Master Mathématiques 1ère année

COMPLÉMENT DE THÉORIE DES GROUPES

Nicolas JACON

Université de Reims

Table des matières

Chapitre 1

Actions de groupes

1.1 Rappel sur les quotients

Dans cette première partie, nous rappelons la construction du quotient. Soient G un groupe de structure multiplicative et d'élément neutre e_G. Soit H un sous-groupe de G. On définit les deux relations ci-dessous :

- $x\mathcal{R}_1 y$ si et seulement si $xy^{-1} \in H$,
- $x\mathcal{R}_2 y$ si et seulement si $y^{-1}x \in H$.

Alors, on vérifie facilement que $\mathcal{R}_1$ et $\mathcal{R}_2$ sont des relations d'équivalences.

- La relation $\mathcal{R}_1$ est appelée *congruence à droite modulo* H. L'ensemble des classes d'équivalence est noté $H \setminus G$. La classe de congruence à droite d'un élément $x \in G$ est égal à Hx.
- La relation $\mathcal{R}_2$ est appelée *congruence à gauche modulo* H. L'ensemble des classes d'équivalence est noté G/H. La classe de congruence à gauche d'un élément $x \in G$ est égal à xH.

Le cardinal de l'ensemble G/H est appelée *l'indice* de H dans G et il est noté $[G : H]$.

Ces remarques nous permettent de démontrer le résultat important suivant.

Théorème 1.1.1 (Théorème de Lagrange) *Soit G un groupe fini et H un sous-groupe de G. Alors on a :*

$$o(G) = [G : H]o(H).$$

En particulier, l'ordre de H divise l'ordre de G.

Preuve. Le cardinal d'une classe d'équivalence de G/H est égale au cardinal de xH c'est à dire à l'ordre de H. Les classes d'équivalence réalisent une partition de G c'est à dire que tout élément de G est dans une et une seule classe d'équivalence (c'est une propriété générale des classes d'équivalence). On a donc $[G : H]$ classes d'équivalence, chacune de cardinal $o(H)$. Il en résulte que le cardinal de G est égal à $[G : H]o(H)$ d'où le résultat.

□

Ceci implique en particulier que si $x \in G$ alors $o(x)$ divise $o(G)$ et on a $x^{o(G)} = e_G$.

Avant d'étudier plus précisement les structures de ces classes de congruence attachées à un sous-groupe, nous nous intéressons à certains sous-groupes particuliers.

Définition 1.1.2 Soit G un groupe, un sous-groupe H est dit *normal* (ou *distingué*) si et seulement si :

$$\forall x \in G,\ xHx^{-1} = H.$$

On note alors $H \lhd G$. La caractírisation ci-dessus équivaut à dire que

$$\forall x \in G,\ xHx^{-1} \subset H.$$

L'exemple typique de sous-groupe normal est le centre d'un groupe. Un moyen simple de trouver des sous-groupes normaux est d'utiliser des morphismes de groupes. En effet, un sous-groupe est normal si et seulement si c'est le noyau d'un morphisme de groupes.

Exemple 1.1.3 Soit $GL_n(\mathbb{C})$ le groupes des matrices à n lignes et n colonnes à coefficients dans $\mathbb{C}$. Soit $SL_n(\mathbb{C}) := \{M \in GL_n(\mathbb{C}) \mid \det(M) = 1\}$. On a $SL_n(\mathbb{C}) = \mathrm{Ker}(\det)$ (on rappelle que le déterminant est un morphisme de $GL_n(\mathbb{C})$ dans $\mathbb{C}^*$). Il suit que $SL_n(\mathbb{C})$ est un sous-groupe normal de $GL_n(\mathbb{C})$ appelée le *groupe spécial linéaire*.

Remarque 1.1.4 La dfinition de groupes normaux fournit un nouveau critère pour déterminer si un groupe est produit direct de ses sous-groupes. Soit G un groupe et soient H_1 et H_2 deux sous-groupes de G. Alors $G = H_1 \times H_2$ si et seulement si

1. $H_1 \lhd G$ et $H_2 \lhd G$.
2. $H_1 \cap H_2 = \{e_G\}$.
3. $G = H_1H_2$.

A un groupe G et un sous-groupe H, on a associé un certain ensemble G/H, ensemble des classes de congruence à gauche modulo H. On se pose maintenant la question suivante : est-il possible de mettre une structure de groupe sur cet ensemble qui serait "compatible" avec la structure de groupe sur G ? le théorème suivant répond par l'affirmative à ce problème lorsque $H \lhd G$. Das ce cas, les classes de congruence à droite où à gauche sont les mêmes puisque $xH = Hx$ pour tout $x \in G$. On parlera donc seulement ici de classe de congruence et on note G/H l'ensemble de ses classes.

Théorème 1.1.5 *Soit G un groupe et soit $H \lhd G$. Soit $\pi : G \to G/H$ la surjection canonique qui associe à un élément de G sa classe de congruence modulo H. Alors, il existe sur G/H une unique structure de groupe tel que π soit un morphisme de groupe. Le groupe ainsi obtenu est appelé le groupe quotient G/H.*

Preuve. Soit $x \in G$. La surjection canonique π est définie par $\pi(x) = xH$. Supposons qu'on ait une loi interne " $*$ " sur G/H induisant une structure de

groupe sur cet ensemble et tel que π soit un homomorphisme de groupes. Alors, pour $(x, y) \in G^2$, on a :

$$\pi(x.y) = (x.y)H = xH * yH = \pi(x) * \pi(y).$$

La seule structure de groupe possible sur G/H tel que π soit un homomorphisme est donc celle définie par la formule $xH * yH := (xy)H$. Vérifions maintenant que cette loi confère bien une structure de groupe à G/H.

Il faut tout d'abord vérifier que cette loi est bien définie, c'est à dire qu'elle ne dépend pas des choix de x et de y dans les classes de congruences. Soit donc $x' \in G$ et $y' \in G$ tels que $xH = x'H$ et $yH = y'H$. On veut montrer qu'alors $(xy)H = (x'y')H$ c'est à dire que $y^{-1}x^{-1}x'y'H = H$. On a :

$$y^{-1}x^{-1}x'y' = y^{-1}y'y'^{-1}x^{-1}x'y'.$$

On a $x^{-1}x' \in H$ car $xH = x'H$ donc, comme H est normal, on obtient $y'^{-1}x^{-1}x'y' \in H$. De plus, comme $y^{-1}y' \in H$, on obtient $y^{-1}x^{-1}x'y' \in H$. On en déduit donc $y^{-1}x^{-1}x'y'H = H$. Donc la loi $xH * yH := (x.y)H$ définit une loi interne sur G/H. Elle est associative car la loi interne de G l'est. On a un élément neutre qui est $e_G H$ et chaque classe xH possède un inverse qui est $x^{-1}H$. On a donc bien une structure de groupe sur G/H tel que π est un homomorphisme.

□

Ainsi, il est possible de mettre une structure de groupe sur le quotient G/H lorsque H est un sous-groupe normal de G. Réciproquement, on peut montrer que si une telle structure de groupe existe sur G/H alors H est normal.

De la démonstration, on retient en particulier que la loi interne définie sur le groupe quotient est donnée par $xH * yH := (xy)H$ pour $xH \in G/H$ et $yH \in G/H$. Par abus de notation, on notera cette loi interne de la même manière que la loi du groupe G c'est à dire "." en général et parfois "+" lorsque le groupe est commutatif. Un élément de la classe de congruence sera parfois noté $\overline{x}$ pour $x \in G$ au lieu de xH. Si deux éléments x et y de G sont dans la même classe de congruence modulo H, c'est à dire si $\overline{x} = \overline{y}$ (ce qui équivaut à $x^{-1}y \in H$), on note $x \equiv y (\text{mod } H)$ et on dit que x est congru à y modulo H.

En résumé, le groupe quotient G/H est composé des classes de congruence $\overline{x}$ ($x \in G$) avec, pour $(x, y) \in G^2$, $\overline{x} = \overline{y}$ si et seulement si $x \equiv y (\text{mod } H)$ ou encore $xy^{-1} \in H$. La loi interne est donnée par :

$$\overline{x}.\overline{y} = \overline{x.y}$$

Il faudra bien avoir en tête que pour définir une application f de G/H dans un ensemble S, il faudra associer à chaque élément de G/H (et non de G) un élément de S. Ainsi, si $x \equiv y (\text{mod } H)$ c'est à dire si $xH = yH$ on devra avoir $f(\overline{y}) = f(\overline{x})$ sinon f n'est pas bien définie.

Théorème 1.1.6 (Théorème de factorisation pour les groupes) *Soient G et G' deux groupes et $f : G \to G'$ un morphisme de groupes. Soit $H \lhd G$ un sous-groupe normal de G tel que $H \subset \text{Ker}(f)$. Alors il existe un unique morphisme de groupes $\overline{f} : G/H \to G'$ tel que $\overline{f} \circ \pi = f$ où $\pi : G \to G/H$ est la surjection canonique.*

Supposons que l'on dispose de deux groupes G et G' et d'un sous-groupe normal H de G. Si $f : G \to G'$ est un morphisme de groupes tel que $H \subset \mathrm{Ker}(f)$. Alors, le théorème ci-dessus nous montre l'existence d'une unique application $\overline{f} : G/H \to G'$ telle que $\overline{f} \circ \pi = f$. Dans ce cas, on dira que f *passe au quotient.*

Théorème 1.1.7 (Théorème d'isomorphie pour les groupes) *Soient G et G' deux groupes et soit $f : G \to G'$ un morphisme de groupes. Alors on a un isomorphisme :*

$$G/\mathrm{Ker}(f) \simeq \mathrm{Im}(f).$$

□

Exemple 1.1.8 Considérons $GL_n(\mathbb{C})$ et son sous-groupe normal $SL_n(\mathbb{C})$. $SL_n(\mathbb{C})$ est en fait le noyau de l'application déterminant. L'application déterminant est bien sûr surjective dans $\mathbb{C}^*$. En effet si $\lambda \in \mathbb{C}^*$, $A := \begin{pmatrix} \lambda & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & \cdots & 1 \end{pmatrix}$ vérifie $\mathrm{Det}(\mathbb{Z}) = \lambda$. On en déduit que $GL_n(\mathbb{C})/SL_n(\mathbb{C}) \simeq \mathbb{C}^*$ car $\mathrm{Im}(\det) = \mathbb{C}^*$.

Définition 1.1.9 Un groupe G est dit *simple* si il n'a pas de sous-groupe normal non trivial.

Ce type de groupes est particulièrement important. En effet, étant donné un groupe fini G, si on dispose d'un sous-groupe normal H non trivial, on peut ramener l'étude de G à l'étude de H et du groupe quotient G/H. Alors, l'ordre de G/H est plus petit que l'ordre de G. Soit ce groupe est simple, soit on dispose d'un sous-groupe normal et on peut former un autre groupe quotient. On peut ainsi continuer jusqu'à trouver un groupe simple G' et esperer récupérer des propriétés de G à partir de G'.

Ainsi, les groupes simples finis peuvent être perçus comme les composantes de base de tous les groupes finis, de la même façon que tous les nombres entiers peuvent être décomposés en produit de nombres premiers.

La classification des groupes finis simples a été achevée en 1982 et est un des monuments des mathématiques du vingtième siècle. Le résultat est que ce sont les groupes quotients $\mathbb{Z}/p\mathbb{Z}$ avec p premie, les groupes alternés (qui sont des sous-groupes des groupes symétriques), les groupes dits de Chevalley (qui sont des sous-groupes de groupes de matrices associés à des considérations géométriques ...) ainsi que 26 sous-groupes tout à fait inclassables et appelées groupes sporadiques (dont le plus "gros", appelé "le Monstre", possède environ 8.10^{53} éléments !).

