ELEMENTS DE LA THEORIE DES GROUPES.

Licence de Mathématiques
Université d'Angers
1997/98

D. Schaub

Table des matières

Chapitre 1

GENERALITES

1.1 Définition

Définition 1.1.1 *Soit G un ensemble non vide et $* : G \times G \to G,\ (a,b) \mapsto a*b$ une application. $(G,*)$ est un groupe si :*
a) $*$ est associative ie. $\forall a,b,c \in G,\ a*(b*c) = (a*b)*c$;
b) G possède un élément neutre e pour $*$ càd. $\exists e \in G,\ \forall a \in G,\ a*e = e*a = a$;
c) tout $a \in G$ admet un symétrique ie. $\forall a \in G,\ \exists b \in G,\ a*b = b*a = e$.

Exemples :1) $\mathbb{Z}$,$\mathbb{Q}$, $\mathbb{R}$,$\mathbb{C}$ avec l'addition sont des groupes, de même que $\mathbb{Q}^*$, $\mathbb{R}^*$,$\mathbb{C}^*$ pour la multiplication.

2) Si E est un ensemble, l'ensemble $S(E)$ des bijections de E dans E, muni de la composition des applications est un groupe, appelé groupe symétrique de E. Si E n'a qu'un nombre fini n d'éléments, on note S_n le groupe symétrique de E et ses éléments sont appelés *permutations*.

Si, de plus, la loi $*$ est *commutative* (ie. $\forall a,b \in G,\ a*b = b*a$), alors on dit que G est un groupe *commutatif* ou *abélien*.

Les exemples 1) ci-dessus sont des groupes abéliens, mais S_n n'est pas commutatif dès que $n \geq 3$.

Notations : En général, on convient de noter (autant que possible) $+$ la loi lorsqu'elle est commutative, $\times$ ou $\cdot$ sinon.

Lorsque G est un groupe *fini* (càd. de cardinal fini), il peut être commode de dresser la table de ce groupe. Ainsi si $G = \{a_1, \ldots, a_n\}$ la table s'écrit :

$$\begin{array}{ccccc} * & a_1 & a_2 & \cdots & a_n \\ a_1 & a_1a_1 & a_1a_2 & \cdots & a_1a_n \\ a_2 & a_2a_1 & a_2a_2 & \cdots & a_2a_n \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ a_n & a_na_1 & a_na_2 & \cdots & a_na_n \end{array}$$

Exercices : i) Dresser la table du groupe Q_2 des quaternions, où $Q_2 = \{1,-1,i,-i,j,-j,k,-k\}$ avec $i^2 = j^2 = k^2 = -1$ et $ij = k$.

ii) Soit $E = \{1,2,\ldots,n\}$ et $S_n = S(E)$. Une permutation $s \in S_n$ peut se noter :

$$s = \begin{pmatrix} 1 & 2 & \ldots & n-1 & n \\ s(1) & s(2) & \ldots & s(n-1) & s(n) \end{pmatrix}.$$

Par exemple : si $E = \{1,2,3\}$, S_3 contient 6 éléments qui sont $\mathrm{Id} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$, $\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$, $\sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$, $\tau_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$, $\tau_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$, $\tau_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$. Dresser la table de S_3.

Propriétés immédiates :

a) l'élément neutre d'un groupe est unique $(e' = e' * e = e * e' = e)$;
b) le symétrique d'un élément a est unique $(b = (b'a)b = b'(ab) = b')$;
c) $\forall a, b \in G,\ (ab)^{-1} = b^{-1}a^{-1}$;
d) l'équation $ax = b$ a une et une seule solution $x = a^{-1}b$.

1.2 Sous-groupes

Définition 1.2.1 *Soit $H \subset G$ un sous-ensemble non vide. On dit que H est un sous-groupe de G si i) $a, b \in H \Rightarrow ab \in H$; ii) $a \in H \Rightarrow a^{-1} \in H$, on notera $H < G$.*

Les conditions i) et ii) sont évidemment équivalentes à l'unique condition $a, b \in H \Rightarrow ab^{-1} \in H$.

Exemple : S_3 possède 6 sous-groupes $\{\mathrm{Id}\}, \{\mathrm{Id}, \tau_k\}, k = 1,2,3, A_3 = \{\mathrm{Id}, \sigma_1, \sigma_2\}, S_3$.

Un critère qui peut se révéler intéressant lorsque l'emploi de la définition est pénible :

Lemme 1.2.1 *Toute partie stable finie H d'un groupe G est un sous-groupe de G.*

Preuve : Pour tout $h \in H$, l'application $H \to H$, $x \mapsto hx$ est injective, donc (puisque H est fini) surjective et, de même pour l'application $x \mapsto xh$. Mais $h \in H$ et la surjectivité implique qu'il existe $x \in H$ tel que $hx = h$ et y tel que $yh = h$, d'où $x = y = e \in H$. De même, il existe $x \in H$ tel que $hx = e$ (et y tel que $yh = e$), donc $h^{-1} = x = y \in H$.

Attention : ce lemme n'est plus vrai lorsque H n'est pas fini ! (exemple : $\mathbb{N} \subset \mathbb{Z}$).

Lemme 1.2.2 *Les sous-groupes additifs de $\mathbb{Z}$ sont de la forme $n\mathbb{Z}$, $n \in \mathbb{N}$.*

Preuve : $n\mathbb{Z}$ est clairement un sous-groupe de $\mathbb{Z}$. Inversement, soit H un sous-groupe de $\mathbb{Z}$. Si $H = \{0\}$, alors $H = 0\mathbb{Z}$. Sinon, soit $n > 0$ le plus petit tel que $n \in H$ et soit $h \in H$. Alors, par division euclidienne, on peut écrire $h = nq + r$, avec $0 \leq r < n$. Mais $r = h - nq \in H$, donc si $r \neq 0$, il y a contradiction avec la minimalité de n, d'où $r = 0$ et $h = nq$, càd. $H \subset n\mathbb{Z}$. L'inclusion inverse étant immédiate, $H = n\mathbb{Z}$.

Lemme 1.2.3 *L'intersection d'une famille de sous-groupes H_i, $i \in I$ d'un groupe G est un sous-groupe de G.*

Preuve : Soit $H = \cap_{i \in I} H_i$, $a, b \in H \Rightarrow a, b \in H_i, \forall i \Rightarrow ab^{-1} \in H_i, \forall i \Rightarrow ab^{-1} \in H$.

Attention : la réunion de 2 sous-groupes n'est pas, en général, un sous-groupe (sauf dans le cas d'inclusion de l'un dans l'autre).

Définition 1.2.2 *Soient A, B deux sous-ensembles non vides d'un groupe G, on pose : $A \cdot B = \{ab | a \in A, B \in B\}$.*

Remarque : Si H est un sous-groupe, alors $H \cdot H = H$.

Lemme 1.2.4 *Soit $H < G$ un sous-groupe et $a, b \in G$. Alors a) $Ha = H$ ssi $a \in H$; b) $Ha = Hb$ ssi $ab^{-1} \in H$ (et $aH = bH \Leftrightarrow a^{-1}b \in H$).*

Preuve : a) pour tout $h \in H$, on a $ha = h' \Rightarrow a = h^{-1}h' \in H$ et inversement $a \in H \Rightarrow ha \in H, \forall h \in H$.

b) $Ha = Hb \Rightarrow \forall h \in H, \exists h' \in H, ha = h'b$, d'où $ab^{-1} = h^{-1}h' \in H$ et ; inversement, $ab^{-1} \in H \Rightarrow$ (par a) $Hab^{-1} = H$, d'où $Ha = Hb$.

1.3 Relations d'équivalences

Soit H un sous-groupe d'un groupe G. On définit sur G une relation d'équivalence, appelée *relation d'équivalence à gauche (resp. à droite) associée à* H, par :

$$a \equiv_g b \text{ modulo } H \Leftrightarrow ab^{-1} \in H$$

$$(\text{resp. } a \equiv_d b \text{ modulo } H \Leftrightarrow a^{-1}b \in H).$$

Rappelons qu'une relation d'équivalence sur un ensemble est réflexive, symétrique et transitive. On vérifie immédiatement que la relation $\equiv_g$ (ou $\equiv_d$) est bien une telle relation.

La *classe à gauche de* a pour cette relation est l'ensemble des $b \in G$ qui sont liés à a par $\equiv_g$ mod. H, càd. l'ensemble $\{b \in G | b \equiv_g a \text{ mod. } H\} = \{b \in G | ba^{-1} \in H\} = Ha$ (de même, la classe à droite de a est aH).

Lemme 1.3.1 *1)* $Ha \cap Hb \neq \emptyset \Rightarrow Ha = Hb$ *(id. pour les classes à droite) ;*
2) $b \not\in Ha \Rightarrow Ha \cap Hb = \emptyset$.

Preuve : Soit $x \in Ha \cap Hb$, alors $x \equiv_g a$ et $x \equiv_g b$, d'où $a \equiv_g b \Rightarrow Ha = Hb$. Et 2) n'est qu'une reformulation de 1).

L'ensemble des classes à gauche $(G/H)_g$ est le quotient de G par cette relation d'équivalence (et de même pour $(G/H)_d$).

Exemples : 1) La classe à gauche (ou à droite) de e mod.H est H.

2) Si $G = S_3$ et $H = \{\text{Id}, \tau_1\}$, alors la classe à gauche de Id, c'est H, la classe de σ_1, $H\sigma_1 = \{\sigma_1, \tau_1\sigma_1 = \tau_2\}$, la classe à droite de σ_1, $\sigma_1 H = \{\sigma_1, \sigma_1\tau_1 = \tau_3\}$. Les classes à gauche et à droite sont donc distinctes. Ce qui est en général le cas.

Lemme 1.3.2 *Soit* $H < G$ *un sous-groupe. Il existe une bijection de l'ensemble des classes à droite modulo* H *sur l'ensemble des classes à gauche modulo* H*. D'où* $|(G/H)_d| = |(G/H)_g|$ *(où l'on note* $|X|$ *le cardinal de l'ensemble* X*).*

Preuve : Il faut d'abord définir une *application* de $(G/H)_d$ dans $(G/H)_g$. Soit donc xH une classe à droite, associons-lui la classe à gauche Hx^{-1}. Cette correspondance est une application. En effet, si on prend 2 représentants de la classe xH (ie. 2 éléments de xH), x et x', alors $xH = x'H$. La correspondance définie ci-dessus fait correspondre à xH aussi bien Hx^{-1} que Hx'^{-1}. Pour qu'elle soit une application, il faut que ces 2 classes à gauche coincident, autrement dit que $x \equiv_g x'$.

Or $x \equiv_d x'$, d'où $x^{-1}x' \in H$ ou encore $x'^{-1}x \in H \Rightarrow x'^{-1} \in Hx^{-1}$, donc $Hx^{-1} = Hx'^{-1}$.

Cette application est clairement bijective, d'où le résultat.

Définition 1.3.1 *Le cardinal de l'ensemble des classes à gauche modulo* H *(= cardinal de l'ensemble des classes à droite) est appelé indice de* H *dans* G *et noté* $[G : H]$.

On a donc $[G : H] = |(G/H)_d| = |(G/H)_g|$.

Exemple : Si $G = S_3$ et $H = \{\mathrm{Id}, \tau_1\}$, alors $[S_3 : H] = 3$. En fait, σ_1, τ_3 appartiennent à la même classe $\{\sigma_1, \tau_3\}$, de même pour σ_2, τ_2 et Id, τ_1.

Définition 1.3.2 *On appelle ordre d'un groupe G son cardinal, qu'on note $|G|$.*

Ainsi $\mathbb{Z}$,$\mathbb{Q}, \ldots$ sont d'ordre infini, tandis que $|S_3| = 6$ et, plus généralement $|S_n| = n!$, $|Q_2| = 8$.

1.4 Théorème de Lagrange

Théorème 1.4.1 *L'ordre $|H|$ d'un sous-groupe H d'un groupe fini G divise l'ordre $|G|$ de G. L'indice $[G : H]$ divise aussi $|G|$ et*

$$[G : H] = |G|/|H|.$$

Preuve : G est clairement la réunion disjointes des Hx (en effet : tout élément x de G appartient au moins à Hx et $Hx \cap Hy = \emptyset$ ou $Hx = Hy$). D'où $|G| = \sum |Hx|$.

De plus, $|Hx| = |H|$, pour tout x, car l'application $H \to Hx$, $h \mapsto hx$ est bijective, d'où $|Hx| = |Hy|$, pour tous $x, y \in G$ et la somme ci-dessus est égale au nombre de classes fois $|H|$, ce qui est précisément la formule cherchée.

Conséquence : si n ne divise pas $|G|$, alors il n'existe pas de sous-groupe de G d'ordre n. (MAIS ! ! ! si n divise $|G|$, il n'existe pas nécessairement de sous-groupe d'ordre n. Exemple : A_4, qui est d'ordre 12, n'a pas de sous-groupe d'ordre 6.

Corollaire 1.4.1 *Soient H, H' deux sous-groupes d'un groupe fini G, $H \subset H'$, alors $[G : H] = [G : H'][H' : H]$.*

La preuve est immédiate :

$$[G : H] = |G|/|H| = \frac{[G : H']|H'|}{|H|} = [G : H']\frac{|H'|}{|H|} = [G : H'][H' : H].$$

Corollaire 1.4.2 *Soient H, K 2 sous-groupes d'un groupe fini G, alors*

$$|HK| = \frac{|H||K|}{|H \cap K|}.$$

Preuve : Notons $I = H \cap K$, c'est un sous-groupe de K. Alors $(K/I)_g = \{Ik_1, \ldots, Ik_n\}$ sont les classes à gauche de K modulo I. Je prétends que HK est la réunion disjointe des Hk_i.

En effet : d'une part, $hk \in HK$ et k peut s'écrire $k = \lambda k_j, \lambda \in I \subset H$ (puisque K est la réunion des Ik_j), d'où $hk = (h\lambda)k_j \in Hk_j$.

D'autre part, $Hk_i \cap Hk_j \neq \emptyset \Rightarrow \exists h, h' \in H$ tel que $hk_i = h'k_j$, d'où $h'^{-1}h = k_j k_i^{-1} \in H \cap K = I$ et donc $k_j \in Ik_i$. Or deux classes ont une intersection vide.

Enfin, comme ci-dessus, $|Hk_i| = |H| = |Hk_j|$, donc

$$|HK| = n|H| = \frac{|K|}{|I|}|H| = \frac{|K|}{|H \cap K|}|H|.$$

1.5 Sous-groupes distingués

On a vu que si $H = \{\mathrm{Id}, \tau_1\} < S_3$, alors $\sigma_1 H \neq H\sigma_1$. Regardons à présent $H = A_3 = \{\mathrm{Id}, \sigma_1, \sigma_2\}$, le groupe alterné de 3 éléments. On constate immédiatement que, pour tout $s \in S_3$, on a $A_3 s = sA_3$ (par exemple : si $s = \tau_1$, $A_3 s = \{\tau_1, \tau_2, \tau_3\} = sA_3$. On dira que A_3 est un sous-groupe distingué.

Définition 1.5.1 *Un sous-groupe H de G est distingué (on note $H \lhd G$) si pour tout $g \in G$, $Hg = gH$ (on dit aussi : invariant ou normal).*

Remarques : 1) Evidemment, dans un groupe *commutatif*, tout sous-groupe est distingué.

2) Attention : $Hg = gH$ ne signifie pas : $\forall h \in H,\ hg = gh$, mais $\exists h' \in H,\ hg = gh'$.

3) Si $H \lhd G$, alors $(G/H)_g = (G/H)_d$ et on notera simplement G/H. Inversement, si $(G/H)_g = (G/H)_d$, alors $H \lhd G$ (en effet : gH est une classe à droite, donc aussi à gauche et contient g, donc est nécessairement Hg ie. $gH = Hg$).

Lemme 1.5.1 *Tout sous-groupe d'indice 2 est distingué.*

Preuve : Si l'indice est 2, cela signifie qu'il n'y a que 2 classes (à gauche ou à droite), autrement dit : $(G/H)_g = \{H, G - H\} = (G/H)_d$.

Lemme 1.5.2 *Les conditions suivantes sont équivalentes : a) $H \lhd G$, b) $\forall x \in G,\ xH = Hx$, c) $\forall x \in G,\ xH \subset Hx$, d) $\forall x \in G,\ xHx^{-1} = H$, e) $\forall x \in G,\ xHx^{-1} \subset H$.*

Preuve : a $\Leftrightarrow$ b $\Rightarrow$ c, d $\Rightarrow$ e et b $\Rightarrow$ d sont clairs.

c $\Rightarrow$ e : $xH \subset Hx \Rightarrow (xh)x^{-1} = h'xx^{-1} = h' \in H \Rightarrow xHx^{-1} \subset H$.

e $\Rightarrow$ b $xh = (xh'x^{-1})x = h'x \in Hx \Rightarrow xH \subset Hx$ et on montre de même que $Hx \subset xH$.

On a envie de définir sur $(G/H)_d$ (ou $(G/H)_g$) une structure "naturelle" de groupe.

Notons $\pi_g : G \to (G/H)_g,\ x \mapsto Hx$ et $\pi_d : G \to (G/H)_d$ les surjections canoniques (lorsque $H \lhd G$, $\pi_g = \pi_d$).

Tout élément de $\pi_g^{-1}(Hx)$ (resp. $\pi_d^{-1}(Hx)$) *représente* la classe Hx (en particulier x représente Hx), mais, bien entendu, il y a plusieurs représentants d'une même classe (en général). Ainsi : x et x' représentent la même classe à gauche ssi $x'x^{-1} \in H$.

Par structure "naturelle", on entend que π_g (resp. π_d) vérifient $\forall x, y \in G,\ \pi_g(xy) = \pi_g(x)\pi_g(y)$ $(*)$ ie. $(Hx)(Hy) = Hxy$ (et l'analogue à droite). On a le :

Théorème 1.5.1 $(*)$ *définit une structure de groupe sur $(G/H)_g$ ssi $H \lhd G$.*

Preuve : $\Leftarrow$ Supposons $H \lhd G$, alors l'application $(G/H)_g \times (G/H)_g \to (G/H)_g$ donnée par $(Hx, Hy) \mapsto Hxy$ est bien définie. A priori, elle est définie par le choix de représentants x et y de Hx et Hy, il s'agit donc de vérifier que le choix d'autres représentants définit la même image. Soient donc x', y' d'autres représentants de Hx, Hy respectivement.

Mais, x, x' représentent la même classe ssi $\exists h,\ x' = hx$ et, de même, $\exists k,\ y' = ky$. D'où $x'y' = h(xk)y = h(h'x)y = hh'xy$, donc $Hxy = Hx'y'$. Et, par conséquent, l'application est bien définie.

Que $(*)$ confère alors une structure de groupe est clair : l'associativité est assurée par $(HxHy)Hz = (Hxy)Hz = H(xy)z = Hxyz = Hx(HyHz)$, l'élément neutre est H et le symétrique de Hx est Hx^{-1}.

$\Rightarrow$ Si $(*)$ donne à $(G/H)_g$ une structure de groupe, alors, $\forall x \in G, h \in H,\ \pi_g(xhx^{-1}) = \pi_g(x)\pi_g(h)\pi_g(x^{-1}) = \pi_g(x)\pi_g(x)^{-1} = H$, d'où $xhx^{-1} \in H$, et donc $H \lhd G$.

Remarque : i) Si la notation est additive, alors $(*)$ s'écrit : $(H + x) + (H + y) = (H + x + y)$.

ii) Si G est commutatif et $H < G$, alors G/H est un groupe commutatif.

Définition 1.5.2 *Lorsque $H \triangleleft G$, on dit que $(G/H, *)$ est le groupe quotient de G par H.*

Exemples : 1) $n\mathbb{Z} \triangleleft \mathbb{Z}$, le groupe quotient est $(\mathbb{Z}/n\mathbb{Z}, +)$.
2) $A_3 \triangleleft S_3$, le quotient est $S_3/A_3 \cong \mathbb{Z}/2\mathbb{Z}$.

1.6 Homomorphismes, isomorphismes

1.6.1 Homomorphismes

Définition 1.6.1 *Une application $f : G \to G'$ d'un groupe G dans un groupe G' est un homomorphisme de groupes si $\forall x, y, \in G,\ f(|xy|) = f(|x|)f(|y|)$.*

Attention aux confusions de notations. Si les lois des groupes sont notées ainsi $(G, \top)$ et $(G', \perp)$, alors la condition s'écrit $f(x \top y) = f(x) \perp f(y)$.

