y \in G$. C'est donc l'ensemble des éléments de G qui commutent avec tous les autres éléments de G.

Definition 8 *: Ce noyau est appelé le centre de G et on le note $Z(G)$. On a donc*

$$Z(G) = \{x \in G / xy = yx, \forall y \in G\}$$

$Z(G)$ est un sous-groupe normal de G, mais ce qui le caractérise le plus, c'est que c'est un sous-groupe abélien de G.

Chapitre 2

Extensions de groupes

Ce chapitre constitue le coeur de ce travail. On y définit pour la première fois la notion d'extension de groupes qui fait intervenir deux groupes quelconques Q et N et qui les met dans un gadget mathématique appelé suite exacte. Tout ceci, et plus encore, est expliqué en détail dans la première section, dans laquelle on caractérise aussi les extensions isomorphes. La deuxième section est un petit interlude qui permet de voir une relation intéressante entre les extensions de groupes et les torseurs sous un groupe. Dans la troisième et dernière section, le problème de la classification des extensions est posé et on en donne une solution complète pour un certain type d'extensions appelées les extensions scindées. Comme on le verra les produits semidirects de groupes vont jouer un rôle prédominant dans cette classification.

2.1 Définition

Soient Q et N deux groupes. On dit qu'un groupe G est une extension de Q par N s'il existe une suite exacte courte :

$$1 \longrightarrow N \xrightarrow{i} G \xrightarrow{p} Q \longrightarrow 1$$

c'est à dire que i est un morphisme injectif, p est un morphisme surjectif de groupes et :

$$Ker(p) \cong Im(i)$$

L'injection i permet d'identifier le groupe N au sous-groupe $i(N)$ de G, ce que nous ferons dans la suite. On peut déja caractériser ce sous-groupe :

Proposition 1 *: Le sous-groupe N (i.e $i(N)$) de G est un sous-groupe normal.*

Preuve : On doit montrer que pour tout $a \in N$ et tout $g \in G$, on a $gag^{-1} \in N$. Comme $p : G \longrightarrow Q$ est un morphisme de groupes, on a

$$p(gag^{-1}) = p(g)p(a)p(g^{-1})$$

et comme $p(g^{-1}) = p(g)^{-1}$ et $p(a) = 1_G$, ceci donne

$$p(gag^{-1}) = p(g)1p(g)^{-1} = 1_G$$

Donc $gag^{-1} \in Kerp \cong Im(i) = N$.

Comme conséquence on obtient que Q est le quotient de G par N. En effet le morphisme $p : G \longrightarrow Q$ est surjectif et son noyau est N. Donc

$$Q \cong \frac{G}{Kerp} = \frac{G}{N}$$

Ainsi pour tout groupe G, si N est un sous-groupe normal de G et si $Q = \frac{G}{N}$ est le groupe quotient, alors G est une extension de Q par N.
Exemple : Soient Q et N deux groupes quelconques et posons $G = N \times Q$ le produit direct de N et Q :

$$G = \{(a, b), a \in N, b \in Q\}$$

On peut voir G comme une extension de Q par N. En effet, on définit deux morphismes $i : N \longrightarrow G$ et $p : G \longrightarrow Q$ par $i(a) = (a, 1_Q)$ et $p((a, b)) = b$. Il faut montrer que i est un morphisme injectif, que p est un morphisme surjectif et que $Kerp \cong Im(i)$. Il est clair que i et p sont des morphismes de groupes. Soit $a \in N$ tel que $i(a) = 1_G = (1_N, 1_G)$ Donc $(a, 1_Q) = (1_N, 1_Q)$ et donc $a = 1_N$. Ceci montre que i est injective. Soit $b \in Q$. On a par exemple $p(1_N, b) = b$ et donc p est surjective. enfin $Kerp = \{(a, b) \in G/b = 1_q\} = \{(a, 1_Q), a \in N\} \cong N$. On a donc une suite exacte

$$1 \longrightarrow N \xrightarrow{i} N \times Q \xrightarrow{p} Q \longrightarrow 1$$

ce qui montre que G est une extension de Q par N. Cette extension est appelée l'extension triviale de Q par N.