1.2 Actions de groupes

Soit S un ensemble et soit G un groupe. Une action de G sur S est une application :

$$\alpha : G \times S \to S$$

telle que :

1. $\forall (g_1, g_2) \in G^2,\ \forall x \in S, \alpha(g_1, \alpha(g_2, x)) = \alpha(g_1 g_2, x)$,

2. $\forall x \in S,\ \alpha(e_G, x) = x$.

On dit alors que G *agit sur* S ou que G *opère sur* S. Pour simplifier on notera $\alpha(x, s) = x.s$ (il ne faut cependant pas confondre l'action de G avec la loi interne de G !). Quand il y aura risque de confusion (en particulier lorsque $X = G$), nous essaierons d'adopter une autre notation pour l'action de G sur X, par exemple, $\alpha(x, s) = x * s$.

En particulier, étant donné un groupe G, G agit toujours sur lui même de deux façons différentes :

- via l'action
$$\begin{array}{ccc} G \times G & \to & G \\ (x, y) & \mapsto & x.y \end{array}$$
On parle *d'action par translation.*
- via l'action
$$\begin{array}{ccc} G \times G & \to & G \\ (x, y) & \mapsto & x.y.x^{-1} \end{array}$$
On parle *d'action par conjugaison.*

Ces deux actions seront particulièrement importantes dans la suite du chapitre.

Définition 1.2.1 Soit G un groupe agissant sur un ensemble X et $x \in X$. *Le stabilisateur de* x est par définition l'ensemble $G_x := \{g \in G, \mid g.x = x\}$. *L'orbite de* x sous l'action de G est l'ensemble $G.x := \{g.x \mid g \in G\}$.

Le stabilisateur d'un élément $x \in X$ sous l'action de G est aussi parfois noté $\mathrm{Stab}_G(x)$. Il est immédiat de vérifier que c'est un sous-groupe de G

On dit qu'une action est *transitive* si il n'existe qu'une seule orbite sous cette action (cette orbite étant bien entendu égale à X), on donne un exemple ci-dessous.

Exemple 1.2.2

1. Soit $GL_n(\mathbb{C})$ l'ensemble des matrices inversibles à n lignes et n colonnes et à coefficients dans $\mathbb{C}$. Alors, $GL_n(\mathbb{C})$ agit sur $\mathbb{C}^n$ via l'action :
$$\begin{array}{ccc} GL_n(\mathbb{C}) \times \mathbb{C}^n & \to & \mathbb{C}^n \\ (A, x) & \mapsto & Ax. \end{array}$$
Soit x un élément non nul de $\mathbb{C}^n$. Alors $A \in G_x$ si et seulement si $Ax = x$ c'est à dire si $(A - I)x = 0$. Donc le stabilisateur de x est l'ensemble des matrices inversibles avec valeur propre 1 et ayant x comme vecteur propre associé à cette valeur propre.
2. Plus généralement, le groupe linéaire $GL_k(V)$, ensemble des applications k-linéaires d'un k-espace vectoriel V (où k est un corps) agit sur V de la même manière.
3. L'ensemble $\mathfrak{S}_n$ des bijections de $\{1, \cdots, n\}$ vers $\{1, \cdots, n\}$ agit sur $\{1, \cdots, n\}$ de la façon suivante :
$$\begin{array}{ccc} \mathfrak{S}_n \times \{1, \cdots, n\} & \to & \{1, \cdots, n\} \\ (\sigma, j) & \mapsto & \sigma(j). \end{array}$$
L'orbite d'un élément $j \in \{1, \cdots, n\}$ est l'ensemble des $\sigma(j)$ pour $\sigma \in \mathfrak{S}_n$. C'est évidemment l'ensemble $\{1, \cdots, n\}$ en entier. On a donc une seule orbite et donc une action transitive.

Supposons que G agisse sur X. Soit $g \in G$ et soit

$$\sigma_g : X \to X$$

tel que $\sigma_g(x) = g.x$ pour tout $x \in X$. Alors σ_g est une bijection. En effet, cette application est évidement surjective car pour tout $x \in X$, on a $\sigma_g(g^{-1}.x) = x$ par les points 1. puis 2. de la définition d'action. Elle est aussi injective car $g.x = g.y$ pour $(x, y) \in X^2$ implique que $x = y$ par ces deux mêmes points. On a donc une application dans le groupe des bijections de X, le groupe symétrique $\mathfrak{S}_X$,

$$\begin{array}{ccc} G & \to & \mathfrak{S}_X \\ g & \mapsto & \sigma_g \end{array}$$

application dont on montre facilement que c'est un morphisme de groupes grâce aux propriétés 1. et 2. des actions de groupes. Réciproquement, la donnée d'un morphisme de groupe Ψ de G dans dans $\mathfrak{S}_X$ induit l'existence d'une action de G sur X :

$$\begin{array}{ccc} G \times X & \to & X \\ (g, x) & \mapsto & \Psi(g)(x) \end{array}$$

On vient donc de montrer la proposition suivante.

Proposition 1.2.3 *La donnée d'une action d'un groupe G sur un ensemble X est équivalente à la donnée d'un morphisme de groupe de G dans $\mathfrak{S}_X$.*

Il faut bien avoir en tête la démarche permettant passer d'un point de vue à un autre.

Proposition 1.2.4 *Soit G un groupe agissant sur un ensemble X. Soit x un élément de X. Alors, il existe une bijection entre l'orbite $G.x$ de x et l'ensemble des classes à gauche de G modulo G_x.*

Preuve. On construit une application Φ de G/G_x, l'ensemble des classes de congruences à gauche de G modulo G_x vers l'orbite $G.x$ de x. Pour $g \in G$, on pose $\Phi(gG_x) = g.x \in G.x$. Il faut vérifier que cette application est bien définie. Soit donc $g' \in G$ tel que $gG_x = g'G_x$ alors ${g'}^{-1}g \in G_x$. On en déduit donc $({g'}^{-1}g).x = x$ d'où $g.x = g'.x$. L'application Φ est donc bien définie. Elle est de plus clairement surjective et si $g.x = g'.x$ alors $({g'}^{-1}g).x = x$ et donc ${g'}^{-1}g \in G_x$. Ceci implique $gG_x = g'G_x$ donc elle est injective. Φ est donc une bijection entre G/G_x et $G.x$ ce qui prouve la proposition.

□

Attention, le stablisateur d'un élément n'est pas forcément un sous-groupe normal de G donc on n'a pas nécessairement une structure de groupe sur l'ensemble G/G_x.

Supposons qu'un groupe G agisse sur X. Alors ceci nous permet d'obtenir une partition de notre ensemble X.

En effet, il existe un ensemble S tel que $X = \coprod_{x \in S} G.x$ c'est à dire que $X = \cup_{x \in S} G.x$ et $G.x \cap G.y = \emptyset$ si $x \neq y$ sont dans S . Pour S, il suffit de prendre un représentant de chaque orbite : on obtient alors évidemment $X = \cup_{x \in S} G.x$ et si $G.x \cap G.y \neq \emptyset$ alors il existe $(g, g') \in G^2$ tel que $g.x = g'.y$ d'où $({g'}^{-1}g).x = y$ ce qui signifie que x et y sont dans la même orbite.

1.3 Premières conséquences

{cons1}

Une première conséquence, pratiquement directe, est le théorème suivant :

Théorème 1.3.1 (Théorème de Cayley) *Tout groupe fini est isomorphe à un sous-groupe du groupe symétrique.*

Preuve. G agit sur lui-même par translation d'où l'existence d'un morphisme de groupes :

$$\begin{array}{ccc} G & \to & \mathfrak{S}_{|G|} \simeq \mathfrak{S}_n \\ g & \mapsto & \sigma_g \end{array}$$

Ce morphisme est injectif car σ_g est l'identité si et seulement si $g = e_G$ (il suffit de considérre l'image de 1 par σ_g)

□

On donne ici deux exemples d'applications des premières propriétés étudiées ci-dessus. On considère l'ensemble des isométries directes laissant invariant un cube dans $\mathbb{R}^3$, c'est à dire, l'ensemble des transformations affines qui conservent les distances et les angles orientés. Ce groupe C agit naturellement sur l'ensemble des grandes diagonales du cubes $\mathcal{D}$. En effet, une isométrie conserve la distance et une grande diagonale du cube réalise le diamètre du cube. Ceci définit donc un morphisme

$$C \to \mathfrak{S}_{\mathcal{D}}$$

Cette application est surjective car chaque transposition est l'image d'une symétrie orthogonale d'axe la droite joignant le milieu des arêtes joignant les diagonales. Maintenant supposons que l'on dispose d'une isométrie qui fixe toutes les diagonales du cube. On vérifie facilement que c'est alors l'identité (la symétrie de centre O fixe ces diagonales mais on a supposé que l'isométrie est directe). Bref, notre morphisme est injectif et donc c'est un isomorphisme, on vient de montrer :

{iso}

Proposition 1.3.2 *Le groupe des isométries directes du cube est isomorphe à* $\mathfrak{S}_4$.

Un peu plus exotique : considérons le groupe $\mathrm{GL}_2(\mathbb{F}_2)$. Ce groupe agit sur l'ensemble des éléments de $\mathbb{F}_2^2$ de façon naturelle. Si $g \in \mathrm{GL}_2(\mathbb{F}_2)$ alors $g.x = 0_{\mathbb{F}_2^2}$ pour $x \in \mathbb{F}_2^2$ implique que $x = 0_{\mathbb{F}_2^2}$ donc G agit sur $\mathbb{F}_2^2 \setminus \{0\}$. On obtient ainsi un morphisme de groupes :

$$\varphi : \mathrm{GL}(\mathbb{F}_2) \to \mathfrak{S}_{\mathbb{F}_2^2 \setminus \{0\}} \simeq \mathfrak{S}_3$$

Montrons que φ est bijectif. Supposons que $g \in \mathrm{GL}_2(\mathbb{F}_2)$ vérifie $g.x = x$ pour tout $x \in \mathbb{F}_2^2 \setminus \{0\}$. Comme on a $g.0 = 0$, il suit que g est l'identité. Ceci implique que φ est injective. Concernant la surjectivité, on peut raisonner par cardinalité, trouver un élément de $\mathrm{GL}_2(\mathbb{F}_2)$ revient à se donner un vecteur non nul de $\mathbb{F}_2$: on a trois choix possibles et ensuite un autre vecteur non nul et non colinéaire à celui-ci, ce qui nous donne deux choix. Donc le cardinal est de 6, comme celui de $\mathfrak{S}_3$. On conclut donc qu'on a un isomorphisme de groupes :

$$\mathrm{GL}_2(\mathbb{F}_2) \simeq \mathfrak{S}_3$$

1.4 Equations aux classes

Le théorème suivant est fondamental :

Théorème 1.4.1 (Equation des classes) *Soit G un groupe agissant sur un ensemble fini X. Soit S un système de représentants des orbites (comme ci-dessus) c'est à dire $X = \coprod_{x\in S} G.x$ (réunion disjointe). Alors, on a :*

$$o(X) = \sum_{x\in S} [G : G_x],$$

où $o(X)$ désigne le cardinal de X.