Ainsi, en notation additive, elle devient $f(x+y) = f(x)+f(y)$. En particulier, si la première est notée $\cdot$ et la deuxième $+$, par exemple : $\log : (\mathbb{R}^*, \cdot) \to (\mathbb{R}, +)$, on a $\log(xy) = \log(x)+\log(y)$. log est donc un homomorphisme de groupes.

Exemples fondamentaux : 1) Si $H < G$, l'injection canonique $H \to G,\ x \mapsto x$ est un homomorphisme de groupes.

2) Si $H \triangleleft G$, la surjection canonique $\pi : G \to G/H$ est un homomorphisme de groupes (c'est d'ailleurs ainsi qu'on a muni G/H de sa structure de groupe quotient ; $(*)$ n'est rien d'autre que la condition voulue).

Lemme 1.6.1 *Si $f : G \to G'$ est un homomorphisme de groupes, alors l'image par f du neutre e de G est le neutre e' de G' et $\forall x \in G,\ f(x)^{-1} = f(x^{-1})$.*

Preuve : $f(e)f(e) = f(ee) = f(e) = f(e)e' \Rightarrow f(e) = e'$. Et si $x \in G,\ f(x)f(x^{-1}) = f(xx^{-1}) = f(e) = e'$.

Si $f : G \to G'$ et $g : G' \to G$" sont des homomorphismes de groupes, alors $g \circ f : G \to G$" est un homomorphisme de groupes.

1.6.2 Image, noyau d'un homomorphisme de groupes

Soit $f : G \to G'$ un homomorphisme de groupes. L'*image de G par f* est l'ensemble $\mathrm{Im}(f) = \{f(x) | x \in G\}$. C'est clairement un sous-groupe de G' (en effet, $x', y' \in \mathrm{Im}(f) \Rightarrow x' = f(x), y' = f(y)$, d'où $x'y' = f(x)f(y) = f(xy) \in \mathrm{Im}(f)$).

L'homomorphisme f est surjectif ssi $\mathrm{Im}(f) = G'$.

Le *noyau* de f est l'ensemble $\ker(f) = \{x \in G | f(x) = e'\}$ où e' est l'élément neutre de G'. Le noyau est un sous-groupe distingué de G.

C'est un sous-groupe : $x, y \in \ker(f) \Rightarrow f(x) = f(y) = e' \Rightarrow f(xy^{-1}) = e' \Rightarrow xy^{-1} \in \ker(f)$.

Il est distingué : on a $\forall x \in G,\ x\ker(f)x^{-1} \in \ker(f)$. En effet, $\forall k \in \ker(f),\ f(xkx^{-1}) = f(x)e'f(x)^{-1} = e'$, d'où $xkx^{-1} \in \ker(f)$.

Remarque : En notation additive, $\ker(f) = \{x \in G | f(x) = 0\}$ et en notation multiplicative, $\ker(f) = \{x \in G | f(x) = 1\}$.

Si $H \triangleleft G$, alors $H = \ker(\pi : G \to G/H)$.

Lemme 1.6.2 *Un homomorphisme de groupes $f : G \to G'$ est injectif ssi $\ker(f) = \{e\}$.*

Preuve : $\Rightarrow$ Supposons f injective et soit $x \in \ker(f)$, alors $f(x) = e' = f(e) \Rightarrow x = e$.

$\Leftarrow f(x) = f(x') \Rightarrow f(x)f(x')^{-1} = e' \Rightarrow f(xx'^{-1}) = e' \Rightarrow xx'^{-1} \in \ker(f) = \{e\} \Rightarrow xx'^{-1} = e \Rightarrow x = x'$.

Définition 1.6.2 *Un homomorphisme de groupes $f : G \to G'$ est un isomorphisme de groupes si f est bijectif. On dit alors que G et G' sont isomorphes. Un isomorphisme de G dans lui-même est appelé automorphisme.*

Remarquons que si $f : G \to G'$ est un isomorphisme, l'application réciproque $f^{-1} : G' \to G$ est encore un homomorphisme de groupes.

Théorème 1.6.1 ***de décomposition***

Tout homomorphisme de groupes $f : G \to G'$ se factorise à travers un homomorphisme surjectif $\pi : G \to G/\ker(f)$ et un homomorphisme injectif $\tilde{f} : G/\ker(f) \to G'$ càd. $f = \tilde{f} \circ \pi$.

Preuve : Rappelons que $\ker(f)$ est un sous-groupe distingué de G, parler du quotient $G/\ker(f)$ a donc bien un sens et π est alors un homomorphisme surjectif. Il ne reste donc qu'à construire $\tilde{f}$. On a "envie" de la définir ainsi : $x\ker(f) \mapsto f(x)$. Le problème, à nouveau, est que ceci est défini en utilisant un représentant de la classe $x\ker(f)$. Pour que ce soit bien défini comme application, il faut montrer que si x' est un autre représentant de $x\ker(f)$, alors $f(x) = f(x')$.

Or, x et x' appartiennent à la même classe ssi $x'^{-1}x \in \ker(f) \Rightarrow f(x'^{-1}x) = f(x')^{-1}f(x) = 1 \Rightarrow f(x') = f(x)$. Donc $\tilde{f}$ est bien définie. On vérifie immédiatement que c'est un homomorphisme de groupes injectif.

Enfin, $f(x) = \tilde{f}(x\ker(f))$ par construction de $\tilde{f}$, d'où $f = \tilde{f} \circ \pi$.

Observons qu'alors $\tilde{f} : G/\ker(f) \to \mathrm{Im}(f)$ est un isomorphisme de groupes.

Soient H, K deux sous-groupes d'un groupe G, on a vu qu'en général, HK n'est pas un sous-groupe de G (exemple : dans S_3, $H = \{\mathrm{Id}, \tau_1\}, K = \{\mathrm{Id}, \tau_2\}$, alors $HK = \{\mathrm{Id}, \tau_1, \tau_2, \sigma_1\}$ n'est pas un sous-groupe de S_3). Mais on a le résultat suivant :

Lemme 1.6.3 *Si $H \triangleleft G$, alors $HK = KH$ est un sous-groupe de G. Si, de plus, $K \triangleleft G$, alors $HK \triangleleft G$.*

Preuve : Soient $hk, h'k' \in HK$, il s'agit de montrer que $hk(h'k')^{-1} \in HK$. Or $hk(h'k')^{-1} = hk(k'^{-1}h'^{-1}) = h(kh_1)k_1 = h(h_2k_2)k_1 \in HK$. On voit de même que $HK = KH$.

Supposons de plus $K \triangleleft G$, alors $\forall x \in G,\ x(hk)x^{-1} = h'xx^{-1}k' = h'k' \in HK$.

Remarque : sous la première hypothèse seule, HK est le plus petit sous-groupe contenant $H \cup K$.

Théorème 1.6.2 *Soient $H, K < G$ et on suppose que K est distingué dans G. Alors $H \cap K$ est distingué dans H et*

$$\frac{H}{H \cap K} \cong \frac{HK}{K}.$$

Preuve : Pour tout $x \in G,\ y \in H \cap K, x^{-1}yx \in K$, puisque $K \triangleleft G$, mais si $x \in H,\ x^{-1}yx \in H$, donc $x^{-1}yx \in H \cap K$, d'où la première affirmation.

Considérons l'application $H \to HK,\ h \mapsto he$, c'est clairement un homomorphisme de groupes. Composons avec la surjection canonique $HK \to HK/K$ (K est bien un sous-groupe distingué de HK, puisque $y \in K, hk \in HK \Rightarrow (hk)^{-1}yhk = k^{-1}(h^{-1}yh)k \in K$), on obtient un homomorphisme $H \to HK/K$ dont le noyau est clairement $H \cap K$.

D'autre part, dans toute classe $(hk)K$, il y a un représentant de la forme he, d'où la surjectivité.

Théorème 1.6.3 *Soient $H, K \triangleleft G$ tels que $K \subset H$. Alors $H/K \triangleleft G/K$ et*

$$\frac{G/K}{H/K} \cong G/H.$$

Preuve : Utilisons la surjection canonique $\pi : G \to G/K$. Il faut montrer que $\forall x \in G, h \in H,\ \pi(x)^{-1}\pi(h)\pi(x) \in \pi(H) = H/K$; or, $\pi(x)^{-1}\pi(h)\pi(x) = \pi(x^{-1}hx)$ et $x^{-1}hx \in H$.

Par ailleurs, on a un homomorphisme surjectif $G/K \to G/H, xK \mapsto xH$ (on vérifie aisément que c'est bien défini, que c'est un homomorphisme de groupes et que c'est surjectif). Le noyau de cette application est clairement H/K, d'où le résultat par le théorème 1.6.1.

Théorème 1.6.4 *Soit K un sous-groupe distingué d'un groupe G et $\pi : G \to G/K$ la surjection canonique. Alors $S^* \mapsto S = \pi^{-1}(S^*)$ est une bijection croissante de l'ensemble des sous-groupes de G/K, ordonné par inclusion, sur l'ensemble des sous-groupes de G contenant K ; cette bijection préserve l'invariance ie. $T \lhd S$ ssi $T/K \lhd S/K$.*

La démonstration s'appuie sur les 2 lemmes suivants :

Lemme 1.6.4 *Soit $f : G \to G'$ un homomorphisme de groupes et H' un sous-groupe de G'. Alors $f^{-1}(H')$ est un sous groupe de G.*

Preuve : Il suffit de voir que si $x, y \in H = f^{-1}(H')$, alors $xy^{-1} \in H$. Or $f(xy^{-1}) = f(x)f(y)^{-1} \in H'$, d'où la conclusion.

Lemme 1.6.5 *Soient H, K deux sous-groupes d'un groupe G tel que $K \subset H$ et $K \lhd G$. Soit $\pi : G \to G/K$ la surjection canonique. Alors $H \lhd K$ et $\pi(H)$ est un sous-groupe de G/K qu'on peut identifier à H/K .*

Preuve : La première affirmation est triviale. D'autre part, on a vu que l'image d'un sous-groupe par un homomorphisme est un sous-groupe, on en déduit que $\pi(H) < G/K$. Il est clair que les applications $hK \mapsto \pi(h)$ et $\pi(h) \mapsto hK$ sont des homomorphismes inverses l'un de l'autre réalisant ainsi un isomorphisme de $\pi(H)$ avec H/K.

Cependant, on peut réaliser H/K comme *sous-ensemble* (et donc aussi sous-groupe) de G/K en remarquant que la classe hK d'un élément h de H est entièrement contenue dans H et inversement, $x \notin H$ implique que $xK \cap H = \emptyset$.

Preuve du théorème : D'après le lemme précédent, $f : H \mapsto \pi(H) = H/K$ est une application de l'ensemble des sous-groupes de G contenant K dans l'ensemble des sous-groupes de G/K. Et il est clair que $H' \subset H \Rightarrow \pi(H') \subset \pi(H)$, l'application est donc croissante.

Elle est injective car $\pi(H) = \pi(H') \Rightarrow \forall h \in H,\ \exists h' \in H'$ tel que $\pi(h) = \pi(h') \Rightarrow \pi(hh'^{-1}) \in K \subset H'$, d'où $h \in H'$ et donc $H \subset H'$. Les deux groupes H et H' jouant des rôles symétriques, on a donc aussi $H' \subset H$, d'où $H = H'$.

La surjectivité est assurée par le premier lemme, car, pour un sous-groupe S de G/K, $H = \pi^{-1}(S)$ est un sous-groupe de G, contenant K tel que $f(H) = S$.

On vérifie immédiatement que l'application f^{-1} est aussi croissante.

Il reste à montrer que $T \lhd S \Leftrightarrow T/K \lhd S/K$. Or $T/K = \pi(T), S/K = \pi(S)$ et $T \lhd S \Leftrightarrow \forall s \in S,\ \forall t \in T,\ s^{-1}ts \in T \Leftrightarrow \pi(s^{-1}ts) \in \pi(T) \Leftrightarrow \pi(s)^{-1}\pi(t)\pi(s) \in T/K \Leftrightarrow \forall \overline{s} \in S/K,\ \forall \overline{t} \in T/K,\ \overline{s}^{-1}\overline{t}\overline{s} \in T/K \Leftrightarrow T/K \lhd S/K$.

Exercice : Chercher tous les sous-groupes de $\mathbb{Z}/12\mathbb{Z}$.

1.7 Groupes cycliques

1.7.1 Sous-groupe engendré par un ensemble

Définition 1.7.1 *Soit X un sous-ensemble d'un groupe G. L'intersection de tous les sous-groupes de G contenant X est un sous-groupe appelé sous-groupe engendré par X, on le notera $gr(X)$. On dit que X est un système de générateurs de $gr(X)$.*

Il est clair que $\mathrm{gr}(X)$ est le plus petit sous-groupe de G contenant X (il est l'un des termes de l'intersection !).

Lemme 1.7.1 *$gr(X) = \{x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n},\ x_i \in X,\ \alpha_i = \pm 1\}$.*

Preuve : L'ensemble $\{x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n},\ x_i \in X,\ \alpha_i = \pm 1\}$ est un sous-groupe de G (il suffit de voir que si x, x' sont de cette forme, alors xx'^{-1} est encore de cette forme).et, bien sûr, il contient X, d'où il contient $\mathrm{gr}(X)$.

Inversement, $x_i \in X \Rightarrow x_i \in \mathrm{gr}(X) \Rightarrow x_i^{\alpha_i} \in \mathrm{gr}(X) \Rightarrow x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n} \in \mathrm{gr}(X)$.

Il faut remarquer que dans l'écriture ci-dessus les x_i ne sont pas nécessairement distincts.

Si $X = \{a_1, \ldots, a_n\}$, on écrira $\mathrm{gr}(X) = \mathrm{gr}(a_1, \ldots, a_n)$.

Exemples : 1) $\mathrm{gr}(e) = \{e\}$; si $H < G, \mathrm{gr}(H) = H$ (en particulier, $\mathrm{gr}(G) = G$).

2) Dans $\mathbb{Z}/4\mathbb{Z}$, $\mathrm{gr}(1) = \mathbb{Z}/4\mathbb{Z}$ et $\mathrm{gr}(2) = \{0, 2\} \cong \mathbb{Z}/2\mathbb{Z}$.

1.7.2 Définition et propriétés

Définition 1.7.2 *Un groupe G est monogène si G admet un unique générateur $a \in G$ ie. $G = gr(a)$ et cyclique si, de plus, G est fini.*

Attention : $\mathrm{gr}(a) = \mathrm{gr}(b)$ n'implique pas $a = b$ (exemple : $\mathbb{Z}/3\mathbb{Z} = \mathrm{gr}(1) = \mathrm{gr}(2)$).

Théorème 1.7.1 *Soit G un groupe monogène. Si G est infini, G est isomorphe à $\mathbb{Z}$; si G est d'ordre $n \geq 1$, G est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.*

Preuve : Soit $\phi : \mathbb{Z} \to G =< x >$ définie par $\phi(k) = x^k$, c'est clairement un épimorphisme dont le noyau est un sous-groupe de $\mathbb{Z}$, donc $\mathrm{Ker}(\phi) = 0$, et alors ϕ est un isomorphisme de $\mathbb{Z}$ sur G, ou $\mathrm{Ker}(\phi) = n\mathbb{Z}$ et $\mathbb{Z}/n\mathbb{Z} \cong G$ est fini.

Exemples : $\mathbb{Z}/n\mathbb{Z} = \mathrm{gr}(1)$ est cyclique, mais S_3 n'est pas cyclique : $\mathrm{gr}(\tau_i) = \{\mathrm{Id}, \tau_i\}$, $\mathrm{gr}(\sigma_j) = \{\mathrm{Id}, \sigma_j, \sigma_j^2\}$.

Remarque : Si $G = \mathrm{gr}(a)$, alors $G = \{a^n; n \in \mathbb{Z}\}$ (ou, en notation additive, $G = \{na; n \in \mathbb{Z}\}$) et G est donc commutatif.

Théorème 1.7.2 *Tout groupe fini d'ordre premier est cyclique.*

Preuve : Soit G tel que $|G| = p > 0$, p premier. Soit $x \neq 1$ dans G, alors $|\mathrm{gr}(x)|$ divise p et, comme, $|\mathrm{gr}(x)| \neq 1$, $|\mathrm{gr}(x)| = p = |G|$, d'où $\mathrm{gr}(x) = G$.

On a ainsi montré aussi que tout élément de G, différent du neutre, engendre G.

Définition 1.7.3 *Soit G un groupe quelconque et $x \in G$. S'il existe $n \in \mathbb{N}^*$ tel que $x^n = e$, n est appelé un exposant de x et on dit que x est d'ordre fini. Le plus petit exposant de x est appelé l'ordre de x.*

S'il n'existe pas de n tel que $x^n = e$, on dit que x est d'ordre infini.

Il faut bien sûr adapter la définition pour une notation additive.

Lemme 1.7.2 *1) Tout exposant de x est un multiple de l'ordre de x ;*

2) dans un groupe G, l'ordre de x est l'ordre du sous-groupe $gr(x)$;

3) dans un groupe G, l'ordre de tout élément divise l'ordre $|G|$ du groupe.

4) si $f : G \to G'$ est un homomorphisme de groupes, alors, pour tout $x \in G$, l'ordre de $f(x)$ divise l'ordre de x.

Preuve : 1) Soit m un exposant de x ; écrivons $m = nq + r,\ 0 \leq r < n$. Alors, $e = x^m = (x^n)^q x^r \Rightarrow x^r = e$, d'où $r = 0$, puisque n est le plus petit exposant non nul.

2) $\mathrm{gr}(x) = \{1, x, x^2, \ldots, x^{n-1}\},\ x_i \in \mathrm{gr}(x), \forall 0 \leq i < n$ et $x^i \neq x^j$ pour $i \neq j$), d'où le résultat.

On pourrait aussi remarquer que le noyau de l'homomorphisme surjectif $\mathbb{Z} \to \mathrm{gr}(x),\ m \mapsto x^m$ est $n\mathbb{Z}$ où n est l'ordre de x.

3) est une conséquence immédiate de 2) et du théorème de Lagrange.

4) soit k l'ordre de x, alors $x^k = 1$, d'où $f(x)^k = f(x^k) = 1$, d'où le résultat d'après 1).

Conséquence : dans un groupe fini, tout élément est d'ordre fini.

Attention : la réciproque, à savoir si tout élément de G est d'ordre fini alors G est fini est **fausse** comme le montre l'exemple de $\mathbb{Q}/\mathbb{Z}$. En effet, soit $\alpha = a/b + \mathbb{Z} \in \mathbb{Q}/\mathbb{Z}$, alors $|b| \cdot \alpha = \mathbb{Z}$, d'où α est d'ordre fini et $\mathrm{ord}(\alpha) \,|\, |b|$.

Mais $1/2 + \mathbb{Z}, 1/3 + \mathbb{Z}, \ldots, 1/n + \mathbb{Z}, \ldots$ sont tous distincts puisque $n > k \geq 2 \Rightarrow 0 < |1/k - 1/n| < 1 \Rightarrow 1/k - 1/n \notin \mathbb{Z}$, donc $\mathbb{Q}/\mathbb{Z}$ est infini.

Définition 1.7.4 *Si tous les éléments d'un groupe G sont d'ordre fini, on dit que G est un groupe de torsion.*

Remarques : 1) Tout groupe fini est de torsion (mais il y a des groupes infinis de torsion cf. $\mathbb{Q}/\mathbb{Z}$).

2) L'ensemble des éléments de torsion d'un groupe commutatif G est un sous-groupe de G, appelé sous-groupe de torsion de G.

Théorème 1.7.3 *Soit $G = gr(x)$ un groupe cyclique d'ordre n.*

a) Tout sous-groupe H de G est un groupe cyclique engendré par x^k où k est le plus petit entier > 0 tel que $x^k \in H$. De plus, $k \,|\, n$ et $|H| = n/k$.

b) Si $q \,|\, n$, G possède un unique sous-groupe d'ordre q, engendré par $x^{n/q}$.

La preuve est laissée en exercice (voir TD).

Théorème 1.7.4 *Soit $G = gr(x)$ un groupe cyclique d'ordre n.*

a) L'ordre de x^k est $\frac{n}{pgcd(n,k)}$.

b) x^k engendre G ssi n et k sont premiers entre eux.