Definition 9 *: Soient G_1 et G_2 deux extensions de Q par N. Un morphisme de la première extension vers la deuxième extension est un morphisme de groupes $f : G_1 \longrightarrow G_2$ tel que le diagramme suivant soit commutatif :*

$$\begin{array}{ccccccccc} 1 & \longrightarrow & N & \xrightarrow{i_1} & G_1 & \xrightarrow{p_1} & Q & \longrightarrow & 1 \\ & & \| & & f\downarrow & & \| & & \\ 1 & \longrightarrow & N & \xrightarrow{i_2} & G_2 & \xrightarrow{p_2} & Q & \longrightarrow & 1 \end{array}$$

La commutativité du diagramme veut dire que les compositions des flèches de même source et de même but en suivant des directions différentes sont égales. La proposition suivante montre que tout morphisme d'extensions est forcément un isomorphisme.

Proposition 2 *: Soient G_1 et G_2 deux extensions de Q par N. Alors tout morphisme d'extensions $f : G_1 \longrightarrow G_2$ est un isomorphisme.*

Preuve : Soit $g \in G_1$ tel que $f(g) = 1_{G_2}$. Donc $p_2 \circ f(g) = 1_Q = p_1(g)$. Donc $g \in Kerp_1 = Im(i_1)$. Il existe donc $a \in N$ tel que $g = i_1(a)$. Donc $f \circ i_1(a) = i_2(a) = 1_{G_2}$. Comme i_2 est injective, on doit avoir $a = 1_N$ et donc $g = i_1(a) = 1_{G_1}$. Ceci montre que f est injective. Soit $g \in G_2$. Peut-on trouver $g_1 \in G_1$ tel que $f(g_1) = g$? On sait que $p_2(g) \in Q$, donc il existe $g_1^{'} \in G_1$ tel que $p_2(g) = p_1(g_1^{'})$. On a $(p_2 \circ f)(g_1^{'}) = p_1(g_1^{'}) = p_2(g)$. Donc $gf(g_1^{'-1}) \in i_2(N) = f \circ i_1(N) = f(i_1(N))$. Donc $g = f(g_1^{'})f(a)$ avec $a \in i_1(N) \subset G_1$ et $g = f(g_1^{'}a) = f(g_1)$ avec $g_1 = g_1^{'}a$. Ceci montre que f est surjective.
Cette proposition montre que si on sait que G_1 et G_2 sont deux extensions de Q par N, alors ces deux extensions sont isomorphes dés qu'il existe un morphisme entre elles.

2.2 Torseurs et extensions

Si G est un groupe, un G-torseur est un ensemble E non vide muni d'une action de G sur E i.e d'une application

$$\rho : G \times E \longrightarrow E$$

notée $\rho(g, x) = gx$. De plus cette action doit être libre :

$$gx = x \Longleftrightarrow g = 1_G$$

et transitive :

$$\forall x, y \in E, \exists g \in G / y = gx$$

Pour tout $x_0 \in E$ fixé, on obtient une bijection

$$\rho_{x_0} : G \longrightarrow E$$

donnée par $g \mapsto gx_0$. En effet ρ_{x_0} est injective : si $\rho_{x_0}(g_1) = \rho_{x_0}(g_2)$, alors $g_1 x_0 = g_2 x_0$ et donc $g_1^{-1} g_2 x_0 = x_0$ et donc $g_1^{-1} g_2 = 1_G$, ce qui donne $g_1 = g_2$. De plus elle est surjective : soit $y \in E$. Par transitivité de l'action, il existe $g \in G$ tel que $y = gx_0 = \rho_{x_0}(g)$.
Dans cette bijection l'identité 1_G de G correspond à lélément x_0 de E. Donc, dés qu'on choisit un élément $x_0 \in E$, le G-torseur E s'identifie au groupe G lui-même (qui aura alors perdu son identité).

La relation avec les extensions de groupes est donnée par la proposition suivante :

Proposition 3 *: Soit* $1 \longrightarrow N \xrightarrow{i} G \xrightarrow{p} Q \longrightarrow 1$ *une extension de* Q *par* N*. Alors chaque élément de* Q *vu comme classe modulo* N *est un* N*-torseur*

Preuve : On sait que

$$\frac{G}{N} \cong Q$$

Soit $\overline{x} = \{y \in G / x \equiv y \pmod N\} = \{y \in G / yx^{-1} \in N\}$. L'action de N sur $\overline{x}$ est $\rho : N \times \overline{x} \longrightarrow \overline{x}$ donné par $(a, y) \mapsto ay$. ρ est libre : si $ay = y$, alors $a = yy^{-1} = 1_G = 1_N$ et ρ est transitive : soient $y_1, y_2 \in \overline{x}$. Donc $y_1 \equiv y_2 \pmod N$ i.e $y_{12}^{-1} y_2 = a \in N$ et donc $y_2 = ay_1$.