Preuve. Soit $x \in S$. On utilise la proposition précédente, on a une bijection entre $G.x$ et l'ensemble des classes de congruence à gauche modulo G_x. Ceci signifie que $o(G.x) = [G : G_x]$. Or on a $o(X) = \sum_{x\in S} o(G.x)$ d'où le résultat. □

Théorème 1.4.2 (Formule de Burnside) *Soit X un ensemble fini et soit G un groupe fini agissant sur X. Pour tout $g \in G$, on pose :*

$$\mathrm{Fix}_G(g) := \{x \in X \mid g.x = x\}$$

On note $\mathrm{Orb}_X(G)$ l'ensemble des orbite sous l'action de G. On a alors :

$$\mathrm{Card}(\mathrm{Orb}_X(G)) = \frac{1}{o(G)} . \sum_{g\in G} \mathrm{Card}(\mathrm{Fix}_X(g))$$

Preuve. Considérons l'ensemble suivant :

$$\mathcal{F} := \{(x, g) \in X \times G \mid g.x = x\}$$

Nous allons calculer le cardinal de cet ensemble de deux manières différentes :

- d'une part, en fixant $g \in G$ et en regardant les $x \in X$ fixé par g, il suit :

$$\mathrm{Card}(\mathcal{F}) = \sum_{g\in G} \mathrm{Card}(\mathrm{Fix}_X(g))$$

- d'autre part, en raisonnant de façon inverse, on a aussi :

$$\mathrm{Card}(\mathcal{F}) = \sum_{x\in X} \mathrm{Card}(G_x).$$

  Maintenant, on sait que l'on a une bijection entre l'orbite $G.x$ et l'ensemble des classes de G module G_x. Ceci implique donc que

$$\mathrm{Card}(G_x) = \frac{\mathrm{Card}(G)}{\mathrm{Card}(G.x)}.$$

  Ensuite, on regroupe les éléments de chaque orbite :

$$\mathrm{Card}(\mathcal{F}) = \sum_{x\in \mathrm{Orb}_X(G)} \mathrm{Card}(G)$$

  soit encore

$$\mathrm{Card}(\mathcal{F}) = \mathrm{Card}(\mathrm{Orb}_X(G)) \,\mathrm{Card}(G)$$

et le résultat suit en comparant les deux formules.

□

Signalons la conséquence suivante concernant une classe particulière de groupes. Soit p un nombre premier. Un *p-groupe* est un groupe d'ordre une puissance de p. Par exemple $\mathbb{Z}/8\mathbb{Z}$ est un 2-groupe (il est d'ordre 2^3 avec 2 premier).

{X}

Proposition 1.4.3 *Soit G un p-groupe agissant sur un ensemble fini X et soit X^G l'ensemble des points fixes sous l'action de G c'est à dire $X^G = \{x \in X \mid \forall g \in G\ g.x = x\ \}$. On a alors :*

$$o(X^G) \equiv o(X)\ (mod\ p)$$

Preuve. D'après le théorème de Lagrange, l'ordre de chaque sous-groupe de G divise l'ordre de G. L'ordre d'un sous-groupe est donc une puissance de p car G est un p-groupe. Ainsi $[G : G_x]$ est soit divisible par p soit égale à 1. De plus, $[G : G_x] = 1$ si et seulement si $o(G_x) = o(G)$ c'est à dire si pour tout $g \in G$, on a $g.x = x$ c'est à dire si $x \in X^G$. On utilise maintenant l'équation des classes : tous les $[G : G_x]$ sont nuls modulo p excepté si $x \in X^G$ ce qui démontre la proposition.

□

{centre}

Corollaire 1.4.4 *Soit G un groupe fini. On considère l'action de G sur lui-même par conjugaison. Soit $\{x_1, \ldots, x_n\}$ un système de représentants des orbites : $G = \sqcup_{1 \leq j \leq n} G.x_j$, on a :*

$$o(G) = o(Z(G)) + \sum_{\substack{Card(G.x_j) \geq 2 \\ 1 \leq j \leq n}} \mathrm{Card}(G.x_j)$$

Preuve. On utilise l'équation aux classes. Soit $G.x$ une orbite associeé à l'action par conjugaison avec $x \in G$. Cette orbite est de cardinal 1 si et seulement si pour tout $y \in G$, on a $yxy^{-1} = x$ c'est à dire si et seulement si $x \in Z(G)$. Dans l'ensemble $\cup_{1 \leq j \leq n} G.x_j$, on a donc $o(Z(G)$ orbites à un élément d'où le résultat.

□

Ce dernier théorème est assez utile lorsque l'on veut étudier le centre d'un groupe, par exemple montrer qu'il est abélien ou montrer qu'il a un certain ordre. Donnons maintenant une série d'applications plus ou moins directes.

1.5 Quelques applications directes

Commençons par quelques applications générales :

Proposition 1.5.1 *Le centre d'un p-groupe n'est pas réduit à 1 élément.*

Preuve. G agit sur lui même par conjugaison comme dans la proposition 1.4.4. On utilise alors la proposition 1.4.3, on remarquant que l'ensemble X^G n'est autre que le centre de G. Bref, le centre est congru à 0 modulo p et donc est au moins de cardinal p (car $e_G \in Z(G)$) d'où le résultat.

□

{ab}

Corollaire 1.5.2 *Tout groupe d'ordre p^2 avec p premier est abélien.*

Preuve. Soit G un groupe d'ordre p^2. On sait déjà que son centre est non trivial d'après le travail précédent. Il est donc de cardinal p ou p^2. Supposons que celui-ci soit de cardinal p. Il est alors cyclique et il existe $g \in G$ tel que $Z(G) = \langle g \rangle$. Prenons un élément $h \in G \setminus Z(G)$ non trivial. Il ne peut être d'ordre p^2 sinon G serait cyclique et donc commutatif, ce qui contredit l'hypothse $o(Z(G)) = p$. On a donc $o(h) = p$. On a $\langle h \rangle \cap Z(G) = \{1\}$. En effet, sinon on aurait un élément non trivial dans les deux groupes. Cet élément serait d'ordre p et engendrerait les 2 groupes, ce qui contredirait l'hypothèse $h \notin Z(G)$.

Montrons que tout élément de G s'écrit de façon unique sous la forme $g^i h^j$ avec $(i, j) \in \{0, \ldots, p-1\}$. Pour ceci, remarquons que si l'on a $g_1 h_1 = g_2 h_2$ pour $(g_1, g_2) \in Z(G)^2$ et $(h_1, h_2) \in \langle h \rangle^2$ alors $g_2^{-1} g_1 = h_2 h_1^{-1} \in \langle h \rangle \cap Z(G)$ donc $g_1 = g_2$ et $h_1 = h_2$. Par cardinalité, on en déduit le résultat

Les éléments de $H = \langle h \rangle$ commutent avec ceux de $Z(G)$.

Donc G est les produit direct de deux groupes commutatifs, il est donc commutatif ce qui est une contradiction.

Théorème 1.5.3 (Théorème de Cauchy) *Soit G un groupe fini et p un nombre premier divisant l'ordre n de G. Alors G possède (au moins) un élément d'ordre p*

Preuve. On considère l'ensemble

$$\mathcal{A} := \{(x_1, \ldots, x_p) \in G^p \mid x_1 \ldots x_p = 1\}$$

On a une bijection entre $\mathcal{A}$ et G^{p-1} donc cet ensemble est de cardinal n^{p-1}. On vérifie alors que l'on a une action de $\mathbb{Z}/p\mathbb{Z}$ sur $\mathcal{A}$:

$$\begin{array}{rccc} \phi : & \mathbb{Z}/p\mathbb{Z} \times \mathcal{A} & \to & \mathcal{A} \\ & (k, (x_1, ..., x_p)) & \mapsto & (x_{1+k}, ..., x_{p+k}) \end{array}$$

où les indices s'entendent modulo p. Maintenant, un élément $(x_1, \ldots, x_p) \in \mathcal{A}$ est invariant sous cette action si et seulement si $x_1 = \ldots = x_p$. On a alors $x_1^p = 1$ et donc x_1 est d'ordre 1 ou p. On utilise alors l'équation des classes : il existe un sous-ensemble $\mathcal{X}$ d'éléments de $\mathcal{A}$ tel que

$$\sharp\mathcal{A} = \sum_{x \in \mathcal{X}} [H : H_x]$$

où $H = \mathbb{Z}/p\mathbb{Z}$. Si $H = H_x$ alors x est invariant sous l'action de $\mathbb{Z}/p\mathbb{Z}$ sur $\mathcal{A}$, sinon, l'ordre $[H : H_x]$ est égal à p. En prenant l'équation des classes modulo p, on obtient que le nombre d'éléments d'ordre p dans G est congru à -1 modulo p.

□

A partir de là, on peut assez en déduire le premier théorème de Sylow (l'existence de p-Sylow) que nous verrons dans le prochain chapitre et qui généralise dans un certain sens ce théorème.

1.6 Une application de la formule de Burnside

On se pose ici la question suivante : combien y a t-il de manière différentes de colorier un cube avec 3 couleurs différentes. A priori, le cube ayant six faces,

on obtient 3^6 possibilités, mais il faut prendre en compte le fait que lorsque l'on fait une rotation du cube avec un coloriage fixé, le coloriage doit être considéré comme le même.

Autrement dit, le groupe des rotations du cube agit sur l'ensemble des 3^6 coloriages possibles. Ce que l'on veut avoir c'est le nombre d'orbites sous cette action. On va donc utiliser la formule de Burnside. Le groupe des rotations du cube est composés de :

- l'identité
- les rotations d'axes passant par sommets opposés et d'angle $\pm 2\pi/3$ (il y en a 8),
- les rotations d'axe les centres des faces opposés et d'angle $\pm\pi$ (il y en a 3),
- les rotations d'axe les centres des faces opposés et d'angle $\pm\pi/2$ (il y en a 6),
- les rotations d'axe les centres des cotés opposés et d'angle $\pm\pi$ (il y en a 6),

(des orientations étant fixés une fois pour toutes.) On vérifie que ces rotations laissent bien stable le cube et on conclut par cardinalité en utilisant notre discussion dans la section 1.3.

Pour chacune des rotations, on regarde le cardinal du fixateur associeé c'est à dire le nombre de coloriage fixé par la rotation en question.

- pour l'identité, il y en a 3^6 (6 faces à fixer).
- pour les rotations d'axes passant par sommets opposés et d'angle $\pm 2\pi/3$, il y en a 3^2 (2 faces à fixer)
- les rotations d'axe les centres des faces opposés et d'angle $\pm\pi$, il y en a 3^4 (4 faces à fixer)
- les rotations d'axe les centres des faces opposés et d'angle $\pm\pi/2$, il y en a 3^3 (3 faces à fixer)
- les rotations d'axe les centres des cotés opposés et d'angle $\pm\pi$, il y en a 3^3 (3 faces à fixer)

On trouve alors :

$$\sum_{g\in G} \mathrm{Card}(\mathrm{Fix}_X(g)) = 3^6 + 8\times 3^2 + 6\times 3^3 + 3\times 3^4 + 6\times 3^3 = 1368$$

On obtient alors que le nombre d'orbites est 57 ce qui correspond au nombre de coloriage possibles.

Chapitre 2

Théorèmes de Sylow

Nous allons maintenant étudier précisemment la structure des groupes finis. Etant donné un groupe G, le but est ici de savoir combien G a de sous-groupes, quels sont les ordres de ces sous-groupes, lesquels sont normaux etc .... Les outils fondamentaux pour cette étude vont être donnés par les théorèmes de Sylow. La démonstration de ces théorèmes demande une compréhension en profondeur des actions de groupes et de l'équation des classes.

2.1 Enoncé des théorèmes

Les théorèmes de Sylow concerne l'étude d'un certain type de sous-groupes d'un groupe donné : les p-sous-groupes de Sylow (ou plus simplement p-Sylow) dont voici la dfinition.

Définition 2.1.1 Soit G un groupe fini d'ordre n, p un nombre premier qui divise n et p^α la plus grande puissance de p qui divise n. On appelle *p-sous-groupe de Sylow* de G tout sous-groupe de G d'ordre p^α.

Un p-sous-groupe de Sylow est donc en particulier un p-groupe. L'inverse n'est pas vrai car si $\alpha \geq 2$, un sous-groupe d'ordre p est un p-groupe mais pas un p-sous-groupe de Sylow.

Rappellons qu' un entier n se factorise de façon unique sous la forme :

$$n = \prod_{i=1}^{r} p_i^{\alpha_i}$$

où les p_i sont les nombres premiers divisant n et les $p_i^{\alpha_i}$ les plus grandes puissances de p qui divise n.

On dira que deux sous-groupes H et H' de G sont *conjugués* si il existe $g \in G$ tel que $H = gHg^{-1}$.