Là encore la preuve est laissée en exercice.

Exemple : On note $\phi(n)$ le nombre de générateurs de $\mathbb{Z}/n\mathbb{Z}$. Cette fonction s'appelle l'indicateur d'Euler. Si $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ est la décomposition de n en facteurs premiers, on a :
$\phi(n) = n(1 - 1/p_1) \cdots (1 - 1/p_k)$.

1.8 Groupes définis par générateurs et relations

Soit $X = \{x_i; i \in I\}$ un ensemble et X^{-1} un ensemble en bijection avec X, dont les éléments seront notés $\{x_i^{-1}; i \in I\}$.

Un *mot* de l'alphabet X est une suite vide (notée 1) ou finie de symboles appartenant à $T = X \cup X^{-1}$ (ie. un élément de T^n).

Un mot $w = t_1 \cdots t_n$ est *réductible* s'il contient des symboles voisins du type $x_i x_i^{-1}$ ou $x_i^{-1} x_i$ (par exemple : $x_2 x_1 x_1 x_2^{-1}$ est irréductible, mais $x_1 x_2 x_2^{-1} x_3$ est réductible). On peut réduire un mot à un mot irréductible en éliminant tous les symboles voisins du type ci-dessus.

Soit $F(X)$ l'ensemble des mots réduits (en particulier, $e \in F(x)$ et $X \subset F(X)$). On définit sur $F(X)$ le produit de 2 mots réduits $a = t_1 \cdots t_m,\ b = u_1 \cdots u_n$ par $a \cdot b$ est le mot réduit obtenu à partir de $t_1 \cdots t_m u_1 \cdots u_n$ en effectuant toutes les réductions possibles.

Ce produit confère à $F(X)$ une structure de groupe dont l'élément neutre est le mot vide 1, le symétrique d'un mot $t_1 \cdots t_m$ étant le mot $t_m^{-1} \cdots t_1^{-1}$.

Définition 1.8.1 *$F(X)$ est le groupe libre à ensemble générateur X. Le cardinal de X est appelé degré du groupe libre $F(X)$. Remarquons encore que l'on note souvent si $|X| = n$, $F_n(X)$ ou même F_n.*

Théorème 1.8.1 *Soit G un groupe engendré par un ensemble $M = \{g_i; i \in I\}$ et soit $X = \{x_i; i \in I\}$ un alphabet. L'application $\phi : X \to M$ qui à x_i associe g_i se prolonge de manière unique en un homomorphisme surjectif de groupes $F(X) \to G$.*

L'application ϕ est clairement surjective et est un homomorphisme.

Les éléments du noyau H de ϕ s'appellent *relations fondamentales* de G sur X. Si un ensemble H' de relations est tel que le plus petit sous-groupe normal de $F(X)$ contenant H' est H, alors G est entièrement déterminé par X et H' car $G \cong F(X)/H$. On dit que G est *défini par générateurs (les éléments de X) et relations (les éléments de H')*. Le couple X, H' est une *présentation* du groupe G, on notera $< X, H' >$. Si le couple est fini, on dit que G admet une présentation finie.(Remarque : une relation est donc un mot u, mais souvent, on préfère écrire $u = 1$)

Exemples : 1) Le groupe $\mathbb{Z}/n\mathbb{Z}$ est un groupe de présentation $X = \{x\},\ H' = \{x^n\}$, autrement dit $< x, x^n >$.

2) Le groupe de Klein $\frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}}$ est de présentation $X = \{x, y\},\ H' = \{x^2, y^2, x^{-1}y^{-1}xy\}$ ou $< \{x, y\}, x^2, y^2, x^{-1}y^{-1}xy >$.

3) Dans le groupe symétrique S_3, on a remarqué que $\tau_2 = \tau_1\sigma_1$, $\sigma_2 = \sigma_1^2$, $\tau_3 = \tau_1\sigma_2 = \tau_1\sigma_1\sigma_1$, d'où tous les éléments de S_3 sont des mots en τ_1 et σ_1. On remarque aussi les relations $\tau_1^2 = 1$, $\sigma_1^3 = 1$ et $(\tau_1\sigma_1)^2 = 1$. On obtient ainsi une présentation de S_3 par $< x, y; x^2, y^3, (xy)^2 >$.

En effet soit G le groupe défini par cette présentation. On s'aperçoit que les classes (à gauche) modulo le sous-groupe $H = \{1, y, y^2\}$ sont au nombre de 2 seulement, à savoir H et Hx, d'où $|G| = 2|H| = 6$. Or l'application $\phi : G \to S_3$ définie par $\phi(x) = \tau_1$, $\phi(y) = \sigma_1$ est bien définie et est clairement un homomorphisme surjectif, et donc, puisque G et S_3 ont même nombre d'éléments, un isomorphisme.

1.9 Produit de groupes

Définition 1.9.1 *Soient G, H 2 groupes. On appelle produit direct de G et H l'ensemble $G \times H = \{(g, h); g \in G,\ h \in H\}$ muni de la loi définie par : $(g, h)(g', h') = (gg', hh')$.*

Bien entendu, les notations sont à adapter à l'écriture particulière des lois sur G et H. Par exemple, si les lois sont notées additivement sur G et H, le produit sera muni d'une loi, en général également notée additivement, décrite par : $(g, h) + (g', h') = (g + g', h + h')$.

L'élément neutre de $G \times H$ est $(1, 1)$ et le symétrique de (g, h) est (g^{-1}, h^{-1}).

Exemples : 1) $G \times \{1\}$ est un sous-groupe distingué de $G \times H$ isomorphe à G par l'application $x \mapsto (x, 1)$ (en effet, $(x, 1)(y, 1)^{-1} = (xy, 1) \in G \times \{1\}$ et $(x, y)(g, 1)(x, y)^{-1} = (xgx^{-1}, yy^{-1}) = (xgx^{-1}, 1) \in G \times \{1\}$).

2) Le groupe de Klein $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ qui est un groupe d'ordre 4, non isomorphe à $\mathbb{Z}/4\mathbb{Z}$.

3) $A_3 \cong \mathbb{Z}/3\mathbb{Z}$ et $H = \{1, \tau_3\} \cong \mathbb{Z}/2\mathbb{Z}$, mais $HA_3 = S_3$ (car $A_3 \lhd S_3 \Rightarrow HA_3 < S_3$ et les cardinaux sont les mêmes) n'est pas isomorphe à $H \times A_3$ (en effet, $HA_3 = S_3$ qui n'est pas commutatif, tandis que $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ l'est).

Lemme 1.9.1 *Soient H, K deux sous-groupes distingués d'un groupe G. Si $H \cap K = \{1\}$ et $HK = G$, alors $G \cong H \times K$ et $\forall h \in H, k \in K,\ hk = kh$.*

Preuve : Commençons par montrer que $\forall h \in H, k \in K,\ hk = kh$. On sait que $\forall x \in G, h'x = xh$. Si maintenant $x \in K$, on a aussi $xh = hx',\ x' \in K$. d'où $h'x = hx' \Rightarrow h^{-1}h' = x'x^{-1} = 1 \in H \cap K$, et, par conséquent, $h = h'$ et $x = x'$, d'où $hx = xh$.

Considérons alors l'application $H \times K \to G,\ (h, k) \mapsto hk$. Il est clair qu'elle est bien définie, est un homomorphisme de groupes et est surjective. Son noyau est $\{(h, k) | hk = 1\}$. Mais $hk = 1 \Rightarrow k = h^{-1} \in H \cap K = \{1\}$, d'où $k = h = 1$. L'application est donc aussi injective, donc un isomorphisme.

Théorème 1.9.1 *Soit G un groupe fini, H, K 2 sous-groupes distingués tels que $|H|\,|K| = |G|$, alors, si $H \cap K = \{1\}$ ou $HK = G$, $G \cong H \times K$.*

Preuve : Dans le premier cas, si $H \cap K = \{1\}$, comme $|HK| = |H||K|/|H \cap K|$ (cf 1.4.2), on en déduit que $|HK| = |G|$, d'où HK est un sous-groupe de G de même ordre (fini), donc $HK = G$ et on applique le lemme précédent.

Dans le deuxième cas, $HK = G$ et $|H|\,|K| = |G|$, d'où

$$|G| = \frac{|H||K|}{|H \cap K|} = \frac{|G|}{|H \cap K|},$$

d'où $|H \cap K| = 1$ et $H \cap K = \{1\}$ et encore on conclut par le lemme précédent.

Théorème 1.9.2 *Si $H_1 \lhd H$ et $K_1 \lhd K$, alors $H_1 \times K_1 \lhd H \times K$ et*

$$\frac{H \times K}{H_1 \times K_1} \cong \frac{H}{H_1} \times \frac{K}{K_1}.$$

Preuve : Il suffit de remarquer que l'application

$$\begin{array}{rccc} \phi : & H \times K & \to & \dfrac{H}{H_1} \times \dfrac{K}{K_1} \\ & (h, k) & \mapsto & (hH_1, kK_1) \end{array}$$

est un homomorphisme de groupes surjectif, de noyau $H_1 \times K_1$.

Citons encore deux résultats :

Lemme 1.9.2 *Soient H, K deux groupes finis, $h \in H$, $k \in K$, l'ordre de (h, k) dans $H \times K$ est le ppcm des ordres de h et k.*

Preuve : Notons r, s les ordres respectifs de h, k, m le ppcm de r, s et m' l'ordre de (h, k). Alors $(h, k)^{m'} = (1, 1) \Rightarrow h^{m'} = 1$ et $k^{m'} = 1$, d'où $r|m'$ et $s|m'$, et donc $m|m'$.
Inversement, $m = rr' = ss'$, d'où $(h, k)^m = (h^{rr'}, k^{ss'}) = (1, 1)$ et donc $m'|m$.

Théorème 1.9.3 *Le produit direct de deux groupes cycliques finis est un groupe cyclique ssi leurs ordres sont premiers entre eux.*

Preuve : Si $G = \mathrm{gr}(a)$ et $H = \mathrm{gr}(b)$, alors l'ordre de (a, b) est le ppcm de $|G|$ et $|H|$. Or $\mathrm{ppcm}(|G|, |H|) = |G||H|/\mathrm{pgcd}(|G|, |H|)$. D'où $G \times H = \mathrm{gr}((a, b)) \Leftrightarrow \mathrm{pgcd}(|G|, |H|) = 1$.

Chapitre 2

GROUPES COMMUTATIFS

Dans toute ce chapitre, tous les groupes considérés seront commutatifs. On se propose de décrire complètement un tel groupe. Qu'entend-on par "décrire" ? C'est l'exprimer, à isomorphisme près, en termes de groupes bien connus. Nous en donnerons 3 descriptions.

2.1 Modules sur un anneau principal

On va démontrer un théorème de structure des modules sur un anneau principal, puis appliquer ce résultat à un groupe commutatif G. Un tel groupe peut en effet toujours être vu comme un $\mathbb{Z}$-module. La multiplication externe est donnée par : $\mathbb{Z} \times G \to G,\ (n, x) \mapsto nx = x + \ldots + x,\ n$ fois. Cette opération a bien les propriétés nécessaires pour que G soit un $\mathbb{Z}$-module (la vérification est laissée en exercice).

Soit donc A un anneau principal (rappelons qu'il s'agit donc d'un anneau commutatif unitaire intègre dans lequel tout idéal est monogène ; exemples : $\mathbb{Z}$, $k[X]$ où k est un corps).

Définition 2.1.1 *Un A-module L est libre s'il admet une base, finie ou infinie, càd. un ensemble $X = \{x_i\}_{i\in I}$ d'éléments tels que :*
1) X engendre L ie. tout $u \in L$ peut s'écrire $u = \sum_i a_i x_i$, somme finie ;
2) le système X est libre ie. $\sum_i a_i x_i = 0$, somme finie, implique $a_i = 0,\ \forall i$.

Théorème 2.1.1 *Si L est un A-module libre, toutes les bases de L ont même cardinal.*

Preuve : Il n'est pas nécessaire de supposer A principal pour cela. Soient $\{x_i\}_{i\in I}$ et $\{y_j\}_{j\in J}$ deux bases de L et soit $\mathcal{M}$ un idéal maximal de A. Alors $L/\mathcal{M}L$ est un espace vectoriel sur le corps $A/\mathcal{M}$. Il est immédiat de vérifier que les éléments $\{\overline{x}_i\}_{i\in I}$ et $\{\overline{y}_j\}_{j\in J}$ forment des bases de cet espace vectoriel (le sytème est clairement générateur, il suffit donc de vérifier qu'il est libre : or, si on a une somme finie $\sum_{i\in K} \overline{a}_i\overline{x}_i = 0$, alors $\sum_i a_i x_i \in \mathcal{M}L$, autrement dit, on peut écrire $\sum_{i\in K} a_i x_i = \sum_{i\in K'} m_i x_i \in \mathcal{M}L$ où $m_i \in \mathcal{M}$. Comme les $\{x_i\}_{i\in I}$ forment un système libre, on en déduit que, pour tout $i \in K \cap K'$, $a_i = m_i \in \mathcal{M}$, d'où $\overline{a}_i = 0,\ \forall i$). Or, on sait (même énoncé que ci-dessus, mais pour un espace vectoriel sur un corps) que toutes les bases d'un espace vectoriel ont même cardinal, d'où les cardinaux de I et J sont égaux.

Définition 2.1.2 *Le cardinal de I est appelé rang de L.*

Corollaire 2.1.1 *Le module A^n est libre et tout module libre de rang n est isomorphe à A^n.*

A^n admet la base canonique $\{(0, \ldots, 0, 1, 0, \ldots, 0)\}$. Il suffit d'envoyer les éléments d'une base $\{x_1, \ldots, x_n\}$ de L sur la base canonique de A^n.

Définition 2.1.3 *Soit M un A-module. Un élément $x \in M$ est dit* de torsion *si $x \neq 0$ et s'il existe $a \neq 0,\ a \in A$ tel que $ax = 0$.*

L'ensemble $T(M)$ des éléments de torsion, auquel on ajoute 0, est un sous-module de M, appelé sous-module de torsion *de M.*

M est sans torsion *si $T(M) = 0$.*

Lemme 2.1.1 *$M/T(M)$ est un A-module sans torsion.*

Preuve : Soit $a \in A,\ a \neq 0$ et $\overline{x} \in M/T(M)$ tel que $a\overline{x} = 0$. Alors $ax \in T(M)$, donc il existe $b \neq 0, b \in A$ tel que $(ba)x = 0$. Mais A est intègre (par définition), d'où $ba \neq 0$, d'où x est de torsion ie. $\overline{x} = 0$.

Lemme 2.1.2 *Si M est un A-module libre, alors M est sans torsion.*

Preuve : Soit $\{e_i\}_{i\in I}$ une base de M et supposons que $x \neq 0,\ x \in M,\ ax = 0$. Alors $x = \sum_i x_i e_i$ (somme finie), d'où $ax = \sum_i ax_i e_i = 0 \Rightarrow \forall i,\ ax_i = 0$ et, comme A est intègre, on en déduit $a = 0$.

Attention : Un module peut être sans torsion sans être libre, comme le prouve l'exemple suivant : $\mathbb{Q}$ est un $\mathbb{Z}$-module sans torsion, mais il n'est pas libre (en effet : si p_1/q_1 et p_2/q_2 sont 2 rationnels, alors $q_1p_2(p_1/q_1) + (-q_2p_1)(p_2/q_2) = 0$, autrement dit 2 rationnels sont toujours liés sur $\mathbb{Z}$. Si donc $\mathbb{Q}$ était libre, il serait de rang 1, càd. $\mathbb{Q} \cong \mathbb{Z}$,en tant que $\mathbb{Z}$-module, ce qui est clairement faux). Cependant, nous verrons plus loin une réciproque partielle pour les modules de type fini.

Il s'agit à présent de définir la notion de rang pour un A-module quelconque.

Soit $S = A - \{0\}$. C'est bien sûr une partie multiplicative de A et $S^{-1}A$, le localisé de A par S n'est autre que le corps des fractions K de A.

De même, si M est un A-module, le localisé $S^{-1}M$ est un $S^{-1}A$-module, donc un K-espace vectoriel.

(Rappelons que, si A est intègre et S est une partie multiplicative, par définition, $S^{-1}A = \{\text{classe}(a/s); a \in A, s \in S\}$ où $a/s \equiv b/t$ ssi $at = bs$, et de même $S^{-1}M = \{\text{classe}(x/s); x \in M, s \in S\}$ où $x/s \equiv y/t$ ssi $xt = ys$).

Définition 2.1.4 *Le rang de N est la dimension du K-espace vectoriel $S^{-1}N$.*

Remarque : Si L est un A-module libre, alors son rang est le cardinal d'une base $\{x_i\}_{i\in I}$, d'une part, et d'autre part, par la définition précédente, c'est aussi le cardinal d'une base du K-espace vectoriel $S^{-1}L$. Mais il est immédiat de voir que les classes classe$(x_i/1)$ forment une telle base. Les deux définitions coincident donc bien.

2.2 Décomposition en modules monogènes

Il nous faut d'abord un lemme préliminaire dont on pourrait se passer en utilisant la notion d'anneau noethérien et en sachant qu'un anneau principal est noethérien.

Lemme 2.2.1 *Dans un anneau principal A, toute famille $\mathcal{F}$ d'idéaux de A admet un élément maximal.*

Rappelons d'abord la

Définition 2.2.1 *Un élément I de $\mathcal{F}$ est maximal si $J \in \mathcal{F},\ J \supset I \Rightarrow J = I$.*

Preuve : Soit $I \in \mathcal{F}$, alors soit I est maximal et la question est règlée, soit il existe $I_1 \in \mathcal{F}$ tel que $I \subset I_1$, l'inclusion étant stricte. A nouveau, ou bien I_1 est maximal, ou bien il existe $I_2 \in \mathcal{F}$ tel que $I_1 \subset I_2$. Et on recommence le processus. Si aucun des I_k ainsi obtenu n'est maximal, on aura construit ainsi une suite croissante infinie d'éléments de $\mathcal{F}$.

Soit alors $J = \cup_k I_k$; c'est un idéal de A, donc il est principal : $J = Aa$ où $a \in J$, donc a est dans l'un des I_k, mais alors $J = Aa \subset I_k$, d'où $J = I_k = I_{k+1}$, ce qui contredit le fait que l'inclusion de I_k dans I_{k+1} est stricte.

Conclusion, I_k n'est contenu strictement dans aucun élément de $\mathcal{F}$, il est donc maximal.

Lemme 2.2.2 *Soient M un A-module libre de rang n et N un sous-module de M et $u \in Hom_A(M, A)$ une forme linéaire sur M, alors il existe $e, e' \in M$ tels que $M = Ae \oplus \ker(u)$ (1) et $N = Ae' \oplus (N \cap \ker(u))$ (2).*

Preuve : L'image $u(N)$ est un idéal de A, donc engendré par un élément $a_u \in A$. Mais l'ensemble de tous les $u(N)$, où u parcourt $\mathrm{Hom}_A(M, A)$, est un ensemble d'idéaux de A, donc, d'après le lemme précédent, admet un élément maximal. Soit alors u tel que $u(N) = Aa_u$ est maximal.

Comme on peut supposer $N \neq \{0\}$ (sinon le résultat est trivial), $u(N) \neq \{0\}$, donc $a_u \neq 0$. Soit alors $e' \in N$ tel que $u(e') = a_u$.

Soit maintenant $v \in \mathrm{Hom}_A(M, A)$; alors a_u divise $v(e')$. En effet, soit $d = \mathrm{pgcd}(a_u, v(e'))$, alors, par Bezout, on peut écrire $d = ba_u + cv(e')$, donc $d = bu(e') + cv(e') = (bu + cv)(e')$. Posons $w = bu + cv \in \mathrm{Hom}_A(M, A)$. On a : $Aa_u \subset Ad \subset w(N)$ (la première inclusion, c'est $d|a_u$, la deuxième car $w(N)$ contient d), d'où, par maximalité de a_u, $Aa_u = w(N) \Rightarrow Ad = Aa_u \Rightarrow a_u | v(e')$.