2.3 Extensions scindées

Le problème principal concernant les extensions de groupes est le suivant :
Problème : Etant donnés deux groupes Q et N, classifier (ou trouver) toutes les extensions de Q par N.

Pour les extensions scindées, qu'on va voir ici, ce problème admet une solution complète qui utilise les produits semidirects de groupes. Un autre type d'extensions, les extensions centrales, sera étudié au chapitre suivant. On verra que dans ce cas aussi, on a une réponse complète au problème, mais qui nécessite l'introduction de certains groupes de cohomologie.

Definition 10 *: Une extension de groupes*

$$1 \longrightarrow N \xrightarrow{i} G \xrightarrow{p} Q \longrightarrow 1$$

est dite scindée s'il existe un morphisme de groupes $s : Q \longrightarrow G$ tel que $p \circ s = Id_Q$. s est une section de l'extension.

On a déja vu que chaque classe $\overline{x}$ modulo N (pour $x \in Q$) est en bijection avec N. On peut donc dire qu'une extension est une projection $p : G \longrightarrow Q$ dans laquelle les fibres (les $p^{-1}(x)$ pour $x \in Q$) sont des N-torseurs. Une section s passe par un point de chaque fibre (ici $p(s(\overline{x})) = \overline{x}$).

Pour la commodité du lecteur, rappelons la notion de produit semidirect de groupes. Soient Q et N deux groupes et soit $\rho : Q \longrightarrow Aut(N)$ un morphisme qui va du groupe Q vers le groupe des automorphismes de N. Chaque $\rho(b)$ pour $b \in Q$ est donc un automorphisme de N :

$$\rho(b) : N \longrightarrow N$$

donné par $a \mapsto \rho(b)(a)$ pour $a \in N$. Le produit semidirect de Q par N relativement à ρ est l'ensemble $N \times Q$ muni de la loi :

$$(a, b).\rho(a^{'}, b^{'}) = (a\rho(b)(a^{'}), bb^{'})$$

On le note $N \times_\rho Q$. Montrons que c'est un groupe. On a $((a, b).\rho(a^{'}, b^{'})).\rho(a^{''}, b^{''}) = (a\rho(b)(a^{'}), bb^{'}).\rho(a^{''}, b^{''}) = (a\rho(b)(a^{'})\rho(bb^{'})(a^{''}), bb^{'}b^{''}) = (a, b).\rho(a^{'}\rho(b^{'})(a^{''}), b^{'}b^{''}) = (a, b).\rho((a^{'}, b^{'}).\rho(a^{''}, b^{''}))$. Ceci montre que $.\rho$ est associative. D'autre part on a $(a, b).\rho(1_N, 1_Q) = (a\rho(b)(1_N), b1_Q) = (a, b)$ et $(1_N, 1_Q).\rho(a, b) = (a, b)$. Donc $(1_N, 1_Q)$ est élément neutre. Enfin un calcul facile montre que l'inverse de (a, b) pour $.\rho$ est $(\rho(b^{-1})(a^{-1}), b^{-1})$.

On a des applications $i : N \longrightarrow N \times_\rho Q$, $p : N \times_\rho Q \longrightarrow Q$ et $s : Q \longrightarrow N \times_\rho Q$ donnés par $i(a) = (a, 1_Q)$, $p(a, b) = b$ et $s(b) = (1_N, b)$.