Théorème 2.1.2 (Théorèmes de Sylow) *Soit G un groupe fini d'ordre n et p un nombre premier divisant n.*

1. *Le nombre de p-sous-groupes de Sylow est congru à 1 modulo p.*
2. *Deux p-sous-groupes de Sylow quelconques sont conjugués.*

3. *Tout p-sous-groupe de G est contenu dans un p-sous-groupe de Sylow.*
4. *Le nombre de p-sous-groupes de Sylow divise m où* $n = p^\alpha m$ *et où* $\text{pgcd}(p, m) = 1$.

Ces théorèmes portent le nom du mathématicien norvégien Ludwig Sylow, qui les démontra en 1872. On voit qu'ils permettent de donner une idée sur le nombre de sous-groupes particuliers d'un groupe quelconque. En combinant ces théorème avec éventuellement d'autres résultats, on peut espérer obtenir des résultats importants sur un groupe fixé dont on connaît le cardinal (est-il simple ? produit direct de certains de ses sous-groupes ? isomorphe à un groupe déjà étudié ? etc.)

2.2 Démonstration des théorèmes

Nous allons démontrer ce théorème en quatre temps.

1. Préliminaire. Nous commençons par démontrer le résultat suivant. Soit G un groupe commutatif fini et p un nombre premier tel que p divise $o(G)$. Alors, G contient un élément d'ordre p et donc un sous-groupe d'ordre p.

On raisonne par récurrence sur l'ordre de G. Supposons tout d'abord que $o(G) = p$ alors le résultat est évident (il existe un élément x différent de e_G dans G d'ordre p.) On suppose maintenant la propriété satisfaite pour tout groupe H avec p divisant $o(H)$ et $o(H) < o(G)$. Notons tout d'abord que si G contient un élément x d'ordre pq pour un $q \in \mathbb{N}_{>0}$ alors $o(x^q) = p$. Supposons maintenant que G contienne x avec $o(x) = q$, $x \neq e_G$ et tel que p ne divise pas q. Soit H le sous-groupe engendré par x. H est normal car G est commutatif donc on peut former le groupe quotient G/H. On sait que p divise $o(G)$ et $o(H)$ est premier avec p donc p divise $o(G/H) = o(G)/o(H)$. Par récurrence, il existe donc $\overline{y} \in G/H$ tel que $o(\overline{y}) = p$ avec $y \in G$. Si $y^k = e_G$ alors $\overline{y}^k = e_{G/H}$ donc p divise k et donc p divise l'ordre de y. Il existe donc $r \in \mathbb{N}_{>0}$ tel que $o(y) = rp$ et alors y^r est d'ordre p.

2. Il existe un p-sous-groupe de Sylow dans G. On va montrer le résultat suivant : si G est un groupe d'ordre $p^\alpha m$ avec m premier avec p et $\alpha \geq 0$ alors G contient un sous-groupe d'ordre p^α (la différence avec l'énoncé est qu'ici, on n'exclut pas le cas $\alpha = 0$).

On montre cette propriété par récurrence sur α et m. Si $\alpha = 0$ ou $m = 1$, c'est évident. On suppose maintenant le théorème satisfait pour tout groupe G tel que $o(G') < o(G)$.

Supposons qu'il existe un sous-groupe H de G tel que $[G : H]$ soit premier avec p. Alors l'ordre de H est nécessairement de la forme $n'p^\alpha$ avec n' premier avec p et $n' < m$. On peut alors utiliser l'hypothèse de récurrence : il existe un p-sous-groupe de Sylow de H, il est donc d'ordre p^α, c'est donc un p-sous-groupe de Sylow de G. On peut donc supposer que tout sous-groupe H de G est tel que p divise $[G : H]$. Le groupe G agit par conjugaison sur lui-même :

$$\begin{array}{ccc} G \times G & \to & G \\ (x, y) & \mapsto & x * y := xyx^{-1} \end{array}$$

Sous cette action, on note que les éléments des orbites réduites à un élément correspondent exactement aux éléments du centre de G. En effet, si $G * x$ est

une telle orbite alors pour tout $g \in G$ on a $g * x = gxg^{-1} = x$ (attention, l'action de G sur x est ici définie par $g * x = gxg^{-1}$, il ne faut pas confondre l'action avec la loi interne). On utilise maintenant l'équation des classes : G est la réunion disjointe des orbites réduites à un élément et d'autres orbites $G * x_i$ pour $i = 1, \cdots, r$. On obtient :

$$o(G) = o(Z(G)) + \sum_{i=1}^{r} [G : G_{x_i}].$$

Comme p divise $o(G)$ et tous les $[G : G_{x_i}]$, p divise nécessairement $o(Z(G))$.

Le centre $Z(G)$ est un sous-groupe commutatif de G, le résultat précédent nous montre l'existence d'un sous-groupe H de $Z(G)$ d'ordre p. Comme c'est un sous-groupe de $Z(G)$, il est bien sûr normal (tout élément de G commute avec les éléments de H). On forme le groupe quotient G/H. Il est d'ordre $p^{\alpha-1}m$. Par récurrence, G/H contient un sous-groupe H_1 d'ordre $p^{\alpha-1}$. Soit $\pi : G \to G/H$ la surjection canonique et soit π' sa restriction à $\pi^{-1}(H_1)$. Cette restriction reste surjective dans H_1 et son noyau est $H \subset \pi^{-1}(H_1)$. On a donc $o(\pi^{-1}(H_1)) = o(H_1)o(H) = p^\alpha$. Ainsi $\pi^{-1}(H_1)$ est un sous-groupe d'ordre p^α.

3. Soient H un p-sous-groupe de G, P un p-sous-groupe de Sylow de G. Alors, il existe $g \in G$ tel que $H \subset gPg^{-1}$.

Soit $\mathcal{S}$ l'ensemble des p-sous-groupes de Sylow. $\mathcal{S} \neq \emptyset$ d'après 2.. G agit sur $\mathcal{S}$ par conjugaison :

$$\begin{array}{ccc} G \times \mathcal{S} & \to & \mathcal{S} \\ (g, K) & \mapsto & gKg^{-1} \end{array}$$

Le stabilisateur du p-sous-groupe de Sylow P est :

$$G_P = \{g \in G \mid gPg^{-1} = P\}.$$

P est un sous-groupe de G_P donc p^α divise $o(G_P)$ donc p ne divise pas $[G : G_P]$ donc ne divise pas le cardinal de $G.P := \{gPg^{-1} \mid g \in G\}$.

Maintenant H agit aussi par conjugaison sur $G.P$. Comme H est un p groupe, les orbites sous cette action, qui sont des sous-ensembles de $G.P$, ont soit un élément soit un cardinal divisible par p. Or, on vient de voir que p ne divise pas le cardinal de $G.P$, il suit qu'il existe au moins une orbite à un élément, disons celle de P'. On a donc $hP'h^{-1} = P'$ pour tout $h \in H$ avec P' conjugué à P. Considérons l'ensemble $HP' := \{h.x \mid h \in H,\ x \in P'\}$. C'est un sous-groupe de G car $HP' = P'H$. De plus, P' est un sous-groupe de HP' et il est normal dans HP' (car $hP'h^{-1} = P'$ pour tout $h \in H$ donc pour tout $h \in HP'$). On peut donc former le groupe quotient HP'/P' et on a une surjection canonique $HP' \to HP'/P'$. La restriction de cette application à H est surjective et donc $o(HP'/P') = p^r$ pour un certain r. On a $o(HP') = p^r o(P')$ donc $o(HP') = p^{r+\alpha}$. Or, HP' est un sous-groupe de G qui est d'ordre $p^\alpha m$ donc $r = 0$ et il suit $H \subset P'$. H est donc bien contenu dans un groupe de la forme gPg^{-1} pour un $g \in G$.

Ceci prouve la deuxième et la troisième assertion du théorème.

4. Le nombre de p-sous-groupes de Sylow est congrue à 1 modulo p et divise m.

On garde les mêmes notations que dans les parties précédentes. On sait que l'ensemble des p-sous-groupes de Sylow est égal à l'orbite de P sous l'action de G par conjugaison (P étant un p-sous-groupe de Sylow fixé). Donc le cardinal de $\mathcal{S}$ est égale $[G : G_P]$. Comme $o(P)$ divise $o(G_P)$, ce cardinal divise $[G : P]$ donc m.

Maintenant, remarquons que P agit sur $\mathcal{S}$ par conjugaison. Montrons que la seule orbite de $\mathcal{S}$ à un élément sous cette action est $\{P\}$. Supposons que $hP'h^{-1} = P'$ pour tout $h \in P$ et pour un p-sous-groupe de Sylow P'. Alors PP' est un sous-groupe de G. Exactement comme dans la partie précédente, on montre alors que $P = PP'$ donc $P' \subset P$ c'est à dire $P = P'$ car les deux groupes ont même ordre. L'équation des classes nous donne alors :

$$|\mathcal{S}| = 1 + \sum_{P' \in S, P' \neq P} [P : P_{P'}],$$

où S est tel que $\mathcal{S} = \coprod_{P' \in S} P.P'$. Pour $P' \in S$ et $P \neq P'$, $[P : P_{P'}]$ est divisible par p d'où le résultat. Ceci prouve la première assertion et la quatrième assertion.

□

2.3 Applications et exemples

On verra beaucoup d'applications de ces théorèmes en TD. Signalons toutefois les résultats suivants.

Théorème 2.3.1 (Théorème de Cauchy) *Soit G un groupe fini et p un nombre premier divisant l'ordre de G. Alors G contient un élément d'ordre p.*

Preuve. D'après les théorèmes de Sylow, G possède un p-sous-groupe de Sylow. Un élément non nul x dans ce sous-groupe est d'ordre une puissance de p, disons p^r. Alors $x^{p^{r-1}}$ est d'ordre p car $x^{p^r} = e_G$ et si $x^{p^{r-1}q} = e_G$ alors p^r divise $p^{r-1}q$ donc p divise q.

□

{simple}

Proposition 2.3.2 *Soit H un p-sous-groupe de Sylow de G et n_p le nombre de p-sous-groupes de Sylow de G. Alors H est un sous-groupe normal de G si et seulement si $n_p = 1$.*

Preuve.

1. Supposons que $H \triangleleft G$ et soit H' un p sous-groupe de Sylow de G. D'après le deuxième théorème de Sylow, il existe $g \in G$ tel que $H' = gHg^{-1}$. Comme $H \triangleleft G$, nous avons $gHg^{-1} = H$ pour tout $g \in G$. Donc, on retrouve $H' = H$ et $n_p = 1$.
2. Réciproquement, on suppose que $n_p = 1$. Pour tout $g \in G$, gHg^{-1} est un sous-groupe de G d'ordre égal à $o(H)$, c'est à dire, un p-sous-groupe de Sylow. On a ainsi $gHg^{-1} = H$ car $n_p = 1$. Comme l'égalité précédente est valable pour tout $g \in G$, alors $H \triangleleft G$.

□

Exemple.

1. Soit G un groupe d'ordre $15 = 3.5$. Le nombre de 3-sous-groupes de Sylow n_3 divise 5, et $n_3 \equiv 1(\text{mod } 3)$. La seule valeur possible est 1. Donc, il y a un seul sous-groupe d'ordre 3, et il doit donc être normal. De façon analogue, le nombre de 5-sous-groupes de Sylow n_5 divise 3, et $n_5 \equiv 1(\text{mod } 5)$. Donc, il y a aussi un seul sous-groupe normal d'ordre 5.
2. Soit G un groupe d'ordre $63 = 3^2 \times 7$. D'après les théorèmes de Sylow, le nombre n_7 de 7 Sylow est congru à 1 modulo 7 et divise 9. Il n'y en a donc qu'un. Par la proposition 2.3.2, il est normal et donc G ne peut être simple.
3. Soit $\mathfrak{S}_3$ le groupe des bijections de $\{1, 2, 3\}$ sur $\{1, 2, 3\}$. Il comporte $2.3 = 6$ éléments. Le nombre de 3-sous-groupes de Sylow n_3 divise 2 et $n_3 \equiv 1(\text{mod } 3)$ donc il y en a un seul. Le nombre de 2-sous-groupes de Sylow n_2 divise 3 et $n_2 \equiv 1(\text{mod } 2)$. Il y en a donc 1 ou 3. On peut conclure par exemple en notant que l'on a au moins 2 éléments d'ordre 2 : $\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ et $\sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ et donc on a trois 2-sous-groupes de Sylow.