M étant libre est identifiable à A^n par choix d'une base $\{e_1, \ldots, e_n\}$. Considérons alors, pour $i = 1, \ldots, n$, p_i la projection sur le i-ème facteur, c'est bien une forme linéaire sur M. On a donc, d'après ce qui précède : $a_u \,|\, p_i(e')$, on peut donc écrire $p_i(e') = \alpha_i a_u$. Mais $e' = \sum_{i=1}^n p_i(e') e_i = \sum_{i=1}^n a_u \alpha_i e_i = a_u \sum_{i=1}^n \alpha_i e_i$. Posons $e = \sum_{i=1}^n \alpha_i e_i \in M$. On a alors $e' = a_u e$ et, comme $a_u = u(e') = a_u u(e)$ et que A est intègre, on en déduit que $u(e) = 1$.

Conséquence : Tout $x \in M$ peut s'écrire $x = u(x)e + (x - u(x)e)$ où clairement $u(x - u(x)e) = u(x) - u(x)u(e) = 0$, donc M est somme de Ae et $\ker(u)$. Or, si $y \in Ae \cap \ker(u)$, alors $y = \alpha e$ et $0 = u(y) = \alpha u(e) = \alpha$, donc $y = 0$. La somme est donc directe.

D'autre part, si $y \in N$, on a $u(y) = ba_u$, donc $y = u(y)e + (y - u(y)e) = ba_u e + (y - ba_u e) = be' + (y - be')$ et $y - be' \in N$, d'où le résultat.

Théorème 2.2.1 *Soit A un anneau principal, M un A-module libre de rang n et N un sous-module de M. Alors :*

i) N est libre de rang $k \leq n$;

ii) il existe une base $\{e_1, \ldots, e_n\}$ de M et des éléments $a_1, \ldots, a_k$ de A tels que :

1. *$\{a_1 e_1, \ldots, a_k e_k\}$ forme une base de N ;*
2. *pour tout i, a_i divise a_{i+1}.*

Preuve : i) On fait une récurrence sur le rang de N Si le rang de N est 0, alors $N = \{0\}$ (en effet : $S^{-1}N = \{0\} \Rightarrow \forall x \in N, x/1 = 0$, donc il existe $s \in S$ tel que $sx = 0$, d'où, puisque N est sans torsion, $x = 0$). Dans ce cas, il n'y a rien à démontrer.

Si le rang est $k > 0$, alors d'après le lemme $N \cap \ker(u)$ est de rang $k - 1$, donc libre par l'hypothèse de récurrence, d'où N, qui est la somme directe d'un libre et de Ae', est donc libre de rang k.

ii) On fait ici une récurrence sur le rang n de M. Là encore, si $n = 0$, il n'y a rien à démontrer. Supposons donc $n > 0$. Soit toujours u tel que Aa_u soit maximal. On peut écrire

$M = Ae \oplus \ker(u)$. Alors $\ker(u)$ est libre, par i), et de rang $n-1$ par le lemme. On applique donc l'hypothèse de récurrence à $N \cap \ker(u) \subset \ker(u)$.

Il existe donc $k \leq n-1$; il existe une base $\{e_2, \ldots, e_n\}$ de $\ker(u)$ et il existe $a_2, \ldots, a_k \in A$ tels que $\{a_2e_2, \ldots, a_ke_k\}$ soit une base de $\ker(u) \cap N$ et, pour $i = 2, \ldots, k$, $a_i \mid a_{i+1}$.

On pose $a_1 = a_u$ et $e_1 = e$. Clairement $\{e_1, \ldots, e_n\}$ est une base de M d'après (1) et $\{a_1e_1, \ldots, a_ke_k\}$ est une base de $\ker(u) \cap N$ d'après (2).

Il reste donc à voir : $a_1 \mid a_2$. Soit $v : M \to A$ définie par $v(e_1) = v(e_2) = 1$ et $v(e_i) = 0$ pour $i \geq 2$. alors $v(a_1e_1) = v(a_ue_1) = a_u \in v(N)$, d'où $Aa_u \subset v(N)$, mais, comme Aa_u est maximal, on en déduit $Aa_u = v(N)$. Or, $a_2 = v(a_2e_2) \in v(N) \Rightarrow a_2 \in Aa_u = Aa_1$ ie. $a_1 \mid a_2$. Ceci achève la démonstration.

Définition 2.2.2 *Un A-module M est dit de type fini s'il peut être engendré par un nombre fini d'éléments. Il est monogène s'il peut être engendré par un seul élément.*

Corollaire 2.2.1 *Soit M un A-module de type fini et N un sous-module, alors N est de type fini.*

On a besoin du lemme suivant :

Lemme 2.2.3 *Si M_1, M_2 sont des A-modules et N_1, N_2 des sous-modules respectivement de M_1, M_2, alors on a un isomorphisme canonique :*

$$\frac{M_1 \times M_2}{N_1 \times N_2} \to \frac{M_1}{N_1} \times \frac{M_2}{N_2}.$$

Preuve : il suffit de voir que le noyau de l'homomorphisme canonique $M_1 \times M_2 \to M_1/N_1 \times M_2/N_2$ est précisément $N_1 \times N_2$.
Preuve du corollaire : On peut représenter M comme image d'un libre. En effet, soit $\{x_1, \ldots, x_n\}$ un système de générateurs de M et L le module libre A^n et notons $e_1, \ldots, e_n$ la base canonique de A^n.

Considérons l'application A-linéaire f qui envoie e_i sur x_i pour tout i. Elle est évidemment surjective. Soit $N' = f^{-1}(N)$; c'est un sous-module de L, donc libre et f est une surjection de N' sur N. L'image d'une base (finie !) de N' est donc un système de générateurs de N.

Remarquons qu'un résultat général assure qu'un sous-module d'un module de type fini sur un anneau noethérien est de type fini. Or, un anneau principal est noethérien. Mais cette démonstration n'utilise pas la propriété de noethérianité.

Corollaire 2.2.2 Décomposition en modules monogènes *Soit M un A-module de type fini sur un anneau principal A, alors*

$$M \cong \frac{A}{\mathcal{I}_1} \times \cdots \times \frac{A}{\mathcal{I}_n}$$

avec $\mathcal{I}_1 \supset \mathcal{I}_2 \supset \cdots \supset \mathcal{I}_n$.

Preuve : Remarquons d'abord qu'il n'est pas exclu que l'un (ou plusieurs) des idéaux $\mathcal{I}$ soit réduit à 0.

Soit $L = A^n$ un A-module libre de rang n tel que $L \xrightarrow{\phi} E \to 0$ et $K = \ker(\phi)$. Alors K est un sous-module de L, donc libre de rang $k \leq n$. De plus, toujours d'après le théorème, il existe une base $\{e_1, \ldots, e_n\}$ de L et des éléments $a_1|a_2|\cdots|a_k$ de A tels que $\{a_1e_1, \ldots, a_ke_k\}$ soit une base de K.

D'où

$$E \cong L/K \cong \frac{Ae_1 \times \cdots Ae_n}{Aa_1e_1 \times \cdots Aa_ke_k} \cong \frac{Ae_1}{Aa_1e_1} \times \cdots \frac{Ae_k}{Aa_ke_k} \times A^{n-k}.$$

La partie A^{n-k} est la *partie libre*, le reste est la *partie de torsion*. Mais $Ae_i/Aa_ie_i \cong A/Aa_i$ (il suffit pour cela de considérer le morphisme composé $\phi : A \to Ae_i \to Ae_i/Aa_ie_i$ qui envoie 1 sur l'image canonique de e_i dans le quotient ; cette application est bien surjective et son noyau n'est autre que Aa_i), d'où :

$$E \cong L/K \cong \frac{A}{Aa_1} \times \cdots \times \frac{A}{Aa_k} \times A^{n-k}.$$

D'où le résultat, en posant $\mathcal{I}_i = Aa_i$, pour $i = 1, \ldots, k$ et $\mathcal{I}_i = 0$ pour $i > k$.

Conséquence : Si M est un A-module de type fini sans torsion, alors M est libre. En effet, tous les modules de la décomposition ci-dessus sont de torsion ssi $\mathcal{I}_k \neq \{0\}$ pour tout k.

2.3 Décomposition en modules primaires

Proposition 2.3.1 *Soit A un anneau principal et $a = up_1^{\alpha_1} \cdots p_n^{\alpha_n}$ une décomposition de $a \in A$ en facteurs premiers. Alors :*

$$\frac{A}{Aa} \cong \frac{A}{Ap_1^{\alpha_1}} \times \cdots \times \frac{A}{Ap_n^{\alpha_n}}.$$

Preuve : C'est une conséquence du théorème chinois, puisque les p_i sont 2 à 2 premiers. Ce théorème assure la surjectivité de l'application $A \to \frac{A}{Ap_1^{\alpha_1}} \times \cdots \times \frac{A}{Ap_n^{\alpha_n}}$ définie en envoyant un élément $a \in A$ sur sa classe modulo $Ap_i^{\alpha_i}$ pour chaque i. Par ailleurs il est immédiat de voir que le noyau de cette application est précisément Aa.

Définition 2.3.1 *Un A-module de type fini est dit p-primaire si tous ses éléments sont annulés par une puissance de p où p est un élément irréductible de A.*

Remarque : Les modules de la décomposition ci-dessus sont tous primaires, mais ils sont de plus monogènes. Cependant, un module p-primaire n'est pas nécessairement monogène (ainsi le groupe de Klein $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ est un $\mathbb{Z}$-module 2-primaire, mais n'est bien sûr pas monogène).

Corollaire 2.3.1 *Tout module de torsion de type fini sur un anneau principal se décompose en un produit de modules primaires cycliques.*

Preuve : Utilisant l'existence d'une décomposition en modules monogènes, un A-module M peut s'écrire $M = \frac{A}{\mathcal{I}_1} \times \cdots \times \frac{A}{\mathcal{I}_n}$ avec $\mathcal{I}_s = Aa_s$. Mais d'après ce qui précède, A/Aa_s est un produit de modules primaires, d'où le résultat.

Remarque : Dans la preuve ci-dessus, on décompose chaque a_s en produit de facteurs irréductibles, mais comme tous les a_s divisent a_k (k le plus grand tel que $a_k \neq 0$), il suffit bien sûr de décomposer a_k.

Théorème 2.3.1 *Les modules primaires de la décomposition ci-dessus sont uniquement déterminés par le module M.*

Pour un module M et un élément irréductible de A, notons $M(p) = \{x \in M | px = 0\}$, l'ensemble des éléments de M annulés par p.

Lemme 2.3.1 *Si $M = N_1 \times \cdots \times N_k$ est un produit direct de modules, alors $M(p) = N_1(p) \times \cdots \times N_k(p)$.*

Preuve : Si $x \in M$, alors $x = (x_1, \ldots, x_k)$, $x_i \in N_i$, d'où $0 = px = (px_1, \ldots, px_k)$, donc $px_i = 0$, pour tout i, donc $x_i \in N_i(p)$.

D'autre part, $x = (x_1, \ldots, x_k)$, $x_i \in N_i(p) \Rightarrow px_i = 0, \forall i \Rightarrow px = 0 \Rightarrow x \in M(p)$.

Preuve du théorème : On suppose donc que

$$M = (\frac{A}{p})^{m_1} \times (\frac{A}{p^2})^{m_2} \times \cdots \times (\frac{A}{p^s})^{m_s} \times N$$

où N est la partie de la décomposition ne contenant plus de p et notons M' la partie concernant p (bien sûr certains $m_i = 0$). Alors, d'après le lemme précédent,

$$M(p) = (\frac{A}{p})^{m_1}(p) \times \cdots \times (\frac{A}{p^s})^{m_s}(p) \times N(p)$$

et, bien sûr, $M(p)$ (et $M'(p)$) est un espace vectoriel sur le corps A/p.

Remarquons d'abord que $N(p) = 0$. En effet, soit $x \in N$ tel que $px = 0$, comme il existe q premier avec p tel que $q^r x = 0$, on en déduit (utilisant par exemple Bezout) que $x = 0$.

D'autre part, puisque pour $h \leq k$, $p^k(A/p^h A) = 0$, on a

$$p^k M' = p^k(A/p^{k+1}A)^{m_{k+1}} \times p^k(A/p^{k+2}A)^{m_{k+2}} \times \cdots \times p^k(A/p^s A)^{m_s}.$$

Mais $p^k(A/p^i A) \cong p^k A/p^i A$ (il suffit de considérer l'homomorphisme surjectif $\phi : p^k A \to p^k(A/p^i A)$ défini par $\phi(p^k a) = p^k(a + p^i A)$ dont le noyau est $p^i A$).

D'où $p^k M' \cong (p^k A/p^{k+1}A)^{m_{k+1}} \times \cdots \times (p^k A/p^s A)^{m_s}$ et par suite

$$p^k M' \cap M'(p) = (p^k A/p^{k+1}A)^{m_{k+1}} \times (p^{k+1}A/p^{k+2}A)^{m_{k+2}} \times \cdots \times (p^{s-1}A/p^s A)^{m_s}$$

et, par conséquent, le quotient

$$\frac{p^k M' \cap M'(p)}{p^{k+1}M' \cap M'(p)} \cong (\frac{p^k A}{p^{k+1}A})^{m_{k+1}} \cong (\frac{A}{pA})^{m_{k+1}},$$

qui est un A/p-espace vectoriel de dimension m_{k+1}.

Finalement, on constate que m_{k+1} est la dimension du quotient

$$\frac{p^k M' \cap M'(p)}{p^{k+1}M' \cap M'(p)}$$

qui ne dépend, par sa définition, que de M.

Définition 2.3.2 *Les p_i^j qui interviennent dans la décomposition de M en produit de modules primaires sont appelés diviseurs élémentaires de M. Ils ne dépendent que de M. C'est donc une liste de la forme*

$$(p_1^{\alpha_{11}}, p_1^{\alpha_{12}}, \ldots, p_1^{\alpha_{1k_1}}, p_2^{\alpha_{21}}, \ldots, p_2^{\alpha_{2k_2}}, \ldots)$$

qu'on écrit généralement dans le sens $\alpha_{1k} \geq \alpha_{1k-1} \geq \cdots, \alpha_{2k} \geq \alpha_{2k-1} \geq \cdots$, etc.

Corollaire 2.3.2 *La décomposition d'un A-module M en produit de modules monogènes $M = A/\mathcal{I}_1 \times \cdots \times A/\mathcal{I}_n$ tels que $\mathcal{I}_{i+1} \subset \mathcal{I}_i$, pour tout i, est uniquement déterminée par M.*

Preuve : Pour tout s, $\mathcal{I}_s = Aa_s$ et $a_s = u_s p_{s1}^{\alpha_{s1}} \cdots p_{sr_s}^{\alpha_{sr_s}}$. Or on a vu que les p_i^j et les α_{ij} sont uniquement déterminés par M. Comme $I_n = Aa_n$ est contenu dans $I_j = Aa_j$, pour tout j, a_n doit être divisible par tous les a_j. Par conséquent, $a_n = p_1^{\beta_1} \cdots p_s^{\beta_s}$ où $\beta_i = \max_k \alpha_{ik}$, donc a_n est déterminé uniquement. Puis, on recommence pour a_{n-1}, qui doit être divisible par tous les

précédents, etc... En fait , les a_i sont obtenus en prenant les puissances de p_i situés sur une colonne du tableau ci-dessous :

$$\begin{array}{lcccccc} p_1 & : & \alpha_{11} & \leq & \alpha_{12} & \leq & \cdots \\ p_2 & : & \alpha_{21} & \leq & \alpha_{22} & \leq & \cdots \\ \vdots & & \vdots & & \vdots & & \vdots \\ p_s & : & \alpha_{s1} & \leq & \alpha_{s2} & \leq & \cdots \end{array} .$$

Ainsi $a_1 = p_1^{\alpha_{11}} p_2^{\alpha_{21}} \cdots p_s^{\alpha_{s1}}$, $a_2 = p_1^{\alpha_{12}} p_2^{\alpha_{22}} \cdots p_s^{\alpha_{s2}}$, etc...
Par conséquent, les a_s sont uniquement déterminés par M.

Définition 2.3.3 *Les idéaux $\mathcal{I}_s$ figurant dans la décomposition de M sont appelés les facteurs invariants de M.*

2.4 Exemple

On se propose de chercher tous les groupes commutatifs d'ordre 24. Or $24 = 2^3 \times 3$. Le théorème de décomposition en modules primaires cycliques assure donc que les groupes d'ordre 24 sont de type $(2^3, 3)$, $(2, 2^2, 3)$, $(2, 2, 2, 3)$ (ce sont les diviseurs élémentaires possibles). Il y a donc 3 groupes d'ordre 24 (à isomorphime près). Ce sont :

$$\frac{\mathbb{Z}}{24\mathbb{Z}},\ \frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{4\mathbb{Z}} \times \frac{\mathbb{Z}}{3\mathbb{Z}},\ \frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{3\mathbb{Z}}.$$

Comment obtient-on les facteurs invariants ?

Les facteurs invariants, a_i, sont obtenus, comme on l'a vu plus haut, en prenant les puissances de p_i situés sur une colonne. Ainsi $a_1 = p_1^{\alpha_{11}} p_2^{\alpha_{21}} \cdots p_s^{\alpha_{s1}}$, $a_2 = p_1^{\alpha_{12}} p_2^{\alpha_{22}} \cdots p_s^{\alpha_{s2}}$, etc...

Dans notre cas, on obtient :
– premier exemple : seul facteur invariant 24 ;
– deuxième exemple : $\begin{array}{lcccc} 2 & : & 1 & \leq & 2 \\ 3 & : & 0 & \leq & 1 \end{array}$, d'où $a_1 = 2^1 \cdot 3^0 = 2$, $a_2 = 2^2 \cdot 3 = 12$, ie. $(2, 12)$. On obtient donc le groupe $\mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, qu'on sait bien être isomorphe à celui décrit au-dessus ;
– troisième exemple : $\begin{array}{lcccccc} 2 & : & 1 & \leq & 1 & \leq & 1 \\ 3 & : & 0 & \leq & 0 & \leq & 1 \end{array}$, d'où $a_1 = 2^1 \cdot 3^0 = 2$, $a_2 = 2^1 \cdot 3^0$ et $a_3 = 2^1 \cdot 3^1 = 6$, ie. $(2, 2, 6)$. On obtient ainsi $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$. Là encore c'est bien sûr le même groupe que son correspondant ci-dessus.

2.5 Applications

On peut tirer quelques conséquences simples de l'existence de telles décompositions :

Lemme 2.5.1 *L'ordre d'un élément d'un groupe commutatif fini G est le ppcm des ordres de ses composantes dans la décomposition de G en groupes primaires cycliques.*

Preuve : Soit $G = G_1 \times \cdots \times G_s$ la décomposition de G en groupes cycliques primaires et soit $x \in G$, un élément d'ordre n, $x = (x_1, \ldots, x_s)$, $x_i \in G_i$. Alors $0 = nx = (nx_1, \ldots, nx_s)$, donc, pour tout i, $nx_i = 0$, d'où n est un multiple du ppcm q des ordres des x_i. Inversement,comme $qx_i = 0$, pour tout i, on en déduit $qx = 0$, donc q est un multiple de n, donc $q = n$.

Lemme 2.5.2 *Dans tout groupe commutatif fini, il existe un élément dont l'ordre est le ppcm des ordres des éléments de G.*

Preuve : G est isomorphe à un produit direct de groupes cycliques $G \cong H_1 \times \cdots \times H_r$ avec $|H_r| | \cdots | |H_1|$. L'ordre n_1 de H_1 est un multiple de l'ordre de chaque H_i, donc un multiple de l'ordre de tous les éléments de G, donc un multiple du ppcm des ordres des éléments de G.

Soit h_1 un générateur de H_1, alors $(h_1, 0, \ldots, 0)$ est d'ordre n_1. Il y a donc bien un élément d'ordre n_1, d'où le ppcm des ordres des éléments de G est n_1.

Théorème 2.5.1 ***Chinois généralisé*** *Soient $m, n \in \mathbb{Z}$. Les groupes*

$$\frac{\mathbb{Z}}{m\mathbb{Z}} \times \frac{\mathbb{Z}}{n\mathbb{Z}} \quad et \quad \frac{\mathbb{Z}}{pgcd(m,n)\mathbb{Z}} \times \frac{\mathbb{Z}}{ppcm(m,n)\mathbb{Z}}$$

sont isomorphes.

Il suffit de décomposer m et n en facteurs premiers et constater que les facteurs invariants sont les mêmes.

Remarquons au passage que cela ne donne pas explicitement l'isomorphisme ; il faut construire celui-ci “à la main”.