Proposition 4 *: Ces applications font de $N \times_\rho Q$ une extension scindée de Q par N*

Preuve : Il faut montrer que ces trois applications sont des morphismes de groupes, que i est injective, que p est surjective, que $Kerp \cong Im(i)$ et que $p \circ s = Id_Q$. On a $i(aa^{'}) = (aa^{'}, 1_Q) = (a, 1_Q).\rho(a, 1_Q) = i(a)i(a^{'})$ et donc i est bien un morphisme. De même $p((a, b), (a^{'}, b^{'})) = p(a\rho(b)(a^{'}), bb^{'}) = bb^{'} =$

$p(a,b)p(a^{'},b^{'})$ et p est donc un morphisme. Enfin on a $s(bb^{'}) = (1_N, bb^{'}) = (1_N, b).{}_\rho(1_N, b^{'}) = s(b).{}_\rho s(b^{'})$ et s est donc aussi un morphisme. D'autre part on a $i(a) = (1_N, 1_Q)$ implique que $(a, 1_Q) = (1_N, 1_Q)$ et donc $a = 1_N$, ce qui montre que i est injective. Soit$b \in Q$. On a toujours $p(1_N, b) = b$ et donc p est surjective. Si $(a, b) \in Kerp$, on doit avoir $p(a, b) = 1_Q$. Donc $b = 1_Q$ et $(a, b) = (a, 1_Q) = i(a) \in Im(i)$. D'autre part $p(a, 1_Q) = 1_Q$, donc $p(i(a)) = 1_Q$ i.e $i(a) \in Kerp$. Ceci montre que $Kerp \cong Im(i)$. Il nous reste à montrer que s est une section. On a $(p \circ s)(b) = p(s(b)) = p(1_N, b) = b$ pour tout $b \in Q$. Donc $p \circ s = Id_Q$.

Cette proposition montre donc que tout produit semidirect est une extension scindée. Inversement nous allons montrer que toute extension scindée est un produit semidirect. Soit donc

$$1 \longrightarrow N \xrightarrow{i} G \xrightarrow{p} Q \longrightarrow 1$$

une extension scindée. Définissons

$$\rho : Q \longrightarrow Aut(N)$$

par $\rho(b)(a) = s(b)as(b)^{-1}$ (on suppose comme convenu que $N = i(N) \subset G$). Comme N est normal dans G, $s(b)as(b)^{-1} \in N$ si $a \in N$ et donc ρ est bien définie. Du coup on obtient l'extension scindée

$$1 \longrightarrow N \xrightarrow{i^{'}} N \times_\rho Q \xrightarrow{p^{'}} Q \longrightarrow 1$$

avec la section $s^{'} : Q \longrightarrow N \times_\rho Q$ donnée par $s^{'}(b) = (1_N, b)$.

Proposition 5 *: Il existe un unique isomorphisme $f : N \times_\rho Q \longrightarrow G$ tel que $f \circ s^{'} = s$:*

$$\begin{array}{ccccccccc} 1 & \longrightarrow & N & \xrightarrow{i^{'}} & N \times_\rho Q & \xrightarrow{p^{'}} & Q & \longrightarrow & 1 \\ & & \| & & f\downarrow & & \| & & \\ 1 & \longrightarrow & N & \xrightarrow{i} & G & \xrightarrow{p} & Q & \longrightarrow & 1 \end{array}$$

Preuve : Définissons $f : N \times_\rho Q \longrightarrow G$ par $f(a, b) = as(b)$. Montrons que f est un morphisme de groupes : On a $f((a, b).{}_\rho(a^{'}, b^{'}) = f(a\rho(b)(a^{'}), bb^{'}) = f(as(b)a^{'}s(b)^{-1}, bb^{'}) = as(b)a^{'}s(b)^{-1}s(b)s(b^{'}) = as(b)a^{'}s(b^{'}) = f(a, b)f(a^{'}, b^{'})$. Si $f(a, b) = 1_G$, on doit avoir $as(b) = 1_G$. Donc $p(as(b)) = 1_Q$ i.e $p(a)p(s(b)) =$

1_Q. Comme $p(a) = 1_Q$ et $p(s(b)) = b$, ceci donne $b = 1_Q$ et $a = 1_N = 1_G$. f est donc injective. Soit $g \in G$ et soit $b = p(g)$. On a $p(s(b)) = b = p(g)$. Donc $p(gs(b)^{-1}) = 1_Q$ i.e $gs(b)^{-1} \in Kerp \cong Im(i)$. Il existe donc $a \in N$ tel que $gs(b)^{-1} = a$ et donc $g = as(b) = f(a, b)$, ce qui montre que f est aussi surjective. Enfin montrons que $f \circ s^{'} = s$. On a $f(s^{'}(b)) = f(1_N, b) = s(b)$.