Chapitre 3

Structure des groupes abéliens de type fini

3.1 Sommes directes et base

La somme directe peut être vue comme une généralisation du produit cartésien. Plus tard nous verrons le lien avec la définition que nous avions adoptée lors des cours d'Algèbre linéaire de Licence. Afin d'éviter les risques de confusion avec la somme directe comme nous l'avons entendu dans les annd́es précédentes, nous allons adopter une notation particulière que nous abandonnerons vite par la suite.

Définition 3.1.1 Soit $(G_i)_{i\in I}$ une famille de groupes abéliens. On note $\bigcirc_{i\in I} G_i$ l'ensemble des suites d'éléments $(g_i)_{i\in I}$ pour tout $i \in I$ $g_i \in G_i$ sauf pour un nombre fini d'éléments. C'est naturellement un groupe pour l'addition termes à termes.

{r1}

Remarque 3.1.2

1. Supposons I fini, alors $\bigcirc_{i\in I} G_i$ est tout simplement le produit cartésien $\prod_{i\in I} G_i$.
2. On peut voir chaque G_i comme sous-groupe naturel de $\prod_{i\in I} G_i$. En effet, G_i s'identifie naturellement au sous-groupe de $\prod_{i\in I} G_i$ donné par les $(x_i)_{i\in I}$ où tous les x_i sont nul sauf pour $i = j$.
3. On peut supposer que dans la définition ci-dessus, tous les G_i soient égaux au même groupe abélien G. Le groupe obtenu se note alors souvent $G^{(I)}$.

La propriété universelle des somme directe est donnée ci après :

Théorème 3.1.3 *Soit $(G_i)_{i\in I}$ une famille de groupes abéliens. Soit G' un autre groupe. On suppose que pour tout $j \in I$, l'on dispose d'un morphisme $\varphi_j : G_j \to G'$. Alors, sous l'identification de la remarque 3.1.2-2, il existe un unique morphisme*

$$\varphi : \bigcirc_{i\in I} G_i \to G'$$

tel que la restriction de φ à chaque G_j est égal à φ_j.

Preuve. Un tel morphisme est nécessairement unique car si $g \in \bigcirc_{i\in I} G_i$ alors $g = (g_i)_{i\in I}$ où pour tout $i \in I$, $g_i \in G_i$ est nul sauf pour un nombre fini. On a alors

$$\varphi(g) = \sum_{i\in I} \varphi_i(g_i)$$

d'où l'unicité.

Concernant l'existence, on pose $\varphi((g_i)_{i\in I}) = \sum_{i\in I} \varphi_i(g_i)$ et on voit facilement que φ est un morphisme de groupes.

□

Définition 3.1.4 Soit G un groupe abélien et soit $(H_i)_{i\in I}$ une famille de sous-groupes de G.

1. On dit que les H_i sont en somme direct si la relation $\sum_{i\in I} h_i = 0$ dans G avec $h_i \in H_i$ pour tout $i \in I$ implique $h_i = 0$ pour tout $i \in I$,
2. On dit que les G est somme directe des H_i si tout $x \in G$ s'écrit de manière unique sous la forme $\sum_{i\in I} h_i = x$ avec $h_i \in H_i$ pour tout $i \in I$ tous nuls sauf pour un nombre fini.

Gardons les même notations et considérons le morphisme de groupes

$$\begin{array}{rccc} \varphi : & \bigcirc_{i\in I} H_i & \to & G \\ & (x_i)_{i\in I} & \mapsto & \sum_{i\in I} x_i \end{array}$$

alors la première assertion est équivalente à celle de dire que φ est injective, la seconde à celle de dire que φ est bijective. Dans ce dernier cas, on peut donc identifier les deux groupes de manière complètement canonique. Donc si G est somme directe des H_i, G s'identifie à $\bigcirc_{i\in I} H_i$

Réciproquement, lorsque $G = \bigcirc_{i\in I} H_i$, les H_i peuvent être vus comme des sous-groupes de G qui sont en somme directe : tout $g \in G$ s'écrivant bien sous la forme $\sum_{i\in I} x_i$ (somme finie) avec $x_i \in H_i$ pour $i \in I$ (où l'on a utilisé l'identification de la remarque 3.1.2.) Bref, il est logique de remplacer la notation $\bigcirc$ par $\bigoplus$ ce que l'on fera par la suite, on notera :

$$G = \bigoplus_{i\in I} G_i$$

au lieu de $G = \bigcirc_{i\in I} G_i$. Attention néanmoins à la subtilité suivante, on peut toujours considérer la somme directe de groupes $\bigoplus_{i\in I} G_i$ mais un ensemble de sous-groupes d'un même groupes ne sont pas nécessairement en somme directe.

Définition 3.1.5 Soit G un groupe abélien, on dit qu'une famille $(e_i)_{i\in I}$ (éventuellement infinie) est une base de G si tout $x \in G$ s'écrit de manière unique sous la forme

$$x = \sum_{i\in I} n e_i$$

où $n \in \mathbb{Z}$ et où ne_i signifie

$$\begin{cases} \underbrace{e_i + e_i + \ldots + e_i}_{n \text{ fois}} & \text{si } n > 0 \\ 0 & \text{si } n = 0 \\ \underbrace{(-e_i) + (-e_i) + \ldots + (-e_i)}_{-n \text{ fois}} & \text{si } n < 0 \end{cases}$$

On dit qu'un groupe est libre s'il possède une base.

En gardant les notations ci-dessus, si $(e_i)_{i\in I}$ est une base de G alors
- chaque e_i est d'ordre infini sinon il existerait n_i tel que $n_i e_i = 0$ et deux écritures possibles pour 0
- G est la somme direct des sous-groupes $\mathbb{Z}e_i$.

Réciproquement, si on a les deux propriétés ci-dessus alors on voit que $(e_i)_{i\in I}$ est une base de G.

Ainsi, un groupe libre de base $(e_i)_{i\in I}$ est isomorphe à $\bigoplus_{i\in I}\mathbb{Z}e_i$. Or, chaque $\mathbb{Z}e_i$ est isomorphe à $\mathbb{Z}$ (en envoyant e_i sur 1, l'hypothèse e_i d'ordre infini est primordiale). Donc on a

$$G \simeq \mathbb{Z}^{(I)}$$

Exemple 3.1.6 Pour tout $n \in \mathbb{N}$, le groupe $\mathbb{Z}^n$ est libre. Par contre, un groupe abélien fini n'est jamais libre : si G est une somme directe de $\mathbb{Z}e_i$, G est nécessairement infini !

3.2 Groupes abéliens libres de type fini

Définition 3.2.1 On dit qu'un groupe abélien est libre de type fini s'il possède une base finie.

Un groupe abélien libre de type fini est d'après la discussion ci-dessus isomorphe à un groupe du type $\mathbb{Z}^n$. Nous allons maintenant regarder si cet entier n est un invariant ce qui nous permettra de définir une notion de rang.

Proposition 3.2.2 *Soit G un groupe abélien libre de type fini. Alors toutes les bases de M ont même cardinal appelé le rang de G.*

Preuve. Supposons que l'on dispose de deux bases de G, l'une de cardinal n_1, l'autre de cardinal n_2 et supposons par exemple $n_1 < n_2$. On a $G \simeq \mathbb{Z}^{n_1}$ (en tant que groupe donc) donc on dispose a d'une famille n_2 éléments de $\mathbb{Z}^{n_1}$ linéairement indépendants sur $\mathbb{Z}$. Or, on a $\mathbb{Z}^{n_1} \subset \mathbb{Q}^{n_1}$. Si $v_1, \ldots, v_{n_2}$ sont linéairement indépendant sur $\mathbb{Z}$ il le sont aussi sur $\mathbb{Q}$. Bref, on a n_2 vecteurs $\mathbb{Q}$ linéairement indépendant dans $\mathbb{Q}^{n_1}$ de dimension $n_1 < n_2$. Ceci est absurde. □

{libre}

Théorème 3.2.3 *Soit G un groupe abélien libre de type fini de rang n. Alors tout sous-groupe H de G est libre de type fini et de rang plus petit que n.*

Preuve. On peut supposer que $G = \mathbb{Z}^n$ et on raisonne par récurrence sur n. Si $n = 0$, il n'y a rien à faire. Si $n = 1$, on sait que les sous-groupes de $\mathbb{Z}$ sont de la forme $d\mathbb{Z}$ et sont donc de rang 1. On suppose donc $n > 1$. Soit $e_1, \ldots, e_n$ une base de G. On pose $G_1 = \mathbb{Z}e_1 \oplus \ldots \oplus \mathbb{Z}e_{n-1}$ et $H_1 = H \cap G_1$. Alors $G = G_1 \oplus \mathbb{Z}e_n$ et $G/G_1 \simeq \mathbb{Z}$ est libre de rang 1.

Si $H_1 = H$ alors $H \subset G_1$ et on peut conclure par rérurrence. Sinon, H/H_1 s'injecte naturellement dans G/G_1 (en envoyant, pour $h \in H$, la classe de h modulo H_1 sur la classe de h modulo G_1 ce qui est bien défini.) qui est de rang 1. Donc H/H_1 est libre de rang 1. Soit $v + H_1$ une base de H/H_1 avec $v \in H$. Nous allons montrer que $H = H_1 \oplus \mathbb{Z}v$.

- Soit $x \in H$. Il existe un unique $n \in \mathbb{Z}$ tel que $\pi(x) = n(v + H_1)$ (où $\pi : H \to H/H_1$ est la surjection canonique) alors $\pi(x - nv) = 0 + H_1$ et donc $x - nv \in H_1$ et donc tout $x \in H$ s'écrit $nv + x_1$ avec $x_1 \in H_1$.
- Cette ecriture est unique car si $x = n'v + x_1' \in H$ est une autre écriture alors en appliquant π, il suit $n = n'$ et $x_1 = x_1'$

On a donc $H = H_1 \oplus \mathbb{Z}v$ et on peut appliquer l'hypothèse de récurrence à H_1. Ce groupe est libre de rang plus petit que $n - 1$ donc H est libre de rang plus petit que n.

□

Soit G un groupe abélien libre de type fini et de rang n et soit P un groupe abélien arbitraire. Soit $\mathcal{B} = (e_1, \ldots, e_n)$ une base de G.

- Si on se donne un morphisme f de G dans P alors f est entièrement déterminée par l'image des éléments e_i car la famille de ces éléments est génératrice de M.
- Si on se donne n éléments p_1, …, p_n de P, il existe un morphisme de A-modules envoyant les e_j sur les p_j. Celui-ci est (bien) défini par

$$f(\sum_{1 \leq j \leq n} a_j e_j) = \sum_{1 \leq j \leq n} a_j p_j$$

  les $(a_j)_{1 \leq j \leq n}$ étant des éléments de $\mathbb{Z}$, car la famille des e_i est libre.