Chapitre 3

THEOREMES DE SYLOW

Les groupes considérés dans ce chapitre ne sont pas nécessairement commutatifs. Ce sont pourtant par des groupes du type $S_n,\ n \geq 3$ et $\mathrm{Gl}(\mathbb{C}^2)$ qu'a débuté historiquement l'étude des groupes (Galois, Abel, Cauchy).

3.1 Opération d'un groupe sur un ensemble

3.1.1 Généralités

Définition 3.1.1 *Soit E un ensemble et G un groupe. Une opération (à gauche) de G sur E est une application $G \times E \to E$ notée $(g,x) \mapsto g \cdot x$ telle que, pour tous $g,h \in G,\ x \in E$,*

$$(gh) \cdot x = g \cdot (h \cdot x) \text{ et } e \cdot x = x$$

où e désigne l'élément neutre de G.

Soit E muni d'une opération d'un groupe G. Alors tout $g \in G$ définit une application $t_g : E \to E$ par $t_g(x) = gx$. On a clairement, pour tous $g,h \in G$, $t_{gh} = t_g \circ t_h$.

On en déduit que t_g admet une application réciproque $t_{g^{-1}}$, donc est une bijection de E, autrement dit un élément du groupe des permutations $S(E)$ de E. L'application $\rho : G \to S(E)$ définie par $\rho(g) = t_g$ est un homomorphisme de groupes. On dit que c'est une *représentation* de G dans $S(E)$.

Définition 3.1.2 *Soit $x \in E$, le sous-groupe (le vérifier) $G_x = \{g \in G \,|\, gx = x\}$ est appelé stabilisateur (ou groupe d'isotropie) de x.*

Plus généralement, si A est un sous-ensemble de E, le stabilisateur G_A de A est l'ensemble $\{g \in G \mid gA = A\}$.

Le sous-ensemble de E, $\mathcal{O}_G(x) = \{y \in E \,|\, \exists g \in G; y = gx\}$ (qu'on peut écrire plus simplement $\{gx \,|\, g \in G\}$) est appelé orbite de x

Exemples : 1) Le groupe linéaire $\mathrm{Gl}_n(\mathbb{R})$ opère sur $\mathbb{R}^n$ de la manière suivante : pour $A \in \mathrm{Gl}_n(\mathbb{R}),\ v \in \mathbb{R}^n,\ (A,v) \mapsto Av \in \mathbb{R}^n$. On vérifie immédiatement que cela définit bien une opération sur $\mathbb{R}^n$.

2) On peut aussi faire opérer les matrices inversibles $\mathrm{Gl}_n(\mathbb{C})$ sur l'ensemble $M_n(\mathbb{C})$ des matrices $n \times n$ de la manière suivante : $(A,M) \mapsto AMA^{-1}$. Dans ce cas, rappelons que 2 matrices M, M' sont *semblables* ssi elles appartiennent à la même orbite sous l'action de $\mathrm{Gl}_n(\mathbb{C})$. Chaque orbite possède alors un représentant "canonique" : sa forme de Jordan. Il y a donc un nombre fini d'orbites.

Considérons la relation sur E : xRy ssi il existe $g \in G; y = gx$. On vérifie immédiatement que R est une relation d"équivalence sur E dont les classes sont précisément les orbites. Par conséquent, on a le résultat :

Lemme 3.1.1 *E est réunion disjointe des orbites et si E est fini, $|E| = \sum |\mathcal{O}_G(x)|$.*

Soit $x \in E$ et considérons l'application $\phi : G/G_x \to \mathcal{O}_G(x)$ définie par $gG_x \mapsto gx$. Cette application est surjective par définition de l'orbite de x. De plus, $gx = hx \Rightarrow h^{-1}gx = x$, d'où $h^{-1}g \in G_x$ ou encore $hG_x = gG_x$, donc l'application est aussi injective. On a ainsi montré que ϕ est une bijection, d'où :

Lemme 3.1.2 *Si G est un groupe fini opérant sur un ensemble E, alors $|\mathcal{O}_G(x)| = (G : G_x) = |G|/|G_x|$ ie. $|G| = |G_x||\mathcal{O}_G(x)|$.*
Si de plus E est fini, $|E| = \sum (G : G_x)$.

3.1.2 Conjugaison

L'exemple sans doute le plus important d'opération consiste à faire opérer le groupe G sur lui-même de la manière suivante :

$$\begin{array}{ccc} G \times G & \to & G \\ (g, x) & \mapsto & gxg^{-1} \end{array} .$$

On vérifie immédiatement les deux conditions pour que cette application soit effectivement une opération. Cette opération est appelée *conjugaison.*

Dans le cas du deuxième exemple ci-dessus, si on restreint l'action de $\mathrm{Gl}_n(\mathbb{C})$ à lui-même considéré comme sous-ensemble de $M_n(\mathbb{C})$, l'opération est "une conjugaison" et les orbites sont les classes de conjugaison.

Appliquons les définitions et résultats du paragraphe précédent à la conjugaison. Ainsi : pour un $x \in G$, le stabilisateur G_x est l'ensemble $\{g \in G \mid gxg^{-1} = x\}$ des g qui commutent avec x. On l'appelle encore dans ce cas *normalisateur* ou *centralisateur* de x et on note N_x.

On définit aussi le normalisateur d'un sous-ensemble A, ou plus particulièrement d'un sous-groupe H, de G comme le stabilisateur de A pour la conjugaison. Là encore on peut donner une définition "directe" en disant que $N_A = \{g \in G \mid gAg^{-1} = A\}$. Remarquons que, si H est un sous-groupe de G, N_H est le plus grand sous-groupe de G dans lequel H est distingué. Par conséquent, H est distingué dans G ssi $N_H = G$.

Dans ce cas, comme on le vérifie aisément, t_g est en fait un automorphisme de G et l'application $\phi : G \to \mathrm{Aut}(G) \subset S(G)$ qui à g associe t_g est un homomorphisme de groupes. Le noyau de ϕ est appelé le *centre* de G et noté $Z(G)$ et l'image de t_g est l'ensemble des automorphismes intérieurs (Remarquons au passage que $Z(G) = \cap_{x \in G} N_x$ est l'ensemble des éléments de G qui commutent avec tous les éléments de G. C'est un sous-groupe distingué de G).

Exemple : $Z(\mathrm{Gl}_n(\mathbb{C})) = \{\lambda \mathrm{Id} \mid \lambda \in \mathbb{C}\}$.

La relation d'équivalence associée à cette opération est x *conjugué de* y ssi $\exists g \in G; y = gxg^{-1}$. Les classes d'équivalence pour la conjugaison, autrement dit, les orbites, sont appelées dans ce cas *classes de conjugaison.*

Enonçons dans ce cas les résultats du paragraphe précédent : d'une part, G est la réunion disjointe des classes de conjugaison, d'autre part, si G est fini, $|G| = \sum_{x \in G} |\mathcal{O}_x| = \sum_{x \in G} |G|/|G_x|$. On peut "préciser" ce dernier résultat par la

Formule des classes :

$$|G| = |Z(G)| + \sum_{x \notin Z(G)} |\mathcal{O}_x|.$$

En effet, si $x \in Z(G)$, alors $\mathcal{O}_x = \{x\}$, d'où $\sum_{x \in Z(G)} |\mathcal{O}_x| = |Z(G)|$.

Exemple : Dans S_3, les classes de conjugaison sont : $Z(S_3) = \{1\}$, la classe des transpositions $\{\tau_1, \tau_2, \tau_3\}$, la classe des 3-cycles $\{\sigma_1, \sigma_2\}$. On vérifie sur cet exemple la formule des classes.

3.1.3 Produit semi-direct

Prenons d'abord un exemple : Considérons dans S_4 le sous-groupe invariant engendré (et constitué) par les produits de 2 transpositions à supports disjoints, B_4, d'ordre 4. Soit $K \cong S_3$ le stabilisateur de 4 dans S_4.

Considérons alors le produit ensembliste $B_4 \times K$. On sait déjà qu'on peut le munir d'une structure de groupe par la loi du produit direct. Cela donne un groupe d'ordre 24. Mais il n'est pas isomorphe à S_4 (on compare les lois).

Cependant, on peut définir une loi de manière différente :

$$\forall s, s' \in B_4,\ k, k' \in K,\ (s,k) \cdot (s',k') = (sks'k^{-1}, kk').$$

On vérifie immédiatement que cela définit bien une (autre) structure de groupe sur le produit. Muni de cette structure, le produit est alors isomorphe à S_4.

De manière plus générale, on a :

Définition 3.1.3 *Soient G et H deux groupes et $\phi : H \to Aut(G)$ un homomorphisme de groupes. On définit sur le produit $G \times H$ l'opération :*

$$\begin{array}{ccc} (G \times H) \times (G \times H) & \to & G \times H \\ ((s,t),(s',t')) & \mapsto & (s\phi(t)(s')s', tt') \end{array}.$$

On vérifie immédiatement que cette loi est une loi de groupe sur le produit $G \times H$. On dit que $G \times H$ muni de cette loi est le produit semi-direct de G par H par rapport à ϕ. *On notera, en général, $G \times_\phi H$. Souvent aussi, au lieu d'écrire $\phi(t)(s')$, on préférera la notation $\phi_t(s')$ ou ${}^t s'$.*

Dans l'exemple ci-dessus ϕ est l'aplication $K \to \mathrm{Aut}(B_4)$ définie par $k \mapsto (s \mapsto ksk^{-1})$, ie. l'automorphisme intérieur de S_4 défini par k.

En pratique, H est souvent un sous-groupe de $\mathrm{Aut}(G)$.

Les applications naturelles $G \to G \times_\phi H$ et $H \to G \times_\phi H$ données respectivement par $s \mapsto (s,e)$ et $k \mapsto (e,t)$ sont des homomorphismes de groupes injectifs. De plus l'image de G est un sous-groupe invariant de $G \times_\phi H$.

Exemple : Soit V un espace vectoriel, T le groupe des translations de V et $H = \mathrm{Gl}(V)$. Soit A le groupe des transformations affines de V. On vérifie alors que $A \cong T \times_\phi H$.

Proposition 3.1.1 *Soient H, K deux sous-groupes d'un groupe G tels que $H \triangleleft G$, $H \cap K = \{e\}$, $G = H \cdot K$, alors G est isomorphe au produit semi-direct $H \times_\phi K$ où $\phi : K \to Aut(H)$ est défini par "$\phi(k)$ est l'automorphisme intérieur associé à $k \in K$".*

Preuve : L'application naturelle

$$\begin{array}{ccc} H \times_\phi K & \to & H \cdot K = G \\ (h,k) & \mapsto & hk \end{array}$$

est clairement surjective. On vérifie immédiatement que c'est un homomorphisme de groupes, et son noyau est l'ensemble $\{(h,k); hk = e\} = \{(h,k); h = k^{-1} \in H \cap K\} = \{(e,e)\}$.

3.2 Théorèmes de Sylow

3.2.1 Résultats préliminaires

Théorème 3.2.1 ***de Cauchy*** *Soit G un groupe fini d'ordre n et $p > 0$ un diviseur premier de n, alors G possède un élément d'ordre p.*

Preuve : Par récurrence sur n. Si $n = 2$, le résultat est trivial. Supposons donc le résultat vrai pour tout $m < n$, $n \geq 2$ et soit $p > 0$, $p|n$.

Si $G = Z(G)$ (ie. G est commutatif), G est donc un groupe commutatif fini. D'après le chapitre précédent, on peut donc écrire G est isomorphe à un groupe de la forme $\mathbb{Z}/p^\alpha\mathbb{Z} \times G'$. Or $\mathbb{Z}/p^\alpha\mathbb{Z}$ est un groupe cyclique, donc contient un élément d'ordre p.

On peut donc supposer $G \neq Z(G)$. Deux cas sont possibles :

1) Soit il existe $x \in G - Z(G)$ tel que $p \mid |G_x|$. Mais, $x \notin Z(G) \Rightarrow G_x \neq G \Rightarrow |G_x| < |G|$, et alors, d'après l'hypothèse de récurrence, il existe dans $G_x \subset G$ un élément d'ordre p.

2) Soit pour tout $x \in G - Z(G)$, p ne divise pas $|G_x|$. Mais alors, puisque $n = |\mathcal{O}_x||G_x|$, p divise $|\mathcal{O}_x|$. Or

$$|G| - \sum_{x \notin Z(G)} |\mathcal{O}_x| = |Z(G)|.$$

Comme p divise le premier membre, il divise aussi le second. Mais $Z(G)$ est un groupe commutatif, il possède donc un élément d'ordre p.

Exemple : Dans S_4, il existe au moins un élément d'ordre 2 et un élément d'ordre 3. Ce qu'on peut bien sûr dans ce cas voir directement : ainsi (123) est d'ordre 3 et une transposition est d'ordre 2.

Définition 3.2.1 *Un groupe G est un p-groupe s'il existe $p > 0$ et $k \geq 1$ tels que $|G| = p^k$. (Comparer avec la définition de module p-primaire).*

Théorème 3.2.2 ***de Burnside*** *Tout p-groupe fini G, non réduit à un élément, possède un centre non réduit à un élément et $|Z(G)| \geq p$.*

Preuve : Si $G = Z(G)$, il n'y a rien à démontrer. Sinon, il existe des éléments $x_1, \ldots, x_r$, n'appartenant pas à $Z(G)$, tels que $|G| = |Z(G)| + \sum_{i=1}^{r} |\mathcal{O}_{x_i}|$ (1). Comme $|\mathcal{O}_{x_i}| = [G : G_{x_i}] \mid p^k = |G|$, tous les termes de (1) sont divisibles par p, donc $|Z(G)|$ est divisible par p.

Lemme 3.2.1 *Si $G/Z(G)$ est un groupe cyclique, alors G est commutatif.*

Preuve : Soit $\pi : G \to G/Z(G)$ le morphisme canonique et soit $\pi(g)$ un générateur de $G/Z(G)$. Soient x, y deux éléments de G. Alors il existe r, s tels que $\pi(x) = \pi(g)^r$ et $\pi(y) = \pi(g)^s$. D'où $\pi(g^{-r}x) = 1$ ie. $g^{-r}x \in Z(G)$ et de même pour y. Autrement dit, il existe $x', y' \in Z(G)$ tels que $x = g^r x',\ y = g^s y'$.

On en déduit $xy = (g^r x')(g^s y') = x' g^{r+s} y' = y' g^{s+r} x' = yx$.

Théorème 3.2.3 *Tout groupe d'ordre p^2, où $p > 0$ premier, est commutatif.*

Preuve : D'après le théorème de Burnside, $|Z(G)| \geq p$. Comme $|Z(G)|$ divise p^2, soit $|Z(G)| = p^2$ et G est commutatif, soit $|Z(G)| = p$, d'où $|G/Z(g)| = p$ et $G/Z(G)$ est donc cyclique et on applique le lemme précédent.

Exemple : En application de ce théorème et des résultats sur la classification des groupes commutatifs, on constate que les groupes d'ordre p^2 sont du type (p^2) ou (p, p). Ainsi, par exemple, il n'y a que 2 groupes d'ordre 4 : $\mathbb{Z}/4\mathbb{Z}$ et le groupe de Klein, tous deux commutatifs.

3.2.2 Les théorèmes

Définition 3.2.2 *Un sous-groupe H d'un groupe fini G est un p-sous-groupe de Sylow (on dira plus brièvement un "p-Sylow") si H est un sous-groupe d'ordre p^n où p^n est la plus grande puissance de p qui divise $|G|$.*

Théorème 3.2.4 *Soit G un groupe fini et p un nombre premier divisant $|G|$. Alors il existe un p-sous-groupe de Sylow de G.*

Preuve : On fait une récurrence sur l'ordre de G. Si $|G|$ est premier, le résultat est trivial. Soit donc G un groupe fini et supposons le théorème démontré pour tous les groupes d'ordre strictement inférieurs à $|G|$.

S'il existe $H < G$ tel que $[G : H]$ est premier à p, alors un p-sous-groupe de Sylow de H est aussi un p-Sylow de G et cette existence découle de l'hypothèse de récurrence.

On peut donc supposer que pour tout sous-groupe H, p divise $[G : H]$. De la formule des orbites

$$|G| = |Z(G)| + \sum_{x \notin Z(G)} [G : G_x],$$

on déduit que, puisque tous les indices sont divisibles par p, p divise aussi $|Z(G)|$.

Or $Z(G)$ est un groupe commutatif, donc il y existe un élément a d'ordre p. Soit $H = gr(a)$. Comme $H \subset Z(G)$, H est distingué. Soit alors $f : G \to G/H$ l'homomorphisme canonique. Soit p^n la plus grande puissance de p qui divise l'ordre de G. Alors p^{n-1} divise l'ordre de G/H (rappelons que $|G/H| = |G|/|H| = |G|/p$).

Comme l'ordre de G/H est strictement inférieur à l'ordre de G, il existe, par l'hypothèse de récurrence, un p-Sylow K' de G/H.Soit $K = f^{-1}(K')$ son image réciproque par f. Alors, bien sûr, $H \subset K$ et $f(K) = K'$, d'où $K/H \cong K'$, autrement dit $|K| = p^{n-1}p = p^n$, et K est le p-Sylow cherché.

Théorème 3.2.5 ***(Sylow)*** *Soit G un groupe fini d'ordre $p^n q$ où p est premier et q premier à p, alors :*

i) Si H est un p-sous-groupe de G, alors il existe un p-Sylow K tel que $H < K$;

ii) Tous les p-Sylow sont conjugués ;

iii) Le nombre de p-Sylow est congru à 1 modulo p et divise q.

Preuve : i) Soit S l'ensemble des p-Sylow de G. Alors G opère sur S par conjugaison (si $H < G$, alors, pour tout $g \in G$, $t_g(H) = gHg^{-1} < G$. De plus, t_g est un isomorphisme, donc $t_g(H)$ a même ordre que H, donc si H est un p-Sylow, $t_g(H)$ aussi).

Supposons donc $|G| = p^n q$ où $(p, q) = 1$ et P un p-Sylow (donc $|P| = p^n$) et G_P son stabilisateur. Comme $P < G_P$ (donc $|G_P| \geq |P| = p^n$) et $|G| = p^n q = |G_P||\mathcal{O}_P|$, nécessairement, $|\mathcal{O}_P|$ est premier à p.

Soit H un p-sous-groupe, alors H opère (par conjugaison) sur l'orbite $S_0 = \mathcal{O}_P$. Alors S_0 est réunion d'orbites sous l'action de H. Mais $|H|$ est une puissance de p, donc pour tout sous-groupe propre K de H, p divise $[H : K]$. Comme $|S_0| = \sum_{K \in S_0} [H : N_K]$ et que $|S_0|$ est premier à p, il existe un $P' \in S_0$ tel que $N_{P'} = H$, càd. tel que, pour tout $h \in H$, $hP'h^{-1} = P'$, autrement dit, l'orbite de P' sous l'action de H est réduite au seul élément P'.

De plus, puisque $H = N_{P'}$, $HP' < G$ (car si $ha, kb \in HP'$, $a, b \in P'$, $h, k \in H$, alors $(ha)^{-1}(kb) = a^{-1}h^{-1}kb = h^{-1}a'kb = h^{-1}ka''b \in HP'$) et $P' \lhd HP'$ (se vérifie de manière analogue). De $HP'/P' \cong H/(H \cap P')$, on déduit alors que $|HP'/P'|$ est une puissance de p, et donc aussi $|HP'|$. Comme $|P'|$ est maximal, on a $HP' = P'$, d'où $H \subset P'$.

ii) Soit maintenant H un p-Sylow quelconque de G. Alors on a vu que H est contenu dans un conjugué de P et donc lui est égal (les ordres sont les mêmes).

iii) Prenons alors $H = P$. Le nombre de p-Sylow est le cardinal de $\mathcal{O}_p$, $|\mathcal{O}_P| = |S_0| = \sum_{K \in S_0} [H : N_K]$ et, tous les $[H : N_K]$ sauf un qui vaut 1, sont divisibles par p, donc congrus à 0, modulo p, d'où le premier résultat. Mais, d'autre part, $p^n q = |G| = |\mathcal{O}_P||G_P|$, et comme p est premier à $|\mathcal{O}_P|$, on en déduit que $|\mathcal{O}_P|$ divise q.

3.2.3 Exemple

On se propose de trouver tous les groupes G d'ordre $12 = 4 \times 3$. Le nombre de 3-Sylow de G est congru à 1 modulo 3, et doit diviser 4, donc est 1 ou 4. De même, le nombre de 2-Sylow, est congru à 1 modulo 2 et divise 3, donc est égal à 1 ou 3.