En résumé on obtient le :

Théorème 1 *: Toute extension scindée de Q par N est de la forme $N \times_\rho Q$ pour un certain $\rho : Q \longrightarrow Aut(N)$.*

Preuve : Immédiate d'aprés la discussion précédente.

Chapitre 3

Extensions centrales et cohomologie

Dans ce chapitre on étudie un autre type d'extensions appelées extensions centrales. On verra qu'ici aussi le problème de la classification a une solution complète qui fait intervenir certains groupes dits de cohomologie. La définition de ces groupes n'est pas facile et nécessite un bagage mathématique qui dépasse le niveau de ce mémoire. Mais en nous concentrant sur le H^2, le seul groupe qui nous interesse ici, on arrive à contourner ce problème et à en donner une définition directe via les 2-cocycles et les 2-cobords. La classification des extensions centrales est faite en associant à chaque extension une classe de cohomologie et en fabriquant à partir de chaque classe de cohomologie une extension centrale. Remarquons enfin que comme le noyau d'une extension centrale est abélien, on est dans le cadre de la cohomologie abélienne et qu'on ne touche nullement à la cohomologie non abélienne qui reste un domaine de recherche assez difficile.

3.1 Extensions centrales

Soit $1 \longrightarrow N \longrightarrow G \longrightarrow Q \longrightarrow 1$ une extension de groupes et soit $Z(G)$ le centre de G :

$$Z(G) = \{z \in G / zg = gz, \forall g \in G\}$$

C'est le sous-groupe des éléments de G qui commutent avec tout élément de G.

Definition 11 *: L'extension précédente est dite centrale si* $N \subseteq Z(G)$.

Remarquer que $Z(G)$ est automatiquement un sous-groupe abélien et donc N est aussi abélien. Une extension scindée et centrale est nécessairement triviale comme le montre la proposition suivante :

Proposition 6 *: L'extension scindée* $1 \longrightarrow N \longrightarrow G \longrightarrow Q \longrightarrow 1$ *est centrale si et seulement si elle est triviale i.e que* $G = N \times Q$ *est un produit direct.*

Preuve : Soit $1 \longrightarrow N \longrightarrow G \longrightarrow Q \longrightarrow 1$ une extension scindée. On sait que $G = N \times_\rho Q$ pour un certain $\rho : Q \longrightarrow Aut(N)$. L'extension sera centrale si et seulement si $N \subseteq Z(G) = Z(N \times_\rho Q)$. Tout élément $(c, 1_Q)$ de N doit donc commuter avec tout élément (a, b) de $N \times_\rho Q$ pour la loi $._\rho$ (ici on identifie N à $i(N)$ i.e $c \in N$ à $(c, 1_Q) \in i(N)$). On doit donc avoir

$$(c, 1_Q)._\rho(a, b) = (a, b)._\rho(c, 1_Q)$$

pour tout $c \in N$ et tout $(a, b) \in N \times_\rho Q$. Mais on a

$$(c, 1_Q)._\rho(a, b) = (c\rho(1_Q)(a), 1_Q b) = (ca, b)$$

et

$$(a, b)._\rho(c, 1_Q) = (a\rho(b)(c), b1_Q) = (a\rho(b)(c), b)$$

ce qui donne

$$(ca, b) = (a\rho(b)(c), b)$$

pour tous $c, a \in N$ et tout $b \in Q$. En prenant $a = 1_N$, cette dernière égalité donne

$$\rho(b)(c) = c$$

pour tout $c \in N$ et tout $b \in Q$. Donc $\rho(b) = Id_N$ pour tout $b \in Q$ et le produit semidirect $N \times_\rho Q$ n'est autre que le produit direct $N \times Q$ qui correspond à l'extension triviale.

3.2 Cohomologie des groupes

Soit G un groupe quelconque et soit A un groupe abélien. Un 2-cocycle sur G à coefficients dans A est une fonction :

$$c : G \times G \longrightarrow A$$

telle que

$$c(g_1, g_2) - c(g_1, g_2.g_3) + c(g_1.g_2, g_3) - c(g_2, g_3) = 0 \in A$$

pour tous $g_1, g_2, g_3 \in G$ (condition de 2-cocycle).