On a donc un unique morphisme qui envoie les e_i sur des éléments p_i donnés dans P. Ceci signifie que l'on a une application bijective :

$$\begin{array}{rccc} \Psi : & \mathrm{Hom}(G, P) & \to & P^n \\ & f & \mapsto & (f(e_1), \ldots, f(e_n)) \end{array}$$

On voit facilement que Ψ a une structure de morphisme de groupes ($\mathrm{Hom}(G, P)$ est un groupe pour l'addition), ce qui montre la proposition suivante :

Proposition 3.2.4 *Soit G un groupe abélien libre de type fini et de rang n et soit P un groupe abélien alors on a un isomorphisme*

$$\mathrm{Hom}(G, P) \simeq P^n$$

Gardons les hypothèses ci-dessus et ajoutons le fait que P est un groupe abélien libre de rang fini r de base $(e_1', \ldots, e_r')$. Considérons l'ensemble des matrices $\mathcal{M}_{r \times n}(\mathbb{Z})$ à r lignes et n colonnes et à coefficients dans $\mathbb{Z}$. Cet ensemble a une structure de groupe abélien pour les lois suivantes :

- Soit $(a_{i,j})_{1 \leq i \leq r, 1 \leq j \leq n} \in \mathcal{M}_{r \times n}(\mathbb{Z})$ et $(b_{i,j})_{1 \leq i \leq r, 1 \leq j \leq n} \in \mathcal{M}_{r \times n}(\mathbb{Z})$ alors :

$$(a_{i,j})_{1 \leq i \leq r, 1 \leq j \leq n} + (b_{i,j})_{1 \leq i \leq r, 1 \leq j \leq n} = (a_{i,j} + b_{i,j})_{1 \leq i \leq r, 1 \leq j \leq n}$$

- Soit $(a_{i,j})_{1 \leq i \leq r, 1 \leq j \leq n} \in \mathcal{M}_{r \times n}(\mathbb{Z})$ et $a \in \mathbb{Z}$ alors :

$$a.(a_{i,j})_{1 \leq i \leq r, 1 \leq j \leq n} = (a.a_{i,j})_{1 \leq i \leq r, 1 \leq j \leq n}$$

Il est aussi facile de voir que $\mathcal{M}_{r \times n}(\mathbb{Z})$ est un groupe abélien libre de rang rn car une base est donnée par les matrices dont les coefficients sont tous nuls sauf pour un de ceux-ci qui prend la veleur 1. Notons $\mathcal{B}_1 = (e_1, \ldots, e_n)$ base de G et $\mathcal{B}_2 = (e_1', \ldots, e_r')$, base de P. On vérifie alors qu'on a un isomorphisme :

$$\begin{array}{rccc} \Phi : & \mathrm{Hom}(G, P) & \to & \mathcal{M}_{p \times n}(\mathbb{Z}) \\ & f & \mapsto & \mathrm{Mat}_{\mathcal{B}_2, \mathcal{B}_1}(f) \end{array}$$

où $\mathrm{Mat}_{\mathcal{B}_2,\mathcal{B}_1}(f) = (a_{i,j})_{1\leq i\leq r, 1\leq j\leq n}$ est défini par :

$$\forall j \in \{1,\dots,n\},\ f(e_j) = \sum_{1\leq i\leq r} a_{i,j} e'_i$$

et étant donnée des choix de bases, on peut donc identifier un morphisme de groupe avec la matrice associée. Il suit donc :

Proposition 3.2.5 *Soit G un groupe abélien de type fini et de rang n et soit P un groupe abélien libre de type fini de rang r alors* $\mathrm{Hom}(G,P)$ *est un groupe abélien libre de rang $r.n$.*

Les identifications faites ci-dessus sont compatibles avec les composition d'applications de sorte que si G_1, G_2 et G_3 sont trois groupes abéliens libres de rang fini respectifs m, n et p et avec bases $\mathcal{B}_1$, $\mathcal{B}_2$ et $\mathcal{B}_3$, et si on a deux morphismes $f : G_1 \to G_2$ et $g : G_2 \to G_3$, on a

$$\mathrm{Mat}_{\mathcal{B}_3,\mathcal{B}_1}(g\circ f) = \mathrm{Mat}_{\mathcal{B}_3,\mathcal{B}_2}(g)\,\mathrm{Mat}_{\mathcal{B}_2,\mathcal{B}_1}(f)$$

Théorème 3.2.6 *Soit G un groupe abélien libre de type fini et soit H un sous-groupe de G. Alors il existe un unique entier s tel que $0 \leq s \leq n$, des entiers strictement positifs uniques $d_1,\dots,d_s$ avec $d_i \mid d_{i+1}$ pour $i = 1,\dots,s-1$ et une base $v_1,\dots,v_n$ de G tel que les $v'_j := d_j v_j$ pour $1 \leq j \leq s$ soient une base de H. En particulier, H est de rang s et les d_i ($1 \leq i \leq s$) sont appelées les facteurs invariants de H.*

Preuve. Remarquons que si il existe une base comme dans l'énoncé alors le rang de G est s et ce nombre est donc unique. La preuve de l'unicité des facteurs invariants sera obtenus à la fin du chapitre.

Prouvons donc la partie existence : on se donne une base de G : e_1, …, e_n. H est un sous groupe de G donc d'après le théorème 3.2.3, H est libre de rang $\leq m$, on se donne pour H un système de générateurs w_1, …, w_m que l'on représente dans une matrice $A = (a_{i,j})_{1\leq i\leq m, 1\leq j\leq n}$ dont les colonnes sont les coordonnées de chaque w_i dans la base de G. Nous allons maintenant effectuer des opérations sur les lignes et colonnes de la matrice A :

- retrancher à une colonne j un multiple d'une colonne $k \neq j$, c'est à dire remplacer le génŕecteur w_j par $w_j - \alpha w_k$ pour un $\alpha \in \mathbb{Z}$.
- retrancher à une ligne j un multiple d'une ligne $k \neq j$, c'est à dire remplacer le vecteur de base e_j par $e_j - \alpha e_k$ pour un $\alpha \in \mathbb{Z}$.
- changer le signe d'une ligne ou d'une colonne ce qui revient à changer le signe d'un w_j ou d'un e_i
- permuter des lignes ou colonnes ce qui revient à permuter des génórateurs ou des éléments de la base.

Tout ceci ne change pas la nature des éléments (ils forment une famille génératrice pour l'un et une base pour l'autre). On doit maintenant seulement montrer qu'en effectuant ces opérations, on peut arriver à une matrice $A' = (a'_{i,j})_{1\leq i\leq m, 1\leq j\leq n}$ de la forme :

$$\begin{pmatrix} d_1 & \cdots & 0 & \cdots & 0 \\ \vdots & \ddots & d_s & \cdots & 0 \\ \vdots & & \vdots & & \vdots \\ 0 & \cdots & 0 & \cdots & 0 \end{pmatrix}$$

avec les d_i comme dans l'énoncé. La base cherchée sera celle dans laquelle la matrice est écrite.

Le procédé est une variante du pivot de Gauss sur $\mathbb{Z}$ et est de nature purement algorithmique. Tout d'abord, si tous les coefficients sont nuls, il n'y a rien à démontrer. Sinon, on considère :

$$a := \inf(|a_{i,j}| \mid a_{i,j} \neq 0)$$

En permutant lignes et colonnes, on peut supposer que $a = a_{1,1}$.

- Pour tout $i = 1, 2, \ldots, n$, on effectue la division euclidienne de $a_{1,j}$ par a :

  $$a_{i,1} = qa + r$$

  avec $q \in \mathbb{Z}$ et $r \in [0, a[$.
- On retranche alors q fois la ligne 1 à la ligne i. En faisant cela, on obtient une matrice dont les éléments de la première colonne sont tous strictement plus petit que a (sauf $a_{1,1}$ éevidemment). On recommence alors le procédé. Par récurrence, on aboutit à une matrice de la forme

  $$\begin{pmatrix} a & a_{1,2} & \cdots & a_{1,m} \\ 0 & a_{2,2} & \cdots & a_{2,m} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & a_{n,1} & \cdots & a_{n,m} \end{pmatrix}$$

- On fait exactement la même chose en considérant la première ligne au lieu de la première colonne : on aboutit a une matrice

  $$\begin{pmatrix} a & 0 & \cdots & 0 \\ 0 & a_{2,2} & \cdots & a_{2,m} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & a_{n,1} & \cdots & a_{n,m} \end{pmatrix}$$

- maintenant soit notre nombre a divise tous les éléments non nuls de la matrice. Cet élément correspond alors au d_1 et on peut continuer le procédé en considérant la sous-matrice suivante. Soit a ne divise pas un $a_{i,j}$, on ajoute alors la ligne i à la ligne 1 et on reprend le processus. On voit que le reste obtenu par le procédé ci-dessus va être plus petit que a. Ce procédé va donc nécessairement s'arrêter

On a donc prouver notre théorème par récurrence.

Remarque 3.2.7 La preuve ci-dessus est de nature algorithmique et permet donc d'obtenir les facteurs invariants et une base comme dans le théorème (qui s'appelle une base adaptée, celle-ci n'est pas unique).

- On suppose que H est engendré par $w_1, \ldots, w_s$ que l'on écrit sous forme de combinaison linéaire d'une base $\mathcal{B}$ de G de rang n. On peut supposer $s \leq n$.
- On écrit la matrice A dont chaque colonne est donnée par un w_j exprimé sur la base $\mathcal{B}$ et les $n - s$ dernières colonnes sont nuls.
- Il existe deux bases $\mathcal{E}$ et $\mathcal{E}'$ de G et H tels que

  $$P_{\mathcal{E}\to\mathcal{B}} A P_{\mathcal{B}\to\mathcal{E}'}$$

  a la forme voulue ci-dessus.

- La matrice $P_{\mathcal{E}\to\mathcal{B}}$ est celle qui nous intéresse (c'est celle qui enregistre les opérations sur les lignes de la matrice A) , si on l'inverse, on obtient $P_{\mathcal{B}\to\mathcal{E}}$qui exprime $\mathcal{E}$ dans la base $\mathcal{B}$.

Exemple 3.2.8 On se donne le sous-groupe N de $\mathbb{Z}^4$ engendré par $(1,2,0,0)$, $(0,2,8,0)$, $(1,2,8,0)$ et on désire trouve une base de $\mathbb{Z}^4$ adaptée à N. La base e_1, e_2, e_3, e_4 de $\mathbb{Z}^4$ est donc la base canonique et les vecteurs w_1, w_2 et w_3 sont $(1,2,0,0)$, $(0,2,8,0)$, $(1,2,8,0)$. On écrit la matrice associée :

$$A = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 2 & 2 & 2 & 0 \\ 0 & 8 & 8 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

La stratégie consiste à faire le moins d'opérations possibles sur les lignes afin que la matrice à inverser soit le plus simple possible. On note x, y, z, t les lignes de la matrices. X est équivalente à

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 2 & 2 & 0 & 0 \\ 0 & 8 & 8 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

et les lignes restent x, y, z, t. L_2 devient $L_2 - 2L_1$. On obtient :

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 8 & 8 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

et les lignes sont x, $y-2x$, z, t. Ensuite L_3 devient $C_2 - C_3$ et on obtient

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 8 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

et les lignes sont x, $y-2x$, z, t. La matrice à inverser pour obtenir la base adaptée est :

$$P = \begin{pmatrix} 1 & 0 & 0 & 0 \\ -2 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

son inverse est

$$P = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 2 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

une base adaptée est donnée par $(1,2,0,0)$, $(0,1,0,0)$, $(0,0,1,0)$ et $(0,0,0,1)$. On vérifie que $(1,2,0,0)$, $(0,2,0,0)$, $(0,0,8,0)$ est bien une base de N. Les éléments 2 et 8 sont les facteurs invariants.

3.3 Théorèmes de structures

Le but de cette section est de déterminer complètement la structure d'un groupe abélien de type fini arbitraire. Voici le thforème principal :

{ba}

Théorème 3.3.1 *Soit G un groupe abélien de type fini. Alors il existe $r \in \mathbb{N}$, $l \in \mathbb{N}$ et des entiers $m_1, \ldots m_r$ strictement plus grand que 1 tel que m_i divise m_{i+1} pour $i = 1, \ldots, r-1$ et tel que :*

$$G \simeq \mathbb{Z}/m_1\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}/m_r\mathbb{Z} \oplus \mathbb{Z}^l$$

Si de plus, G est fini, on a $l = 0$. Les entiers r, m_1, ..., m_r sont uniquement définis et sont appelés les facteurs invariants de G.