Cas 1. Si G possède 4 3-Sylow, $H_i, i = 1, 2, 3, 4$, alors le nombre d"éléments d'ordre 3 dans $H_1 \cup H_2 \cup H_3 \cup H_4$ est $2 \times 4 = 8$. Il reste donc 4 éléments dans G. Ceux-ci constituent alors l'unique 2-Sylow V (il existe au moins un 2-Sylow V d'ordre 2^2, et clairement $V \cap H_i = \{1\}$).

L'unicité de ce 2-Sylow implique $V \lhd G$.

a) Soit $V \cong \mathbb{Z}/4\mathbb{Z}$, alors $\mathrm{Aut}(V) \cong \mathbb{Z}/2\mathbb{Z}$. Par conséquent, le seul homomorphisme possible $\phi : H_i \to \mathrm{Aut}(V)$ est trivial (si $\phi(h) \neq \mathrm{Id}$, alors son ordre doit être 3, ce qui est impossible). Donc $G = V \cdot H \cong V \times H$ est commutatif, donc ne contiendrait qu'un seul 3-Sylow, ce qui est contradictoire. Ce cas est donc impossible.

b) Donc $V \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Le groupe des automorphismes de V est alors S_3 (on détaille les différentes applications f possibles : on doit avoir $f((0,0)) = (0,0)$, alors $f((1,0)) = (1,0)$ ou $(0,1)$ ou $(1,1)$. Dans le premier cas, soit $(f(0,1)) = (0,1)$ et alors $f = \mathrm{Id}$, soit $f((0,1)) = (1,1)$ et alors f "transpose" $(0,1)$ et $(1,1)$, etc ...)

Quelles sont alors les possibilités d'homomorphisme $\phi : H_i \to \mathrm{Aut}(V) \cong S_3$? Toujours pour des raisons d'ordre, si $< h >= H_i$, $\phi(h) = \mathrm{Id}$, auquel cas, $G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, d'où G est commutatif et on se heurte au même problème que ci-dessus, c'est à exclure, soit $\phi(h)$ est une permutation circulaire. On obtient alors une seule structure de groupe non-commutatif de ce type : $(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \times_\phi \mathbb{Z}/3\mathbb{Z}$ (il faut se convaincre que les 2 choix possibles donnent 2 groupes isomorphes).

Cas 2. Si G ne possède qu'un 3-Sylow $H \lhd G$ avec $H \cong \mathbb{Z}/3\mathbb{Z}$ et $\mathrm{Aut}(H) \cong \mathbb{Z}/2\mathbb{Z}$. On a toujours $V \cap H = \{1\}$ où V est un 2-Sylow. Alors $G \cong H \times_\phi V$ où $\phi : V \to \mathrm{Aut}(H)$.

Il y a 2 cas possibles :

a) $V \cong \mathbb{Z}/4\mathbb{Z}$ et $\phi : \mathbb{Z}/4\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ est soit trivial, ce qui conduit au cas commutatif $\mathbb{Z}/3/\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, soit $\phi(1) = 1$, d'où un seul cas non commutatif : $\mathbb{Z}/3/\mathbb{Z} \times_\phi \mathbb{Z}/4\mathbb{Z}$.

b) $V \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ et $\phi : \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2/\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ est soit trivial, ce qui conduit au cas commutatif $\mathbb{Z}/3/\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2/\mathbb{Z}$, soit ϕ envoie un des éléments, différent de $(0,0)$ sur 1 (et on complète pour que cela définisse un homomorphisme ; il ya 3 possibilités, mais finalement cela donne la même situation), d'où un seul cas non commutatif : $\mathbb{Z}/3/\mathbb{Z} \times_\phi (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2/\mathbb{Z})$.

Chapitre 4

Appendice : SUITES EXACTES

Définition 4.0.3 *On dit qu'une suite d'homomorphismes de groupes*

$$F \xrightarrow{f} G \xrightarrow{g} H$$

est exacte si $\ker(g) = im(f)$.

Plus généralement, une suite

$$\cdots \to F_{i-1} \to F_i \to F_{i+1} \to \cdots$$

est exacte si toutes les sous-suites à 3 termes le sont.

Exemples :

1) La suite $1 \to G \xrightarrow{f} G'$ est exacte ssi f est injective.

2) La suite $G \xrightarrow{f} G' \to 1$ est exacte ssi f est surjective.

3) Suites exactes courtes :

La suite $1 \to F' \xrightarrow{f} F \xrightarrow{g} F'' \to 1$ est exacte ssi f est injective, g est surjective et $\ker(f) = \mathrm{im}(g)$.

Donnons un exemple : soit H un sous-groupe distingué d'un groupe G, alors la suite $1 \to H \to G \to G/H \to 1$ est exacte. Il en est ainsi, par exemple, de la suite $1 \to Sl(\mathbb{R}^2) \to Gl(\mathbb{R}^2) \xrightarrow{\det} \mathbb{R}^* \to 1$.

Définition 4.0.4 *On dit qu'une application $f : E \to F$ est rétractable si $\exists r : F \to E$ telle que $r \circ f = Id_E$.*

Une application $f : E \to F$ est sectionnable si $\exists s : F \to E$ telle que $f \circ s = Id_F$.

Remarque : une rétraction r est surjective (en effet : tout $x \in E$ peut s'écrire $x = r(f(x))$, donc est l'image par r d'un élément de F) et une section s est injective (en effet : $s(x) = s(y) \Rightarrow x = f(s(x)) = f(s(y)) = y$).

Lemme 4.0.2 *$f : E \to F$ est injective $\Leftrightarrow$ f est rétractable $\Leftrightarrow$ pour tout couple d'applications $u, v : X \to E$, $f \circ u = f \circ v \Rightarrow u = v$. De même, $f : E \to F$ est surjective $\Leftrightarrow$ f est sectionnable $\Leftrightarrow$ pour tout couple d'applications $u, v : F \to X$, $u \circ f = v \circ f \Rightarrow u = v$.*

Preuve : Si f est injective, on définit r par $r(f(x) = x,\ \forall x \in E$ et $r(y)$ quelconque, si $y \notin \mathrm{im}(f)$. Cette application r vérifie bien $rf = \mathrm{Id}_E$.

Supposons $f(x) = f(y)$ et considérons $X = \{a\}$ un singleton et $u, v : X \to E$ définies respectivement par $u(a) = x$, $v(a) = y$. Alors on a $f(u(a)) = f(v(a))$, d'où par hypothèse $u = v$ et donc $x = u(a) = v(a) = y$.

On procède de manière analogue pour la surjectivité.

Revenons aux homomorphismes de groupes. Dans ce cas, il n'est pas vrai, que si f est un homomorphisme de groupes, f est injective implique qu'il existe un *homomorphisme de groupes* $r : F \to E$ tel que $rf = \mathrm{Id}_E$. En effet, soit l'injection $5\mathbb{Z} \to \mathbb{Z}$. S'il existait $r : \mathbb{Z} \to 5\mathbb{Z}$, rétraction de l'injection canonique i, on aurait $r(1) = \pm 5$ car r doit être surjectif (donc doit envoyer un générateur - ± 1 - de $\mathbb{Z}$ sur un générateur de $5\mathbb{Z}$, d'où $r(i(5)) = r(5 \times 1) = 5r(1) = \pm 25$ ce qui est en contradiction avec $ri = \mathrm{Id}_E$.

On montrerait de même, utilisant par exemple $\mathbb{Z} \to \mathbb{Z}/5\mathbb{Z}$ que f surjective n'implique pas qu'il existe une section qui soit un homomorphisme de groupes.

Remarque : lorsqu'il s'agit d'homomorphismes (de groupes), si f vérifie la dernière des équivalences du lemme, avec u, v des homomorphismes, on dira que f est un monomorphisme (resp. épimorphisme).

Proposition 4.0.1 *Un homomorphisme de groupes est injectif ssi c'est un monomorphisme. De même, un homomorphisme de groupes* commutatifs *est surjectif ssi c'est un épimorphisme.*

Preuve : Il résulte du lemme précédent qu'un homomorphisme injectif est un monomorphisme. Inversement, soit $f : E \to F$ un monomorphisme. Soit $H = \ker(f)$ et $u : H \to E$ l'injection canonique, $v : H \to E$ défini par $v(h) = 1, \forall h$. Alors, $fu(h) = 1 = fv(h)$, ie. $fu = fv$, d'où $u = v$ càd. $H = \{1\}$.

Pour la surjectivité, il suffit de même de montrer que si f est un épimorphisme, alors f est surjective. Si f n'est pas surjective, alors il existe $y \in F$ tel que $y \notin \mathrm{im}(f)$. Soit $u : F \to F/\mathrm{im}(f)$ la surjection naturelle et $v : F \to F/\mathrm{im}(f)$ définie par $v(x) = 0, \forall x$. On a $u(y) \neq v(y) = 0$, donc $uf \neq vf$, or $uf = vf = 0$!

Théorème 4.0.6 *Pour toute suite exacte de groupes* $1 \to F \xrightarrow{f} E \xrightarrow{g} G \to 1$*, il y a équivalence de :*

i) $E \cong F \times G$ *;*

ii) f *est rétractable ;*

iii) g *est sectionnable par une section* s *telle que l'image de* s *soit contenue dans le centralisateur de* $im(f)$*.*

Preuve : i) $\Rightarrow$ ii) Si $E = F \times G$ et $f : F \to F \times G$ est $f(x) = (x, 1)$, il suffit de définir $r : E \cong F \times G \to F$ par $r((x, y)) = x$. Il est clair que c'est bien un homomorphisme et que $rf = \mathrm{Id}_E$.

i) $\Rightarrow$ iii) Définissons $s : G \to F \times G \cong E$ par $s(y) = (1, y)$. Cela définit bien une section de g et l'image de s est l'ensemble $\{1\} \times G$. Soit $I_f = \mathrm{im}(f) = F \times \{1\}$. Le centralisateur $C(I_f) = \{(x, y) | (x, y)(z, 1) = (z, 1)(x, y)\}$ contient clairement les éléments de la forme $(1, y)$.

ii) $\Rightarrow$ i) Soit $r : E \to G$ une rétraction de f. Elle est surjective (tout $x \in E$ peut s'écrire $x = r(f(x))$). Soit alors $\phi : E \to F \times G$ définie par $\phi(x) = (r(x), g(x))$. C'est un homomorphisme de groupes.

Il est surjectif. Soit en effet $(a, b) \in F \times G$, alors ce couple peut s'écrire $(a, b) = (r(x), g(y))$. Soit alors $z = y[fr(x^{-1}y)]^{-1}$. On a alors $r(z) = r(y)[r(x^{-1})r(y)]^{-1} = r(x) = a$ et $g(z) = g(y)g([fr(x^{-1}y)]^{-1}) = g(y) = b$, puisque $gf = 1$.

Il est injectif. Soit $x \in \ker(\phi)$, alors $(r(x), g(x)) = (1, 1)$. Or $\ker(g) = \mathrm{im}(f)$, donc $g(x) = 1 \Rightarrow x = f(y)$ pour un $y \in F$. D'où $r(x) = r(f(y)) = y = 1$ et $x = f(y) = f(1) = 1$.

iii) $\Rightarrow$ i) Soit donc s une section de g telle que son image soit contenue dans le centralisateur de $\mathrm{im}(f)$. Remarquons que s est alors injective (en effet, $s(x) = s(y) \Rightarrow x = gs(x) = gs(y) = y$).

Soit $\psi : F \times G \to E$ définie par $\psi((x,y)) = f(x)s(y)$. Vérifions que c'est un homomorphisme de groupes. On a $\psi((x,y)(x',y)) = \psi(xx',yy') = f(xx')s(yy') = f(x)f(x')s(y)s(y')$ et comme $s(y)$ appartient au centralisateur de I_f, $f(x')s(y) = s(y)f(x')$ et $\psi((x,y)(x',y)) = [f(x)s(y)][f(x')s(y')] = \psi((x,y))\psi((x',y'))$.

Montrons que ψ est injectif. Supposons donc $\psi((x,y)) = 1$ càd. $f(x)s(y) = 1$. Alors $1 = g(f(x)s(y)) = g(f(x))g(s(y)) = y$, d'où $f(x) = 1$. Or f est injective, donc $x = 1$.

L'homomorphisme ψ est aussi surjectif. Soit $x \in E$, alors $g[x(sg(x)^{-1})] = g(x)g(x)^{-1} = 1$, donc $x(sg(x)^{-1}) \in \ker(g) = \mathrm{im}(f)$ ie. il existe $y \in F$ tel que $f(y) = x(sg(x)^{-1})$. Alors $\psi(y, g(x)) = f(y)s(gx)) = x(sg(x)^{-1})sg(x) = x$.

Exemple : On a la suite exacte $1 \to O^+(\mathbb{R}^3) \xrightarrow{i} O(\mathbb{R}^3) \xrightarrow{\det} \{\pm 1\} \to 1$. Définissons $s : \{\pm 1\} \to O(\mathbb{R}^3)$ par $s(\epsilon) = \epsilon \mathrm{Id}_{\mathbb{R}^3}$. Cela définit bien une section de det (en effet : $\det(s(1)) = 1$ et $\det(s(-1)) = -1$). De plus, les éléments de l'image de s, $\{\pm \mathrm{Id}_{\mathbb{R}^3}\}$, commutent à tout élément de $O(\mathbb{R}^3)$, donc à l'image de f. On peut donc appliquer le théorème et conclure que $O(\mathbb{R}^3) \cong O^+(\mathbb{R}^3) \times \mathbb{Z}/2\mathbb{Z}$.

Remarque : Dans le cas d'une suite exacte de groupes commutatifs $0 \to E \xrightarrow{f} F \xrightarrow{g} G \to 0$, f rétractable équivaut à g sectionnable qui équivaut encore à $F \cong E \times G$ et on a : $F = \mathrm{im}(f) \cdot \mathrm{im}(s)$ où s est une section de g.

Théorème 4.0.7 *Soit $E \times_\phi F$ un produit semi-direct de groupes. Notons $j : E \to E \times_\phi F$ et $p : E \times_\phi F \to F$ les homomorphismes canoniques (càd. $j(e) = (e,1)$ et $p(e,f) = f$). Alors la suite $1 \to E \xrightarrow{j} E \times_\phi F \xrightarrow{p} F \to 1$ est exacte et $s : F \to E \times_\phi F$ définie par $s(f) = (1,f)$ est une section de p.*

Preuve : La suite est exacte : en effet, j est injective, p est surjective et $pj(e) = p((e,1)) = 1$, d'où $\mathrm{im}(j) \subset \ker(p)$. De plus, $(e,f) \in \ker(p) \Leftrightarrow p((e,f)) = f = 1$, d'où $(e,f) \in \mathrm{im}(j)$.

s est un homomorphisme de groupes car $s(ff') = (1,ff') = (1\phi(1)(1), ff') = (1,f)(1,f') = s(f)s(f')$.

En outre, $ps(f) = f,\ \forall f \in F$.

Réciproquement :

Théorème 4.0.8 *Soit $1 \to E \xrightarrow{f} F \xrightarrow{p} G \to 1$ une suite exacte de groupes. Si g est sectionnable et si s est une section de p, alors il existe $\phi : G \to Aut(f(E))$, défini par $\phi(g)(f(e)) = s(g)f(e)s(g)^{-1}$, tel que $F \cong f(E) \times_\phi G$ (ou encore utilisant l'isomorphisme de E avec $f(E)$, $F \cong E \times_\phi G$).*

Preuve : Comme la suite est exacte, on a $f(E) = \ker(g) \lhd F$. Par conséquent, $\phi(g)(f(e)) = s(g)f(e)s(g)^{-1}$ est bien élément de $f(E)$, donc $\phi(g)$ définit bien un automorphisme de $f(E)$. On vérifie aussi immédiatement que ϕ est un homomorphisme.

Soit à présent $u : f(E) \times_\phi G \to F$ l'application définie par $u((f(e),g)) = f(e)s(g)$.

C'est un homomorphisme de groupes : $u((f(e),g)(f(e'),g')) = u((f(e)\phi(g)(f(e')), gg') = u((f(e)s(g)f(e')s(g)^{-1}, gg') = f(e)s(g)f(e')s(g)^{-1}s(g)s(g') = f(e)s(g)f(e')s(g')$

$= u((f(e),g)u(f(e'),g')$.

Il est injectif : $f(e)s(g) = 1 \Rightarrow 1 = p(f(e)s(g)) = pf(e)ps(g) = 1 \times g = g$, donc $g = 1$ et par conséquent, $f(e) = 1$.

Il est surjectif : Soit $x \in F$, alors $x = xs(p(x))^{-1}s(p(x))$. Or $p(xs(p(x))^{-1}) = p(x)p(x)^{-1} = 1$, d'où $xs(p(x))^{-1} \in \ker(p) = \mathrm{im}(f)$, ie. $\exists e \in E$ tq. $xs(p(x))^{-1} = f(e)$. D'où $u((f(e),p(x)) = f(e)s(p(x)) = x$.

Retenons donc que pour une suite exacte $1 \to E \xrightarrow{f} F \xrightarrow{p} G \to 1$, si f est rétractable, alors $F \cong E \times G$, produit direct, si g est sectionnable, alors on peut seulement conclure que $F \cong E \times_\phi G$, un produit semi-direct.

Chapitre 5

GROUPES ET GEOMETRIE

Dans ce chapitre, nous allons donner une application de la théorie des groupes à la géométrie. En particulier, nous allons chercher les sous-groupes finis du groupe orthogonal de $\mathbb{R}^2$ et $\mathbb{R}^3$.

5.1 Le groupe orthogonal

Rappelons que si (E, q) est un espace euclidien réel de dimension finie (on pourrait se contenter de supposer que q est une forme quadratique non dégénérée), alors les endomorphimes u de E qui conservent le produit scalaire ie. tels que $q(u(x)) = q(x),\ \forall x \in E$ sont appelés transformations orthogonales (ou isométries) de E pour q. L'ensemble de ces transformations forme un sous-groupe de $Gl(E)$ appelé groupe orthogonal de q et noté $O(E, q)$ (ou simplement $O(E)$ s'il n'y a pas de doute sur le produit scalaire).

Rappelons aussi qu'une application linéaire est orthogonale ssi elle transforme une base orthonormée en une base orthonormée. Une matrice réelle $n \times n$ est orthogonale ssi ses vecteurs colonnes (ou lignes) forment une base orthonormée de l'espace euclidien $\mathbb{R}^n$. On montre qu'une matrice A est orthogonale ssi elle vérifie ${}^tAA = I \Leftrightarrow {}^t A = A^{-1}$.

L'ensemble des matrices orthogonales forme un sous-groupe de $Gl(n, \mathbb{R})$, noté $O(n, \mathbb{R})$. Il suffit pour cela de constater qu'une matrice orthogonale A représente une transformation orthogonale u dans une base orthonormée $\mathcal{E}$ de E ie. $A = \mathrm{Mat}(u, \mathcal{E})$. En effet, A est la matrice de passage d'une base orthonormée à une base orthonormée, par conséquent les vecteurs colonnes $\{u(e_1), \ldots, u(e_n)\}$ de A forment une base orthonormée de $\mathbb{R}^n$, càd. $\|u(e_i)\| = 1$ et $< u(e_i), u(e_j) >= 0,\ i \neq j$. Conséquence u est une isométrie. Inversement, si u est orthogonale, sa matrice dans une base orthonormée est orthogonale.

Définition 5.1.1 *Etant donné un endomorphisme f d'un espace vectoriel réel E, un sous-espace V de E est dit irréductible sous f si $f(V) \subset V$ (ie. V est f-stable) et si, pour tout sous-espace W de V, $f(W) \subset W \Rightarrow W = \{0\}$ ou $W = V$.*

Théorème 5.1.1 *Soit f un endomorphisme d'un espace vectoriel réel E. Alors il existe un sous-espace V de E irréductible sous f et* $\dim V \leq 2$.

Preuve : Rapportons E à une base $\mathcal{E}$. Alors soit $A = \mathrm{Mat}(f, E)$. On peut donc considérer A comme un endomorphisme de $\mathbb{R}^n$. Mais on peut aussi considérer l'endomorphisme de $\mathbb{C}^n$ représenté par A.

Le polynôme caractéristique de A est à coefficients réels (puisque A est à coefficients réels), par conséquent ses racines sont ou bien réelles, ou bien complexes conjuguées.