Pour $c, \tilde{c}$ deux cocycles,un cobord $h : c \longrightarrow \widetilde{c}$ entre eux est une fonction :

$$h : G \longrightarrow A$$

telle qu'on ait :

$$\tilde{c}(g_1, g_2) = c(g_1, g_2) + (dh)(g_1, g_2)$$

avec

$$(dh)(g_1, g_2) = h(g_1 g_2) - h(g_1) - h(g_2)$$

pour tous $g_1, g_2 \in G$. dh est le 2-cobord défini par h. Les 2-cocycles forment un groupe abélien (pour l'addition des fonctions) $C(G, A)$ et les 2-cobords forment un sous-groupe $B(G, A) \subseteq C(G, A)$.

Definition 12 *:Le 2-groupe de cohomologie de G à coefficients dans A est le groupe quotient :*

$$H^2(G, A) = \frac{C(G, A)}{B(G, A)}$$

Les éléments de $H^2(G, A)$ sont donc les classes d'équivalence de 2-cocycles modulo les 2-cobords. $H^2(G, A)$ est un groupe abélien. Si $[c]$ est la classe du deux cocycle c, on a

$$[c_1] + [c_2] = [c_1 + c_2]$$

avec

$$(c_1 + c_2)(g_1, g_2) = c_1(g_1, g_2) + c_2(g_1, g_2)$$

Pour tout 2-cocycle c, on a

$$c(1_G, g) = c(1_G, 1_G) = c(g, 1_G)$$

ce que l'on peut vérifier facilement en utilisant la condition de cocycle.

Definition 13 *: Un 2-cocycle c est dit normalisé si*

$$c(1_G, g) = c(1_G, 1_G) = c(g, 1_G) = 0_A$$

pour tout $g \in G$.

Tout cocycle c est équivalent (modulo les cobords) à un cocycle normalisé. En effet soit c un cocycle et soit $h : G \longrightarrow A$ le cobord donné par $h(g) = c(g, g)$. Alors $\tilde{c} = c + dh$ est un cobord normalisé équivalent à c :

$$\tilde{c}(1_G, 1_G) = (c + dh)(1_G, 1_G)$$

$$= c(1_G, 1_G) + c(1_G.1_G, 1_G.1_G) - c(1_G, 1_G) - c(1_G, 1_G)$$

$$= 0_A$$

3.3 Classification par le H^2

Soit

$$1 \longrightarrow N \longrightarrow G \longrightarrow Q \longrightarrow 1$$

une extension centrale. Donc $N \subseteq Z(G)$ est un groupe abélien et on peut parler de $H^2(Q, N)$. Nous allons montrer ici que les (classes d'isomorphismes d') extensions centrales de Q par N sont classifiées par les éléments de $H^2(Q, N)$. Autrement dit chaque extension centrale définit une classe de cohomologie et inversement à chaque classe de cohomologie correspond une extension centrale.

Soit$[c] \in H^2(Q, N)$ une classe de cohomologie réprésentée par le 2-cocycle $c : Q \times Q \longrightarrow N$ qu'on peut supposer être normalisé. Définissons un groupe $Q \times_c N$ de le manière suivante : $Q \times_c N = Q \times N$ en tant qu'ensemble avec l'opération :

$$(b_1, a_1) \cdot (b_2, a_2) = (b_1 b_2, a_1 + a_2 + c(b_1, b_2))$$

Proposition 7 *: Cette opération fait de $Q \times_c N = Q \times N$ un groupe.*

Preuve : Comme N est abélien, sa notation sera additive. On vérifie facilement que $(1_Q, 0_N)$ est élément neutre (avec $0_N = 1_N$). Montrons l'associativité. On a

$$((b_1, a_1) \cdot (b_2, a_2)) \cdot (b_3, a_3) = (b_1 b_2 b_3, a_1 + a_2 + a_3 + c(b_1, b_2) + c(b_1 b_2, b_3))$$

et

$$(b_1, a_1) \cdot ((b_2, a_2) \cdot (b_3, a_3)) = (b_1 b_2 b_3, a_1 + a_2 + a_3 + c(b_2, b_3) + c(b_1, b_2 b_3))$$

et la différence entre les deux expressions est exactement

$$(1_Q, 0_N)$$

(en utilisant la définition d'un cocycle) qui sont donc égales. Enfin un calcul facile montre que l'inverse de (b, a) est $(b^{-1}, -a - c(b, b^{-1}))$.