Commençons par établir un lien entre un groupe G engendré par un nombre fini de générateurs $g_1, \ldots, g_n$ et le groupe abélien de type fini $\mathbb{Z}^n$. Ceci se fait grâce à l'application suivante :

$$\begin{array}{rccc} \varphi : & \mathbb{Z}^n & \to & G \\ & (a_1, \ldots, a_n) & \mapsto & \sum_{1 \leq i \leq n} a_i x_i \end{array}$$

On vérifie que c'est un morphisme de groupe surjectif. En quotientant par la noyau, on en déduit le résultat suivant :

Proposition 3.3.2 *Tout groupe abélien de type fini est quotient d'un groupe abélien libre de type fini.*

De même, si l'on se donne un sous-groupe H de G, on a un isomorphisme entre un quotient de $\varphi^{-1}(H)$ et H. Or, $\varphi^{-1}(H)$ est un sous-groupe de $\mathbb{Z}^n$, il est donc libre et de type fini, un quotient d'un groupe de type fini étant de type fini, on en déduit que H est aussi de type fini.

Proposition 3.3.3 *Tout sous-groupe d'un groupe abélien de type fini est de type fini.*

{pra}

Lemme 3.3.4 *Soit $(G_i)_{i \in I}$ une famille de groupe abélien et pour tout $i \in I$, soit H_i un sous-groupe de G_i. On pose $G := \oplus_{1 \leq i \leq n} G_i$ et $H := \oplus_{1 \leq i \leq n} H_i$. Alors on a $G/H \simeq \oplus_{1 \leq i \leq n} G_i/H_i$.*

Preuve. Remarquons que pour tout $i \in I$, on a $H \cap G_i = H_i$. Donc l'image de G_i dans G/H s'identifie à G_i/H_i. Ces images engendrent le quotient G/H puisque les G_i engendrent G. Ils sont enfin en somme directe car si pour une famille $(x_i)_{iin I} \in \oplus_{i \in I} G_i$, on a

$$\sum_{i \in I} \pi(x_i) = 0$$

alors on a $\pi(\sum_{i \in I} x_i) = 0$ donc $\sum_{i \in I} x_i \in H$ donc $x_i \in H_i$ pour tout $i \in I$ et donc $\pi(x_i) = 0$ pour tout $i \in I$.

□

La proposition suivante est la partie "existence" du théorème principal.

{fi}

Proposition 3.3.5 *Soit G un groupe abélien de type fini. Alors il existe $r \in \mathbb{N}$, $l \in \mathbb{N}$ et des entiers $m_1, \ldots m_r$ strictement plus grand que 1 tel que m_i divise m_{i+1} pour $i = 1, \ldots, r-1$ et tel que :*

$$G \simeq \mathbb{Z}/m_1\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}/m_r\mathbb{Z} \oplus \mathbb{Z}^l$$

Si de plus, G est fini, on a $l = 0$.

Preuve. Soit $(x_i)_{i=1,\ldots,n}$ des générateurs de G, On considère la surjection

$$\begin{array}{rccc} \varphi : & \mathbb{Z}^n & \to & G \\ & (a_1, \ldots, a_n) & \mapsto & \sum_{1 \leq i \leq n} a_i x_i \end{array}$$

Le noyau $H := \mathrm{Ker}(\varphi)$ est un sous-groupe de $\mathbb{Z}^n$, on peut donc appliquer le théorème 3.3.1. il existe un unique entier s tel que $0 \leq s \leq n$, des entiers strictement positifs uniques $d_1, \ldots, d_s$ avec $d_i \mid d_{i+1}$ pour $i = 1, \ldots, s-1$ et une base $v_1, \ldots, v_n$ de G tel que les $v'_j := d_j v_j$ pour $1 \leq j \leq s$ soient une base de H. On a :

$$\mathbb{Z}^n = \mathbb{Z}v_1 \oplus \ldots \oplus \mathbb{Z}v_n$$

et

$$H = \mathbb{Z}m_1 v_1 \oplus \ldots \oplus \mathbb{Z}m_s v_s$$

en quotienttant et en utilisant le lemme, il vient :

$$G \simeq \mathbb{Z}^n/H \simeq \mathbb{Z}/m_1\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}/m_r\mathbb{Z} \oplus \mathbb{Z}^l$$

ici, on a supprimé les facteurs $\mathbb{Z}/m_i\mathbb{Z}$ avec $m_i = 1$.

□

Rappelons que si est G un groupe, on dit qu'un élément $g \in G$ est de torsion si il est d'ordre fini. La torsion d'un groupe notée G_{tor} est l'ensemble de ses éléments de torsion et on dit qu'un groupe G est sans torsion si $G_{\mathrm{tor}} = 0$ et de torsion si $G_{\mathrm{tor}} = G$. Le théorème ci-dessus permet donc de calculer explicitement la torsion d'un groupe, en gardant ces notations, on voit en effet que

$$G_{\mathrm{tor}} = \mathbb{Z}/m_1\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}/m_r\mathbb{Z}.$$

Ce corollaire est donc complètement directe :

Corollaire 3.3.6 *Un groupe abélien de type fini est libre si et seulement si il est sans torsion.*

Nous nous intéressons maintenant à l'unicité de la décomposition de la proposition 3.3.5. Celle-ci impliquera l'unicité du théorème 3.3.1. Gardons les notations de celui-ci. Tout d'abord, on peut noté que l'entier l est bien un invariant : il est égal au rang de G/G_{tor} ce qui implique donc son unicité. Pour simplifier, on peut donc supposer que G est un groupe abélien fini. Soit p un nombre premier, on peut considérer le sous-groupe pG de G et son quotient G/pG. On considère l'application suivante :

$$\begin{array}{rccc} \Psi : & \mathbb{Z}/p\mathbb{Z} \times G/pG & \to & G/pG \\ & (n, x) & \mapsto & nx \end{array}$$

et on vérifie que celle-ci est bien défini et est un morphisme de groupe. On voit que cette application munit G/pG d'une structure de $\mathbb{F}_p$-espace vectoriel où $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$.

{nul}

Lemme 3.3.7 *Soit G un groupe abélien fini et soit p un nombre premier. Les conditions suivantes sont équivalentes :*

1. *$G/pG \neq 0$*
2. *p divise l'ordre de G*

Preuve. Supposons $G/pG \neq 0$ et considérons le morphisme de multiplication par p

$$\begin{array}{rccc} \chi : & G & \to & G \\ & x & \mapsto & px \end{array}$$

si $G/pG \neq 0$ alors χ n'est pas surjective donc non injective donc son noyau est différent de $\{0\}$ et donc il existe un élément x non nul tel que $px = 0$. Donc p divise nécessairement l'ordre $o(x)$ donc $o(G)$. Réciproquement, si p divise l'ordre de G alors G contient des éléments d'ordre p donc χ n'est pas injective donc non surjective et donc $G/pG \neq 0$.

□

{dim}

Lemme 3.3.8 *Soit G un groupe abélien fini tel que*

$$G \simeq \mathbb{Z}/m_1\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}/m_r\mathbb{Z}$$

Soit p un nombre premier alors la dimension du $\mathbb{F}_p$-espace vectoriel G/pG est égal au nombre d'indices j tel que p divise m_j.

Preuve. Posons pour $j =, \ldots, r$:

$$H_j := \mathbb{Z}/m_j\mathbb{Z}.$$

On a

$$pG \simeq pH_1 \oplus \ldots \oplus pH_r$$

et en utilisant le lemme 3.3.4, il suit

$$G/pG \simeq H_1/pH_1 \oplus \ldots \oplus H_r/pH_r$$

Maintenant, d'après le lemme 3.3.7, chaque composante H_j/pH_j ci-dessus est non nul si et seulement si p divise l'ordre de H_j qui est m_j. Mais chaque H_j est aussi cyclique donc engendré par un unique élément x. Cet élément est générateur de H_j/pH_j vu comme $\mathbb{F}_p$ espace vectoriel. Donc H_j/pH_j est de dimension 0 ou 1 et il est de dimension 1 si et seulement si p divise l'ordre de H_j. Ceci prouve le résultat.

□

Voici maintenant la partie unicité du théorème principal :

Proposition 3.3.9 *Les nombres r et les entiers $m_1, \ldots, m_r$ de la proposition 3.3.5, sont uniquement définis.*

Preuve. D' après le lemme 3.3.8, , pour tout nombre premier p, on a

$$\dim_{\mathbb{F}_p}(G/pG) \leq r$$

avec égalité si et seulement si p divise m_1 (car m_i divise m_{i+1} pour tout i). Donc r est égal à

$$\sup\{\dim_{\mathbb{F}_p}(G/pG) \mid p \text{ premier}\}$$

d'où l'unicité de r. Pour l'unicité des m_j, on raisonne par récurrence sur $o(G)$. Si $o(G) = 1$, il n'y a rien à faire. Sinon, on se donne un nombre premier p qui divise m_1, on considère le groupe pG. Il est cylique et on a :

$$pG \simeq \mathbb{Z}/m'_1\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}/m'_r\mathbb{Z}$$

avec $m'_j = m_j/p$ pour tout $j = 1, \ldots, r$. Notons que certains m'_j peuvent être égaux à 1. Dans le cas contraire, on a l'unicité des m'_j par hypothèse de récurrence et donc des m_j. Sinon, il y a $r - r'$ facteurs m_j égaux à p où r' est le nombre de termes dans la décomposition canonique de pG, les autres m_j sont égaux aux pm'_j ce qui permet de conclure.

□

Remarque 3.3.10 Finalement, on peut montrer l'unicité des facteurs invariants du théorème 3.3.1. Soit t le plus grand entier j tel que $d_j = 1$. On a :

$$G/H \simeq \bigoplus_{t+1 \leq j \leq s} \mathbb{Z}/d_j\mathbb{Z} \oplus \mathbb{Z}^l$$

avec $l = n - s$ donc $(G/H)_{\text{tor}} \simeq \bigoplus_{t+1 \leq j \leq s} \mathbb{Z}/d_j\mathbb{Z}$ et donc les $d_j > 1$ sont uniques d'après le théorème, de même s est le rang de H qui est unique.

Chapitre 4

Classification des groupes de petites cardinaux

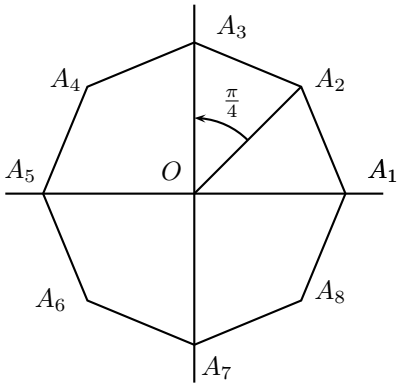
Le but de ce dernier chapitre est de donner une classification de tous les groupes d'ordre plus petit que 11. On pourra trouver dans la littérature des classifications plus ambitieuses mais nécéssitant l'introduction du produit semi-direct ce que nous évitons ici.

4.1 Groupe diédral

On se place ici dans le plan affine euclidien rapporté à un sepère orthonormé. On se donne un polygône $\mathcal{P}_n$ à n côtés centré en O, à n sommets $A_1, \ldots, A_n$ et tel que l'un des sommets A_1 est sur l'axe (Ox). On considère le groupe D_n des isométrie du plan qui conserve $\mathcal{P}_n$. C'est bien sûr un groupe pour la loi de composition.

Définition 4.1.1 Pour $n \geq 2$, le groupe D_n s'appelle le groupe diédral de degreé n.

Nous allons étudier la structure de ce groupe.