Si A admet une valeur propre réelle, $\lambda \in \mathbb{R}$, alors il existe un vecteur propre $x \in \mathbb{R}^n$. Le sous-espace engendré par x est alors f-stable et irréductible (puisque de dimension 1).

Sinon, soit $x \in \mathbb{C}^n$ un vecteur propre correspondant à la valeur propre λ. Si $\overline{x}$ désigne le vecteur dont les coordonnées sont les conjugués des coordonnées de x, $\overline{x}$ est un vecteur propre pour la valeur propre $\overline{\lambda}$ (en effet : $f(\overline{x}) = A\overline{X} = \overline{AX} = \overline{f(x)} = \overline{\lambda x} = \overline{\lambda}\overline{x}$).

Je prétends que le sous-espace H engendré par $y = x+\overline{x}$ et $z = \frac{1}{i}(x-\overline{x})$ est un sous-espace f-stable de $\mathbb{R}^n$ de dimension 2 - car x et $\overline{x}$ sont des vecteurs propres correspondants à 2 valeurs propres distinctes - (calculons $f(\alpha y + \beta z) = \alpha f(y) + \beta f(z) = \alpha f(x) + \alpha f(\overline{x}) + (\beta/i)f(x) - (\beta/i)f(\overline{x}) = \alpha\lambda x + \alpha\overline{\lambda}\overline{x} + (\beta/i)\lambda x - (\beta/i)\overline{\lambda}\overline{x}$, puis écrivons $\lambda = a + ib$. En effectuant, on trouve que $f(\alpha y + \beta z) = (\alpha a + \beta b)y + (\beta a - \alpha b)z$ (*)).

D'autre part, si $W \subset H$ est un sous-espace strict f-stable, alors $f(W) \subset W$. Mais $\dim W \leq 1$. Si $\dim W = 1$, il existe $\alpha, \beta \in \mathbb{R}$ tels que $W =< \alpha y + \beta z >$ et $f(W) \subset W$ signifie alors que il existe $\mu \in \mathbb{R}$ (à la fois $f(\alpha y + \beta z)$ et $\alpha y + \beta z$ sont dans $\mathbb{R}^n$) tel que

$$f(\alpha y + \beta z) = \mu(\alpha y + \beta z).$$

Le calcul ci-dessus donne alors (utilisant (*)) le système

$$\begin{array}{rcl} (a-\mu)\alpha + b\beta & = & 0 \\ -b\alpha + (a-\mu)\beta & = & 0 \end{array}$$

dont le déterminant est $(a-\mu)^2 + b^2$. Or $\lambda \notin \mathbb{R}$, donc $b \neq 0$ et par conséquent ce déterminant est non nul. La seule solution est donc $\alpha = \beta = 0$ ou $W = \{0\}$.

Corollaire 5.1.1 *Pour toute transformation orthogonale u d'un espace euclidien réel E, E est somme directe (orthogonale) de sous-espaces V_i irréductibles sous u de dimension 1 ou 2.*

Cela va résulter du lemme suivant :

Lemme 5.1.1 *Si $u \in O(E,q)$ et si V est u-stable, alors $V^\perp$ est u-stable.*

Preuve : Comme $u(V) \subset V$ et u injective, $u(V) = V$, d'où aussi $u^*(V) = u^{-1}(V) = V$ (car u orthogonale ssi $u^* = u^{-1}$). Soit alors $x \in V^\perp$, pour tout $y \in V$, $< u(x), y >=< x, u^*(y) >= 0$ puisque $u^*(y) \in V$. Donc $u(x) \in V^\perp$.

Preuve du corollaire : On fait une récurrence sur la dimension de E. Si $\dim E = 1$, il n'y a rien à démontrer.

Supposons donc $\dim E \geq 2$. D'après le théorème, on sait qu'il existe $V \subset E$, u-stable, irréductible, de dimension ≤ 2. Alors $V^\perp$ est aussi u-stable, de dimension $< n$. Par hypothèse de récurrence, $V^\perp$ est somme directe orthogonale de sous-espaces V_i, u-stables, irréductibles, de dimension ≤ 2, donc aussi $E = V \oplus V^\perp$.

Ce corollaire permet donc de ramener l'étude des transformations orthogonales de E à l'étude des transformations orthogonales en dimension 1 ou 2.

5.1.1 Les groupes $O(E)$ pour $\dim E = 1$ ou 2

Lorsque la dimension de E est 1 et $u \in O(E)$, alors $\forall x \in E, u(x) = ax$ et $q(u(x)) = q(x) \Leftrightarrow a^2x^2 = x^2$ autrement dit, $a^2 = 1$ ou $a = \pm 1$, donc $u = \pm id_E$.

Théorème 5.1.2 *Soit (E,q) un espace euclidien réel de dimension 2 et $u \in O(E)$. Alors il existe une base orthonormée dans laquelle la matrice de u s'écrit :*

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \text{ ou } \begin{pmatrix} a & b \\ b & -a \end{pmatrix} \text{ avec } a^2 + b^2 = 1.$$

Preuve : La matrice de u dans une base orthonormée est orthogonale, écrivons-la $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$. On doit alors avoir $a^2 + c^2 = b^2 + d^2 = 1$ et $ab + cd = 0$.

Si $b \neq 0$, alors $a = -cd/b$, d'où $c^2(b^2 + d^2) = c^2 = b^2$ et par conséquent $c = \epsilon b$ où $\epsilon = \pm 1$. On en déduit encore $ab + \epsilon bd = 0 \Rightarrow a = -\epsilon d$. On a aussi $1 = a^2 + c^2 = a^2 + (\epsilon b)^2 = a^2 + b^2$.

Si $b = 0$, on a $d^2 = 1$ et $c = 0$, d'où le résultat.

Remarque : Les éléments de $O(2)$ de déterminant $+1$ forment un sous-groupe distingué de $O(2)$, noté $SO(2)$ ou $O^+(2)$. Ce sont les *rotations*.

Dans le cas général, il existe donc une base orthonormée de E dans laquelle la matrice d'une transformation orthogonale est de la forme :

$$\begin{pmatrix} I_p & 0 & 0 & \dots & 0 \\ 0 & -I_q & 0 & \dots & 0 \\ 0 & 0 & R_1 & \dots & 0 \\ 0 & 0 & 0 & \dots & R_s \end{pmatrix}$$

où I_n désigne la matrice unité d'ordre n et R_i une matrice du type de celles du théorème (il suffit en effet de prendre une décomposition de E en sous-espaces irréductibles $T = \oplus V_i$. Ceux-ci sont de dimension 1 ou 2, on prend dans chacun une base orthonormée, on obtient ainsi une base orthonormée dans laquelle la matrice est du type voulu).

5.2 Sous-groupes finis de $SO(\mathbb{R}^2)$ et $SO(\mathbb{R}^3)$

Soit $(E, <, >)$ un espace euclidien réel, de dimension finie, S la sphère unité de E et $O(E)$ le groupe orthogonal de E.

Définition 5.2.1 *On dit qu'une opération d'un groupe G sur un ensemble E est transitive si elle n'a qu'une seule orbite ie. $\forall x, y \in E$, il existe $g \in G$ tq. $y = gx$.*

Lemme 5.2.1 *Les groupes $O(E)$ et $SO(E)$ opèrent transitivement sur S. La restriction $g \mapsto g_{|S}$ est un homomorphisme injectif.*

Preuve : Etant donnés deux points de S, il suffit de les prolonger chacun en une base orthonormée (directe) pour constater qu'il existe une isométrie envoyant l'un sur l'autre. Il y a donc une seule orbite sous $O(E)$ ($SO(E)$).

Soit ϕ définie par $\phi(g) = g_{|S}$. Cette application est clairement un homomorphisme de groupes. Le noyau est constitué des g tels que $g_{|S} = \mathrm{Id}_S$, or, si $\dim E = n$, g fixant (plus de) $n + 1$ points "indépendants" est nécessairement l'identité de E.

Remarque : une bijection linéaire f de E qui envoie S sur lui-même est nécessairement une isométrie.

Soit $x \in E$ et H_x l'hyperplan orthogonal à x.

Théorème 5.2.1 *Les stabilisateurs $O(E)_x$ (resp. $SO(E)_x$) et $O(H_x)$ (resp. $SO(H_x)$) sont isomorphes. La sphère S et l'ensemble $O(E)/O(E)_x$ sont isomorphe en tant que $O(E)$-ensembles.*

Preuve : Soit $g \in O(E)$, alors $g(x) = x \Rightarrow g(H_x) = H_x$, donc $g_{|H_x} \in O(H_x)$. Soit $\phi : O(E) \to O(H_x)$ définie par $\phi(g) = g_{|H_x}$.

C'est un homomorphisme injectif (un élément g du noyau fixe H_x et $x \notin H_x$, donc g fixe $n + 1$ points "indépendants", d'où $g = \mathrm{Id}$).

Il est surjectif car si $f \in O(H_x)$, en prenant g telle que $g_{|H_x} = f$ et $f(x) = x$, on a bien $g \in O(E)$ et $\phi(g) = f$.

Pour tout $x \in S$, l'application $\phi_x : O(E)/O(E)_x \to S$ telle que $\phi(gO(E)_x) = gx$ est bien définie (car $g' \in gO(E)_x \Rightarrow g^{-1}g' \in O(E)_x \Rightarrow g^{-1}g'x = x \Rightarrow gx = g'x$), surjective (par transitivité de l'opération) et injective ($gx = g'x \Rightarrow g' \in O(E)_x$ par définition du stabilisateur) et cette application commute à l'opération de $O(E)$.

5.2.1 Sous-groupes de $SO(\mathbb{R}^2)$

Il est clair que $SO(\mathbb{R}^2)$ est isomorphe à $S = \{z \in \mathbb{C} | \|z\| = 1\}$ (l'isomorphisme consiste à envoyer la rotation d'angle θ sur le complexe $e^{i\theta}$). Or :

Lemme 5.2.2 *Soit K un corps (fini ou non), tout sous-groupe fini du groupe multiplicatif K^* est cyclique.*

Preuve : laissée en exercice (voir aussi TD).

Ici S est un sous-groupe de $\mathbb{C}^*$, donc tout sous-groupe fini G de $SO(\mathbb{R}^2)$ est isomorphe à un sous-groupe fini de $\mathbb{C}^*$, donc est cyclique. Si $|G| = n$, alors G est le groupe des rotations qui stabilisent un polygone régulier à n côtés. En effet : si $z = e^{i\theta}$ correspond à un générateur de G, alors G stabilise l'ensemble $\{1, e^{i\theta}, \dots, e^{i(n-)\theta}\}$, donc les n sommets d'un polygone régulier. Comme $g \in G$ est une isométrie, g transforme aussi côté en côté, d'où g stabilise le polygone ie. G est isomorphe à un sous-groupe du groupe des rotations qui stabilisent le polygone. Or, on a vu (cf. TD) que ce dernier est d'ordre n, donc G est isomorphe au groupe des rotations qui stabilisent un polygone régulier à n côtés.

Le stabilisateur d'une droite D de $\mathbb{R}^2$ est bien sûr un sous-groupe de $O(\mathbb{R}^2)$ de la forme $\{\mathrm{Id}_{\mathbb{R}^2}, \sigma\} \cong \mathbb{Z}/2\mathbb{Z} \cong \{-1, 1\}$ où σ désigne la symétrie par rapport à D. La suite $1 \to SO(\mathbb{R}^2) \to O(\mathbb{R}^2) \to \{-1, +1\} \to 1$ est exacte et scindée par $s : \{-1, 1\} \to O(\mathbb{R}^2)$ où $s(1) = \mathrm{Id}_{\mathbb{R}^2}, s(-1) = \sigma$ (on vérifie immédiatement que $\det \sigma = -1$), d'où $O(R^2) \cong SO(\mathbb{R}^2) \times_\phi \{-1, 1\}$.

Remarquons que, comme $s(-1)$ n'appartient pas au centralisateur de $SO(\mathbb{R}^2)$, donc le produit est bien semi-direct et non direct.

Exercice : montrer que si n est impair, $O(\mathbb{R}^n) \cong SO(\mathbb{R}^n) \times \{-1, 1\}$.

Soit alors G un sous-groupe fini de $O(\mathbb{R}^2)$, on peut écrire le diagramme suivant (où l'on voit que les diagrammes peuvent être utiles !) :

$$\begin{array}{ccccccccc} 1 & \longrightarrow & SO(\mathbb{R}^2) & \xrightarrow{j} & O(\mathbb{R}^2) & \xrightarrow{\det} & \{1,-1\} & \longrightarrow & 1 \\ & & \uparrow{\scriptstyle \alpha} & & \uparrow{\scriptstyle \beta} & & \uparrow{\scriptstyle \gamma} & & \\ 1 & \longrightarrow & G \cap SO(\mathbb{R}^2) & \xrightarrow{j'} & G & \longrightarrow & C & \longrightarrow & 1 \end{array}$$

où j, j', α, β sont les inclusions naturelles et C désigne le conoyau de j'. Les deux suites horizontales sont exactes. L'application γ est naturellement définie par $\gamma(\bar{g}) = \det(\beta(g))$ (on vérifie que c'est bien défini).

Alors l'image $\mathrm{im}(\gamma)$ est un sous-groupe de $\{-1, 1\}$ donc est 0 ou $\{-1, 1\}$. Dans le premier cas, cela signifie que $C = 0$, donc que $G = G \cap SO(\mathbb{R}^2)$ ie. $G \subset SO(\mathbb{R}^2)$, dans le deuxième cas $C = \{-1, 1\}$, et alors, comme G n'est pas contenu dans $SO(\mathbb{R}^2)$, on a $G \cap O^-(\mathbb{R}^2) \neq \emptyset$(rappelons que $O(\mathbb{R}^2) = SO(\mathbb{R}^2) \cup O^-(\mathbb{R}^2)$). Il existe donc une symétrie $\sigma \in G \subset O(\mathbb{R}^2)$. Alors $s(1) = \mathrm{Id}, s(-1) = \sigma$ constitue une section de $G \to \{-1, 1\}$ (comme d'ailleurs de det). Ainsi G est obtenu comme produit semi-direct d'un groupe cyclique et de $\mathbb{Z}/2\mathbb{Z}$, on vérifie que dans ce cas G est isomorphe à un groupe diédral.

On obtient ainsi le résultat :

Théorème 5.2.2 *Les sous-groupes finis de $O(\mathbb{R}^2)$ sont les groupes cycliques (ceux de $SO(\mathbb{R}^2)$ qui stabilisent un polygone régulier à n côtés) et les groupes diédraux D_n (ceux non contenus dans $SO(\mathbb{R}^2)$).*

5.2.2 Sous-groupes de $SO(\mathbb{R}^3)$

Remarquons tout d'abord qu'une rotation de $\mathbb{R}^3$ ie. un élément $g \neq \mathrm{Id}_{\mathbb{R}^3}$ de $SO(\mathbb{R}^3)$ laisse fixe exactement 2 points de la sphère S (les intersections de l'axe de rotation avec S). On appellera *pôles de g* ces points.

Nous allons énoncer le théorème fondamental, mais, nous ne donnerons qu'une idée de la démonstration, eu égard à sa longueur.

Théorème 5.2.3 *Soit G un sous-groupe fini de $SO(\mathbb{R}^3)$, d'ordre $n > 1$. Soit P l'ensemble des pôles des éléments de G ($\neq Id$). Alors :*

1. *G opère dans P et soit $\mathcal{O} = \{P_1, \ldots, P_k\}$ l'ensemble fini des orbites sous G.*
2. *Le stabilisateur G_x, dans G, de tout $x \in P$ est cyclique. Supposons $x \in P_j$ et soit $e_j = n/|P_j|$ ($e_j = |G_x|$) ; on a $2 \leq e_j \leq n$.*
3. *On a l'égalité $n\sum_{j=1}^{k}(1 - e_j^{-1}) = 2(n-1)$ (*).*
4. *Les seules valeurs possibles de k, des e_j et de n sont :*
   (a) *$k = 2$, $e_1 = e_2 = n$. Dans ce cas, G est un groupe cyclique d'ordre n ;*
   (b) *$k = 3$, $e_1 = 2$*
      i. *$e_2 = 2$ et $2e_3 = n$. Alors G est isomorphe au groupe diédral $D_{n/2}$.*
      ii. *$e_2 = e_3 = 3$ et $n = 12$. $G \cong A_4$, c'est le groupe du tétraèdre.*
      iii. *$e_2 = 3, e_3 = 4$ et $n = 24$. $G \cong S_4$, groupe du cube et de l'octaèdre.*
      iv. *$e_2 = 3, e_3 = 5$ et $n = 60$. $G \cong A_5$, groupe du dodécaèdre (8 sommets, 12 faces) et de l'icosaèdre(12 sommets, 20 faces).*

Remarquons tout de suite en corollaire que cela implique qu'il n'y a que 5 types de polyèdres réguliers !

Début de preuve : 1. Il s'agit seulement de montrer que si $x \in P, g \in G$, alors $g(x) \in P$. Supposons donc x pôle de g' càd. $g'(x) = x$. Alors $g(x) = gg'(x) = (gg'g^{-1})(g(x))$, d'où $g(x)$ est pôle de $gg'g^{-1}$, donc $g(x) \in P$.

Comme G est fini, il n'y a qu'un nombre fini de points fixes (2 pour chaque g), donc P est fini et P étant réunion disjointe des orbites, il n'y a qu'un nombre fini d'orbites, soit k ce nombre.

2. On vérifie que G_x est un sous-groupe du groupe des rotations du plan orthogonal à x. Or on a vu que (cf. cas $O(\mathbb{R}^2)$) les rotations d'un plan forment un sous-groupe de $\mathbb{C}^*$, d'où G_x est cyclique.

On a $2 \leq e_j \leq n$ puisque $\{\mathrm{Id}, g\} \subset G_x \subset G$.

Le fait que $e_j = |G|/|P_j|$ se déduit immédiatement de la bijection entre l'orbite P_j de x et $G \cdot x$.

3. Comptons de deux façons le nombre de couples (g, x), $g \in G$, x pôle de g.

Comme G_x contient e_j éléments, x est pôle de $e_j - 1$ rotations différentes de Id, donc dans P_j, chaque pôle est pôle de $e_j - 1$ rotations autres que Id. Il y a donc $(e_j - 1)|P_j|$ couples dans P_j. Comme $|P_j| = n/e_j$, on a $e_j|P_j| - |P_j| = n - |P_j| = n - n/e_j = n(1 - e_j^{-1})$. Il y a donc au total $\sum_{j=1}^{k} n(1 - e_j^{-1})$ couples.

Mais, d'autre part, il y a $n-1$ rotations $\neq$ Id dans G, chacune a 2 pôles, il y a donc $2(n-1)$ couples. Autrement dit :

$$\sum_{j=1}^{k} n(1-e_j^{-1}) = 2(n-1).$$

Pour obtenir les différents cas énoncés, c'est une pure question d'arithmétique. Ainsi k est nécessairement 2 ou 3, car $k=1$ est impossible (sinon $n=1$ exclu), de même que $k>4$ est impossible... etc...

Reconnaître les différents groupes est laissé en exercice (TD).

Chapitre 6

REPRESENTATIONS LINEAIRES DES GROUPES FINIS

6.1 Généralités

6.1.1 Définitions

Définition 6.1.1 *Une représentation d'un groupe fini G sur un $\mathbb{C}$-espace vectoriel V, de dimension finie, est un homomorphisme de groupes $\rho : G \to Gl(V)$. On dit aussi qu'on a muni V d'une structure de G-module (cela évite de faire référence à ρ, ce qui, s'il n'y a pas de confusion possible, allège les notations).*

On note souvent $\rho(g)(v)$ seulement par gv et on appelle *degré* de ρ la dimension de V.

Exemples : 1) La représentation triviale est donnée par $\rho(g) = \mathrm{Id}_V, \forall g$.

2) Soit G un groupe fini et V l'espace vectoriel engendré par G ie. $V = \{\sum_{g\in G} \lambda_g \cdot g; \lambda_g \in \mathbb{C}\} \cong V^{|G|}$. Alors l'application $G \to Gl(V)$ définie par $\rho(h)(\sum \lambda_g g) = \sum \lambda_g hg$ est bien un homomorphisme de groupes, donc définit une représentation de G, appelée représentation régulière de G.