Proposition 8 *: $Q \times_c N$ est une extension centrale de Q par N qui ne dépend que de la classe $[c]$ de c.*

Preuve : Définissons

$$i : N \longrightarrow Q \times_c N$$

et

$$p : Q \times_c N \longrightarrow Q$$

en posant $i(a) = (1_Q, a)$ et $p(b, a) = b$ pour tout $a \in N$ et tout $b \in Q$. Ce sont là deux morphismes de groupes. De plus on a $p(b, a) = 1_Q$ si et seulement si $b = 1_Q$, ce qui montre que $Kerp \cong Im(i)$. On obtient donc une extension

$$1 \longrightarrow N \xrightarrow{i} Q \times_c N \xrightarrow{p} Q \longrightarrow 1$$

Cette extension est centrale. En effet on a (en supposant toujours c normalisé) :

$$(b, a).(1_N, a^{'}) = (b, a + a^{'} + 0) = (1_N, a^{'}).(b, a)$$

(On identifie $a^{'} \in N$ à $i(a^{'}) = (1_N, a^{'}) \in Q \times_c N$). Il nous reste à montrer que toute cette construction ne dépend que de la classe de c et non pas de c lui-même. Soit $\tilde{c}$ un 2-cocycle équivalent à c. On a donc

$$\tilde{c}(b_1, b_2) = c(b_1, b_2) - h(b_1) - h(b_2) + h(b_1 b_2)$$

avec $h : Q \longrightarrow N$ un cobord. Comme c, $\tilde{c}$ définit une extension :

$$1 \longrightarrow N \xrightarrow{\tilde{i}} Q \times_{\tilde{c}} N \xrightarrow{\tilde{p}} Q \longrightarrow 1$$

Soit

$$f : Q \times_c N \longrightarrow Q \times_{\tilde{c}} N$$

l'application donnée par

$$f = (Id_Q, \tilde{p} - h \circ p)$$

i.e

$$f(b,a) = (b, a - h(b))$$

Il faut montrer que f est un morphisme (et donc un isomorphisme). On a

$$f(b_1,a_1).f(b_2,a_2) = (b_1, a_1 - h(b_1).(b_2, a_2 - h(b_2)$$

$$= (b_1b_2, a_1 + a_2 - h(b_1) - h(b_2) + c(b_1,b_2))$$

$$= (b_1b_2, a_1 + a_2 + \tilde{c}(b_1,b_2) - h(b_1,b_2))$$

$$= f((b_1,a_1).(b_2,a_2))$$

En mettant les deux dernières propositions cote à cote, on aura donc montré que toute classe de cohomologie $[c]$ dans $H^2(Q,N)$ définit une extension centrale $Q \times_c N$ de Q par N.

Inversement soit

$$1 \longrightarrow N \xrightarrow{i} G \xrightarrow{p} Q \longrightarrow 1$$

une extension centrale. Soit $s : Q \longrightarrow G$ une section ensembliste de p (qui existe toujours puisque p est surjective). Autrement dit, $s(b) = g$ si $p(g) = b$. Soit $c : Q \times Q \longrightarrow N$ le cocycle défini par

$$c(b_1,b_2) = s(b_1)^{-1}s(b_2)^{-1}s(b_1b_2)$$

Que cela soit un cocycle découle directement de la définition de c. Il faut juste nous assurer que si on change de section alors le cocycle obtenu est équivalent au premier (modulo les cobords). Or si $s' : Q \longrightarrow G$ est une autre section de p et si on pose $h(b) = s'(b)s(b)^{-1}$, on aura automatiquement $\tilde{c} - c = dh$ avec $\tilde{c}$ le cocycle donné par s'. Toute extension centrale définit donc une classe de cohomologie.

On peut résumer tout cela dans le

Théorème 2 *: Les (classes d'isomorphismes d') extensions centrales de Q par N sont en bijection avec les éléments (les classes de cohomologie) de $H^2(Q,N)$.*

Bibliographie

[1] S.Lang, Algebra, third edition, Springer, 2002.

[2] N.Bourbaki, Eléments de Mathématiques, Algèbre, Hermann, Paris, 1965.

[3] D.J.S Robinson, A course in the Theory of Groups, Springer-Verlag, 1982.

[4] S.Eilenberg and S.Maclane, Group Extensions and Homology, Annals of Mathematics, vol.48, No.4, October, 1942.