Proposition 4.1.2 *Le groupe diédral D_n est engendré par la rotation $r_{(O,\frac{2\pi}{n})}$ de centre O et d'angle $\dfrac{2\pi}{n}$ et par la symétrie $s_{(OA_1)}$ d'axe (OA_1) où A_1 est un sommet du polygône. En particulier, $\mathcal{D}_n$ est d'ordre $2n$.*

Preuve. Soit $g \in \mathcal{D}_n$. On note $\{A_1, A_2, ..., A_n\}$ les sommets du polygône numérotés de telle façon que $r_{(O,\frac{2\pi}{n})}(A_i) = A_{i+1}$ pour $i \in \{1, ..., k-1\}$ et $r_{(O,\frac{2\pi}{n})}(A_n) = A_1$. On considère deux cas :

- Supposons $g(A_1) = A_1$. Alors, comme g est linéaire et que $g(O) = O$, tous les points de la droite (OA_1) sont invariants par g. Donc g est soit l'identité soit la symétrie $s_{(OA_1)}$ d'axe (OA_1).
- Supposons que $g(A_1) = A_k$ pour $k \neq 1$. On a $r^{k-1}_{(O,\frac{2\pi}{n})}(A_1) = A_k$ d'où $r^{1-k}_{(O,\frac{2\pi}{n})} \circ g(A_1) = A_1$ et il suit que d'après le premier cas $r^{1-k}_{(O,\frac{2\pi}{n})} \circ g$ est soit l'identité soit la symétrie d'axe (OA_1). Ainsi, g s'écrit comme produit de $s_{(OA_1)}$ et $r_{(O,\frac{2\pi}{n})}$.

On en déduit ainsi que les éléments de $\mathcal{D}_n$ sont :

$$\mathrm{Id}, s_{(OA_1)}, r_{(O,\frac{2\pi}{n})}, r_{(O,\frac{2\pi}{n})} \circ s_{(OA_1)} \ \ldots\ r^{n-1}_{(O,\frac{2\pi}{n})}, r^{n-1}_{(O,\frac{2\pi}{n})} \circ s_{(OA_1)}$$

Donc l'ordre de $\mathcal{D}_n$ est $2n$

□

On retrient ici le fait que le groupe diédral est engendré par un élément d'ordre n et un élément d'ordre 2, le produit de ces deux éléments est, de plus, d'ordre 2. Nous allons voir que ceci permet de caractériser ce groupe :

{isodie}

Proposition 4.1.3 *Soit G un groupe engendré par deux éléments a et b tel que $o(a) = n$, $o(b) = 2$ et $o(ab) = 2$ alors G est isomorphe à D_n.*

Preuve. On voit que G contient un sous-groupe cyclique d'ordre n, on a donc n éléments distinct e_G, a,...,a^{n-1}. Par ailleurs, on sait que $o(ab) = 2$ et donc $bab = a^{-1}$. On en déduit alors que les éléments $e_G, a, \ldots, a^{n-1}, b, ab, \ldots, a^{n-1}b$ sont tous distincts (l'égalité $a^k = a^j b$ implique que b est une puissance de a donc n est paire et $b = a^{n/2}$. Alors $bab = a^{-1}$ implique que $n + 2$ est un multiple de n donc $n = 2$. Il suit $b = a$ ce qui est impossible car $o(ab) = 2$).

Comme G est engendré par a et b, tout élément de G est un produit de a et de b. Or, on a $ba^k = a^{n-k}b$ et on conclut que tout élément de G est sous la forme $a^i b^j$. On en déduit que

$$G = \{e_G, a, \ldots, a^{n-1}, b, ab, \ldots, a^{n-1}b\}$$

est d'ordre $2n$. L'isomorphisme entre G et D_n s'explicite alors trivialement.

□

4.2 Rappel et techniques de classification

Pour faire cette classification, nous pouvons déjà noter :

- Les groupes d'ordre p avec p premier sont nécessairement isomorphes à $\mathbb{Z}/p\mathbb{Z}$. En effet, un tel groupe admet des éléments dont l'ordre est divisible par p donc qui sont d'ordre 1 ou p. Le groupe est engendré par un élément arbitraire différent du neutre.

- Les groupes d'ordre p^2 sont nécessairement abélien d'après le corollaire 1.5.2. D'après la classification de la proposition 3.3.5, on obtient donc un groupe soit isomorphe à $\mathbb{Z}/p^2\mathbb{Z}$ soit à $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ (ces deux groupes étant non isomorphe car l'un a un élément d'ordre p^2, pas l'autre).

Nous allons maintenant donner deux résultats utiles pour la classification : le premier concerne les groupes d'ordre $2p$ avec p premier, le second les groupes d'ordre 8.

Proposition 4.2.1 *Soit p un nombre premier différent de 2. Soit G un groupe d'ordre $2p$ alors G est soit isomorphe à $\mathbb{Z}/2p\mathbb{Z}$ soit au groupe diédral D_p*

Preuve. On utilise les théorèmes de Sylow : on voit que l'on a 1 ou p 2-Sylow et exactement un p-Sylow S (celui-ci étant isomorphe à $\mathbb{Z}/p\mathbb{Z}$)

- Supposons que l'on ait exactement un 2-Sylow H. Il est donc d'ordre 2. L'intersection de H et de S est triviale sinon on aurait un élément d'ordre 2 dans S. Ceci est absurde par le théorème de Lagrange : 2 ne divise pas p. H est distingué dans G d'après les théorèmes de Sylow et S aussi. Enfin, par cardinalaté HS est égal à G. Il suit que G est isomorphe au produit de H et S (voir la remarque 1.1.4) donc à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \simeq \mathbb{Z}/2p\mathbb{Z}$.
- Supposons que l'on ait exactement p 2-Sylow. Soit a un générateur de S d'ordre p donc. On prend le générateur d'un des 2-Sylow b. On a donc $a^p = e$ et $b^2 = e$. L'élément ab n'est pas dans S sinon b le serait. Il est donc d'ordre 1 ou 2 et comme $p \neq 2$, il est d'ordre 2. On a donc $(ab)^2 = e$. Le sous-groupe de G engendrée par a et b est isomorphe à D_p d'après la proposition 4.1.3, comme il est d'ordre $2p$, il est isomorphe à G.

□

{indice2}

Lemme 4.2.2 *Soit G un groupe fini et N un sous-groupe de G d'indice 2. Alors N est normal dans G.*

Preuve Soit $x \in G$ et soit $y \in N$, on veut montrer $x^{-1}yx \in N$. Si $x \in N$, alors on a $xNx^{-1} = N$. Supposons $x \notin N$. Alors la classe de x modulo N est différente de l'élément neutre, on a donc une partition $G = N \sqcup xN$. L'élément yx n'est pas dans N, il est donc dans xN d'où le résultat.

□

Proposition 4.2.3 *Soit G un groupe d'ordre 8 non abélien alors G est isomorphe au groupe diédral D_4 ou à un autre groupe appelé groupe des quaternions H_8.*

Preuve. Comme G est non abélien, les ordres possibles des éléments de G sont 1, 2 ou 4. Supposons que pour tout x dans G, on ait $x^2 = e$. Alors pour tout $(x, y) \in G^2$, on a $xyxy = e$ et donc $xy = yx$ ce qui implique que G est abélien ce qui est exclus. Donc il existe un élément a d'ordre 4 dans G. Soit N le sous-groupe de G engendrée par a. Il est d'ordre 4 et d'indice 2 dans G donc normal d'après le lemme 4.2.2. Ses éléments sont e, a et a^3 qui sont d'ordre 4 et a^2 qui est d'ordre 2.

Soit b un élément de G qui n'est pas dans N. Si l'on considère la surjection canonique $\pi : G \to G/N$, on a $\pi(b^2) = e_{G/N}$ car G/N est d'ordre 2 donc $b^2 \in N$. Comme b^2 ne peut être d'ordre 4 (sinon b serait d'ordre 8 et G abélien), on a

nécessairement $b^2 = e$ ou $b^2 = a^2$ (le seul élément qui n'est pas d'ordre 4 dans N). On distingue maintenant deux cas :

- Si $b^2 = e$, on note H le sous-groupe engendrée par b. On a comme d'habitude $H \cap N = \{e\}$. Comme N est distingué, on a $bab^{-1} \in N$ et donc, comme a est d'ordre 4, bab^{-1} est aussi d'ordre 4, égal à a ou a^{-1}. Si $bab = a$ alors les éléments de H commutent avec ceux de N. Par cardinalité $HN = G$ est donc le produit direct de ces deux groupes. Comme H et N sont abélien, G l'est aussi ce qui est absurde. On conclut donc $bab^{-1} = a^{-1}$. Le groupe engendrée par a et b est alors isomorphe à D_4 et par cardinalité $G = D_4$.
- Supposons que G n'est pas isomorphe à D_4. Alors on a $b^2 = a^2$. On pose $c = ab$ et $d = ba$. On voit que les éléments b, b^3, c et d ne sont pas dans N car $b \notin N$. Ils sont aussi distincts deux à deux (c et d sont différent sinon G serait abélien.)
  En raisonnant comme ci-dessus, on voit que $c^2 = d^2 = a^2$. On a donc

$$G = \{e, a, a^2, a^3, b, b^3, c, d\}$$

  et on peut alors facilement construire la table de Cayley de G :

$\times$	e	a	a^2	a^3	b	b^3	c	d
e	e	a	a^2	a^3	b	b^3	c	d
a	a	a^2	a^3	e	c	d	b^3	b
a^2	a^2	a^3	e	a	b^3	b	d	c
a^3	a^3	e	a	a^2	d	c	b	b^3
b	b	d	b^3	c	a^2	e	a	a^3
b^3	b^3	c	b	d	e	a^2	a^3	a
c	c	b	d	b^3	a^3	a	a^2	e
d	d	b^3	c	b	a	a^3	e	a^2

  On voit que l'on obtient bien un groupe non isomorphe à D_4 (il y a ici un seul élément d'ordre 2 contre 2 pour le groupe diédral.) Il est appelé groupe des quaternions.

4.3 Classification des groupes d'ordres 1 à 11.

En utilisant les remarques et résultats de la section précédente, A isomorphisme près, on obtient donc la classification suivante :

- $n = 1$, il n'y a qu'un seul groupe d'ordre 1 : le groupe trivial.
- $n = 2$, il n'y a qu'un seul groupe d'ordre 2 (2 est premier) isomorphe $\mathbb{Z}/2\mathbb{Z}$.
- $n = 3$, il n'y a qu'un seul groupe d'ordre 3 (3 est premier) isomorphe $\mathbb{Z}/3\mathbb{Z}$.
- $n = 4$, un groupe d'ordre 4 est donc abélien (d'ordre 2^2 avec 2 premier), un tel groupe est donc isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ (groupe de Klein) ou à $\mathbb{Z}/4\mathbb{Z}$,
- $n = 5$, il n'y a qu'un seul groupe d'ordre 5 (5 est premier) isomorphe $\mathbb{Z}/5\mathbb{Z}$.
- $n = 6$, il y a deux groupe d'ordre 6 (on a $6 = 2 \times 3$ avec 3 premier), l'un isomorphe à $\mathbb{Z}/6\mathbb{Z}$ l'autre au groupe diédral D_3.

- $n = 7$, il n'y a qu'un seul groupe d'ordre 7 (7 est premier) isomorphe $\mathbb{Z}/7\mathbb{Z}$.
- $n = 8$, il y a 3 groupes abéliens possibles : $\mathbb{Z}/8\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ et deux groupes non abéliens D_4 et H_8.
- $n = 9$ un groupe d'ordre 9 est abélien (d'ordre 3^2 avec 3 premier), un tel groupe est donc isomorphe à $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ ou à $\mathbb{Z}/9\mathbb{Z}$,
- $n = 10$, il y a deux groupes d'ordre 10 (on a $10 = 2 \times 5$ avec 5 premier), l'un isomorphe à $\mathbb{Z}/10\mathbb{Z}$ l'autre au groupe diédral D_5.
- $n = 11$, il n'y a qu'un seul groupe d'ordre 11 (11 est premier) isomorphe $\mathbb{Z}/11\mathbb{Z}$.