Définition 6.1.2 *Un morphisme de représentations de G (ou morphisme de G-modules) est une application linéaire $\phi : V \to W$ telle que le diagramme suivant soit commutatif :*

$$\begin{array}{ccccc} & V & \stackrel{\phi}{\to} & W & \\ g & \downarrow & & \downarrow & g \ , \\ & V & \stackrel{\phi}{\to} & W & \end{array}$$

pour tout $g \in G$. Plus précisément, cela signifie que si $\rho : G \to GL(V)$ et $\tau : G \to GL(W)$ sont les 2 représentations, ϕ doit vérifier : $\tau(g) \circ \phi = \phi \circ \rho(g)$, pour tout $g \in G$.

Les deux représentations sont dites équivalentes *si ϕ est un isomorphisme.*

Remarquons que cela définit une relation d'équivalence sur l'ensemble des représentations linéaires de G.

On vérifie aisément que $\ker(\phi)$, $\mathrm{im}(\phi)$ et $\mathrm{Coker}(\phi) = W/\mathrm{im}(\phi)$ sont alors aussi des G-modules.

Définition 6.1.3 *Une sous-représentation d'une représentation $\rho : G \to GL(V)$ est un sous-espace vectoriel W de V invariant sous G ie. tel que $\forall g \in G, \forall w \in W,\ \rho(g)(w) \in W$.*

Une représentation $\rho : G \to Gl(V)$ est dite irréductible, si V n'admet pas de sous-espace invariant propre non nul.

Soient $\rho' : G \to Gl(V')$ et $\rho'' : G \to Gl(V'')$ deux représentations de G, alors l'application $\rho : G \to Gl(V' \oplus V'')$ définie par $\rho(g)(v' + v'') = \rho(g)(v') + \rho(g)(v'')$ est une représentation appelée somme directe de ρ' *et ρ'' qu'on note $\rho' + \rho''$.*

Etant données deux représentations $\rho : G \to Gl(V)$ et $\tau : G \to Gl(W)$, on peut définir une représentation $\sigma : G \to Gl(\mathrm{Hom}(V, W))$ par $\sigma(g)(\phi)(v) = \tau(g)(\phi(\rho(g^{-1})(v)))$, pour toute application $\phi \in \mathrm{Hom}(V, W)$, ce qu'on peut plus facilement "visualiser" sur le diagramme :

$$\begin{array}{ccc} V & \stackrel{\phi}{\to} & W \\ \rho(g^{-1}) \uparrow & & \downarrow \tau(g) \\ V & \stackrel{\sigma(g)(\phi)}{\to} & W \end{array} .$$

En particulier, on définit ainsi la représentation *duale* d'une représentation $\rho : G \to Gl(V)$, en prenant pour $\tau : G \to GL(\mathbb{C}) = \mathbb{C}^*$ la représentation triviale. Cela définit une structure de G-module sur le dual V^* de V par $\sigma : G \to V^*$ où $\sigma(g)(v^*) =^t (\rho(g^{-1})(v^*)$.

6.1.2 Complète réductibilité

Théorème 6.1.1 *Si W est une sous-représentation d'une représentation V d'un groupe **fini** G, alors il existe une sous-représentation W' de G telle que le G-module V soit la somme directe $W \oplus W'$ des G-modules W et W'.*

Preuve : Soit U un supplémentaire de W dans V et $\pi_0 : V \to W$ la projection sur W parallèlement à U. Posons

$$\pi(v) = \sum_{g \in G} g(\pi_0(g^{-1}v)) \in W.$$

C'est bien sûr une application linéaire et $v \in W \Rightarrow \pi_0(g^{-1}v) = g^{-1}v \Rightarrow \pi(v) = \sum_{g \in G} gg^{-1}v = |G|v$, ce qui prouve que π se surjecte sur W. Soit alors $W' = \ker(\pi)$.

W' est un sev de V invariant sous G (car $\pi(v) = 0 \Rightarrow \pi(hv) = \sum_{g \in G} g(\pi_0(g^{-1}hv))$. Posons $g' = (g^{-1}h)^{-1}$ ie. $g' = h^{-1}g$, alors $\pi(hv) = h \sum_{g' \in G} g'\pi_0(g'^{-1}v) = h\pi(v) = 0$) et $W' \cap W = \{0\}$ (car $v \in W' \cap W \Rightarrow 0 = \pi(v) = |G|v \Rightarrow v = 0$). Conclusion $V = W \oplus W'$.

Corollaire 6.1.1 *Toute représentation d'un groupe fini est une somme directe de représentations irréductibles.*

Preuve : on fait une récurrence sur la dimension de V. Si $\dim(V) = 1$, il n'y a rien à démontrer puisque les seuls sev de V sont précisément $\{0\}$ et V.

Supposons dès lors que, tout G-module de degré $\leq n$ est somme directe de représentations irréductibles. Soit V de degré $n+1$ une représentation linéaire de G. Alors, soit V est irréductible, et il n'y a rien à démontrer, soit $V = W \oplus W'$, où W est une sous-représentation non triviale de V et W' un supplémentaire. Mais alors, $\dim(W) \leq n$ et $\dim(W') \leq n$.

Autrement dit, par l'hypothèse de récurrence, W et W' sont sommes directes de représentations irréductibles, d'où V l'est.

Remarquons que l'intérêt de ce corollaire est de ramener l'étude de toutes les représentations aux seules représentations irréductibles.

Lemme 6.1.1 de Schur

Si V et W sont des représentations irréductibles de G et $\phi : V \to W$ une application G-linéaire (ie. un morphisme de représentations), alors :

1) soit ϕ est un isomorphisme, soit $\phi = 0$;
2) si $V = W$, alors $\phi = \lambda Id_V$, $\lambda \in \mathbb{C}$.

Preuve : On a la suite exacte d'espaces vectoriels

$$0 \to \ker(\phi) \to V \xrightarrow{\phi} \mathrm{im}(\phi) \to 0.$$

Or $\ker(\phi)$ et $\mathrm{im}(\phi)$ sont G-invariants, d'où $\ker(\phi) = 0$ ou $\ker(\phi) = V$ et $\mathrm{im}\phi = 0$ ou W.

$\ker(\phi) = 0 \Rightarrow \mathrm{im}(\phi) \neq 0 \Rightarrow \mathrm{im}(\phi) = W \Rightarrow \phi$ est un isomorphisme.

$\ker(\phi) = V \Rightarrow \phi = 0$.

Comme il s'agit de $\mathbb{C}$-espaces vectoriels, ϕ admet une valeur propre λ. Alors $\phi - \lambda\mathrm{Id}$ a un noyau non trivial, d'où $\phi - \lambda\mathrm{Id} = 0$.

6.1.3 Exemples

Voyons deux exemples : les groupes abéliens et le groupe symétrique S_3.

Remarquons tout d'abord que, si $\rho : G \to Gl(V)$ est une représentation, alors $\rho(g) : V \to V$ n'est pas, en général, G-linéaire. En effet, pour que $\rho(g)$ soit G linéaire, il faudrait que, pour tout $h \in G$, $\rho(g)(\rho(h)(v)) = \rho(h)\rho(g)(v)$, $\forall v \in V$. Mais ceci implique $\rho(gh) = \rho(g)\rho(h) = \rho(h)\rho(g) = \rho(hg)$, pour tout h, donc que $gh - hg \in \ker(\rho), \forall h$. Donc (au moins lorsque ρ est *fidèle* ie. ρ est injective), $g \in Z(G)$, centre de G.

En fait, $\rho(g)$ **est G-linéaire pour tout ρ ssi** $g \in Z(G)$.

Par conséquent, si G est abélien, pour toute représentation $\rho : G \to Gl(V)$, $\rho(g)$ est G-linéaire. D'où si V est une représentation irréductible de G, d'après le lemme de Schur, $\rho(g) = \lambda\mathrm{Id}_V$. Mais alors, tout sev de V est invariant sous G, autrement dit $\dim_{\mathbb{C}} V = 1$. On a ainsi montré :

Lemme 6.1.2 *Les représentations irréductibles d'un groupe abélien G sont précisément les homomorphismes de groupes $\rho : G \to \mathbb{C}^*(= Gl(\mathbb{C}))$.*

Exemple : Les représentations irréductibles de $\mathbb{Z}/n\mathbb{Z}$ sont données par les racines n-ième de l'unité (en effet, $\rho(1)$ doit être une racine primitive n-ième).

Considérons à présent le cas $G = S_3$.
Pour tout groupe symétrique S_n il y a deux représentations de degré 1, à savoir la représentation triviale et la représentation *alternée* càd. définie par $gv = \mathrm{sgn}(g)v$.

Par ailleurs, il y a une représentation naturelle $\rho : G \to Gl(\mathbb{C}^3)$. Etant donnée une base $\mathcal{E} = \{e_1, e_2, e_3\}$ de $\mathbb{C}^3$, on définit ρ par $ge_i = e_{g(i)}$ ou de manière équivalente $g(z_1, z_2, z_3) = (z_{g^{-1}(1)}, z_{g^{-1}(2)}, z_{g^{-1}(3)})$. Cette représentation n'est pas irréductible puisque la droite $< (1,1,1) >$ est invariante. Un supplémentaire en est $V = \{(z_1, z_2, z_3) | z_1 + z_2 + z_3 = 0\}$. La représentation $\rho : G \to Gl(V)$ est appelée la représentation *standard* de S_3. Elle est irréductible (en effet, sinon il existe un sous-espace de V, invariant sous S_3 de dimension 1, autrement dit il existe dans V un vecteur $z \neq 0$ tel que, pour tout $g \in S_3$, $gz = \lambda z$; pour $g = (12)$, cela entraîne $\lambda = z_2/z_1 = z_1/z_2 = z_3/z_3 = 1$, d'où $z_1 = z_2 = z_3 \Rightarrow 3z_1 = 0 \Rightarrow z = 0$). Nous verrons plus loin comment obtenir toutes les représentations à partir de celles-ci et que celles-ci sont les seules irréductibles.

6.1.4 Produit hermitien

Soit $\rho : G \to Gl(V)$ une représentation du groupe fini G dans un espace hermitien V. Rappelons, sans plus de précisions, qu'un espace hermitien est un espace vectoriel V muni d'un

produit hermitien $<,>$, càd. une application $V \times V \to \mathbb{C}$ telle que $< \alpha_1 x_1 + \alpha_2 x_2, \beta_1 y_1 + \beta_2 y_2 >= \alpha_1\overline{\beta_1} < x_1, y_1 > + \alpha_1\overline{\beta_2} < x_1, y_2 > + \alpha_2\overline{\beta_1} < x_2, y_1 > + \alpha_2\overline{\beta_2} < x_2, y_2 >$ et $< x, y >= \overline{< y, x >}$. On trouve en particulier que $< x, x > \in \mathbb{R}$. On suppose en plus que $< x, x > \geq 0$ et $< x, x >= O \Leftrightarrow x = 0$.

On peut transposer aux produits hermitiens les résultats sur les produits scalaires. En particulier, l'existence de bases orthonormales, la définition de transformations unitaires ie. $u \in \mathrm{End}V$ tq. $< u(x), u(y) >=< x, y >$. Si A est la matrice de u dans une base orthonormée, elle vérifie $A^{-1} = \overline{{}^tA}$. L'ensemble des automorphismes unitaires de V forme un sous-groupe de $Gl(V)$, appelé *groupe unitaire* de V et noté $U(V)$ ($U(\mathbb{C}^n)$ est le groupe des matrices $n \times n$ représentant les automorphismes unitaires de $\mathbb{C}^n$ muni du produit hermitien ordinaire ie. les matrices telles que $A^{-1} = \overline{{}^tA}$).

Lemme 6.1.3 *Toute représentation $\rho : G \to Gl(V)$ d'un groupe fini G, où V est un espace hermitien, est équivalente à une représentation unitaire càd. $\rho' : G \to U(V)$.*

Preuve : Remarquons d'abord que $\phi(x, y) = \frac{1}{|G|} \sum_{g \in G} < gx, gy >, \forall x, y, \in V$ est encore un produit hermitien. Il existe alors $h \in Gl(V)$ tel que $\phi(x, y) =< h(x), h(y) >$ (il suffit d'envoyer une base ϕ-orthonormée sur une base $<,>$-orthonormée). On vérifie alors que $\rho' = h \circ \rho \circ h^{-1}$ est une représentation unitaire de G équivalente à ρ.

Exemple : Si $V = \mathbb{C}^n$, l'application définie par :

$$< (x_1, x_2, \ldots, x_n), (y_1, y_2, \ldots, y_n) >= \sum_{i=1}^{n} x_i \overline{y_i}$$

est un produit hermitien sur $\mathbb{C}^n$, qui est le produit hermitien standard.

Soit G un groupe fini, et soit $V = F(G,\mathbb{C})$, l'espace vectoriel complexe des fonctions complexes. L'application

$$< \phi, \psi >= \frac{1}{|G|} \sum_{g \in G} \phi(g)\overline{\psi(g)}$$

définit une structure hermitienne sur V (on pourrait se contenter de supposer que G est un groupe - topologique - compact et remplacer $\sum$ par l'intégration le long de G).

6.2 Caractères d'une représentation

L'idée générale est qu'il suffit de connaitre toutes les valeurs propres de tous les $\rho(g)$ pour décrire la représentation. Ce qui bien sûr est peu réalisable. Mais il suffit en fait de moins : en effet, la connaissance des *sommes* $\sum \lambda_i^k$ des valeurs propres des puissances $\rho(g^k)$ pour un $g \in G$ équivaut à la connaissance des λ_i, valeurs propres de $\rho(g)$ (fonctions symétriques des racines d'un polynôme).

Définition 6.2.1 *Si V est une représentation de G, son caractère χ_V est la fonction $G \to \mathbb{C}$ définie par $\chi_V(g) = Tr(g_{|V})$, trace de g (ou plutôt $\rho(g)$) sur V.*

Rappelons que la trace d'un endomorphisme u est, par définition, la trace de la matrice qui représente u dans une base. On a les propriétés suivantes : $Tr(A) = Tr({}^tA)$, $Tr(A + B) = Tr(A) + Tr(B)$, $Tr(\lambda A) = \lambda Tr(A)$, $Tr(I_n) = n$, $Tr(AB) = Tr(BA)$, $Tr(B^{-1}AB) = Tr(A)$ (cette dernière relation montre que la notion est indépendante de la base choisie).

On a en particulier $\chi_V(hgh^{-1}) = \chi_V(g)$, autrement dit la fonction χ_V est constante sur les classes de conjugaison de G. C'est donc une fonction centrale. De plus, toujours, d'après la

dernière relation, **deux représentations équivalentes ont même caractère** (rappelons que 2 représentations $\rho : G \to Gl(V)$ et $\tau : G \to gl(W)$ sont équivalentes signifie qu'il existe un isomorphisme $f : V \to W$ tel que $\tau(g) = f \circ \rho(g) \circ f^{-1}$, pour tout $g \in G$).

Proposition 6.2.1 *Soient V, W des représentations de G. Alors $\chi_{V\oplus W} = \chi_V + \chi_W$, $\chi_{V^*}(g) = \chi_V(g^{-1}) = \overline{\chi_V(g)}$.*

Preuve : Pour montrer le premier résultat, on regarde la matrice A_g de g dans une base de $V \oplus W$ constituée de la réunion d'une base de V et d'une base de W. Elle est du type

$$A_g = \begin{pmatrix} A'_g & 0 \\ 0 & A''_g \end{pmatrix}$$

, d'où on déduit immédiatement le résultat.

Pour ce qui est de $\chi_V(g^{-1})$, On prend une représentation unitaire θ, équivalente à la représentation $\rho : G \to Gl(V)$, alors $\chi_\rho(g^{-1}) = \chi_\theta(g^{-1}) = Tr(\theta_{g^{-1}}) = Tr(\theta_g^{-1}) = Tr(\overline{{}^t\theta_g}) = Tr(\overline{\theta_g}) = \overline{\chi_{\theta(g)}} = \overline{\chi_\rho(g)}$.

Le théorème essentiel, qu'on admettra, est :

Théorème 6.2.1 *Les caractères des représentations irréductibles d'un groupe fini G forment une base orthonormale de $\mathcal{K}(G)$, ensemble des fonctions centrales de G ie. $\{f : G \to \mathbb{C}; f(h^{-1}gh) = f(g)\}$.*

Corollaire 6.2.1 *Si $\rho_1, \rho_2, \ldots, \rho_n$ sont les représentations irréductibles de G, alors toute représentation ρ de G s'écrit uniquement (à ordre et équivalence près) $\rho = \sum_{i=1}^n m_i\rho_i$ où $m_i =< \chi_\rho, \chi_{\rho_i} > \in \mathbb{N}$ (appelé* multiplicité *de ρ_i dans ρ).*

De plus, $< \chi_\rho, \chi_\rho >= \sum m_i^2 > 0$ et ρ est irréductible ssi $< \chi_\rho, \chi_\rho >= 1$.

Preuve : Supposons que ρ admette une décomposition irréductible $\rho = \sum n_i\rho_i$. Alors $< \chi_\rho, \chi_{\rho_i} >= n_i$ n'est autre que le nombre de sous-représentations irréductibles de ρ équivalentes à ρ_i, ce qui détermine n_i de manière unique (à équivalence près).

Il est d'autre part clair que $< \chi_\rho, \chi_\rho >= \sum m_i^2 > 0$.

Corollaire 6.2.2 *Soit ρ_i une représentation irréductible de degré d_i, et ρ_r la représentation régulière de G. Alors $< \chi_{\rho_r}, \chi_{\rho_i} >= d_i$.*

Si $\rho_1, \ldots, \rho_n$ sont les représentations irréductibles de G, alors $\sum_{i=1}^n d_i^2 = |G|$.

En particulier, G est abélien ssi toutes ses représentations irréductibles sont de degré 1.

Preuve : Il suffit de se rappeler ce qu'est la représentation régulière, à savoir que V est l'espace vectoriel dont une base est G. L'application $V \to V$ correspondant à $h \in G$ agit alors sur la base par $g \mapsto hg$, et par conséquent, si $h \neq e$, ne laisse invariant aucun élément de la base, autrement dit sa matrice n'a que des 0 sur la diagonale, d'où $Tr(h) = 0$. Conclusion : $\chi_r(e) = |G|$ et $\chi_r(g) = 0$ si $g \neq e$.

Calculons alors

$$< \chi_{\rho_r}, \chi_{\rho_i} >= \frac{1}{|G|}\sum_{g\in G} \chi_{\rho_r}(g)\overline{\chi_{\rho_i}(g)} = \frac{1}{|G|}\chi_{\rho_r}(e)\overline{\chi_{\rho_i}(e)} = \frac{1}{|G|}|G|d_i = d_i$$

(rappelons que $\chi_{\rho_i}(e) = d_i$ puisque la matrice de $\rho_i(e)$ est l'identité).

Mais $< \chi_{\rho_r}, \chi_{\rho_i} >$ n'est autre que la multiplicité de ρ_i dans χ_{ρ_r} et, par conséquent, $< \chi_{\rho_r}, \chi_{\rho_r} >= \sum_{i=1}^n d_i^2$.

D'autre part,

$$\frac{1}{|G|}\sum_{g\in G}\chi_{\rho_r}(g)\overline{\chi_{\rho_r}(g)} = \frac{1}{|G|}\chi_{\rho_r}(e)\overline{\chi_{\rho_r}(e)} = |G|$$

et par suite,

$$\sum_{i=1}^{n} d_i^2 = |G|.$$

Pour un groupe abélien, le nombre de classes de conjugaison est égal à $|G|$, on en déduit donc $d_i = 1,\ \forall i$. Inversement, si toutes les représentations irréductibles de G sont de degré 1, on en déduit que le nombre de classes de conjugaison est égal à $|G|$, autrement dit G est abélien.

Exercices : Trouver les représentations irréductibles :

1. d'un groupe cyclique ;
2. du groupe diédral D_n (on rappelle que D_n est le groupe de présentation $< s, t; s^2, t^n, stst >$). Il faut distinguer les cas n pair et n impair) ;
3. du groupe quaternionique $Q_n =< s, t; t^{2n}, s^2 = t^n, s^{-1}tst >$, groupe d'ordre $4n$.

Bibliographie

[1] S. LANG, Algèbre, Addison-Wesley.

[2] A. BOUVIER, D. RICHARD, Groupes, Herrmann.

[3] J.P. SERRE, Représentation linéaire des groupes finis.

[4] FULTON, HARRIS, Representations, Springer.