Université Paul Sabatier
Année 2017–2018

Licence de mathématiques
Structure algébrique I

Structures algébriques I : Théorie des groupes

Table des matières

Chapitre 1

Notions fondamentales

1.1 Premiers exemples

Avant de donner la définition formelle d'un groupe on regarde deux exemples importants.

Exemple 1.1 (Isométries préservant un triangle équilatéral) *On commence par un exemple d'origine géométrique. Rappelons qu'une isométrie du plan est une transformation du plan préservant les distances, c'est-à-dire une application $f : \mathbb{R}^2 \to \mathbb{R}^2$ tel que pour tout couple de point $p, q \in \mathbb{R}^2$:*

$$d\big(f(p), f(q)\big) = d(p, q).$$

Il y a 4 types de telles isométries (la classification se fait par exemple en termes d'ensemble des points fixes) :

- *Rotations de centre p et d'angle θ ;*
- *Symétries d'axe D ;*
- *Translations de vecteur $\overrightarrow{v}$;*
- *Symétries glissées.*

A noter le statut un peu particulier de l'isométrie identité, qu'on peut voir comme une translation de vecteur nul, ou encore comme une rotation de centre arbitraire et d'angle nul.

Maintenant fixons $T \subset \mathbb{R}^2$ un triangle équilatéral (de sommets A, B, C, énuméré dans le sens trigonométrique), et considérons l'ensemble $\mathrm{Isom}(T)$ *des isométries du plan qui préserve ce triangle équilatéral (cela veut dire $f(T) = T$).*

Le centre de symétrie O de T est préservé par une telle isométrie, ainsi $\mathrm{Isom}(T)$ *ne contient que des rotations (centrées en O) et des symétries (d'axe passant par O). A partir de cette remarque il est facile de dresser la liste des 6 éléments dans* $\mathrm{Isom}(T)$ *(avec les notations naturelles) :*

$$\mathrm{Isom}(T) = \{r_{2\pi/3}, r_{-2\pi/3}, S_A, S_B, S_C, id\}.$$

Les deux remarques importantes sont :

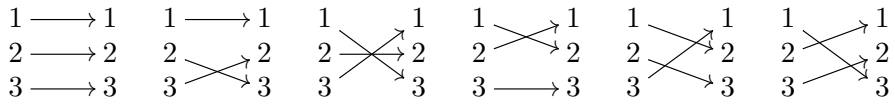
- *Cet ensemble est stable par composition, par exemple :*

$$S_A \circ S_B = r_{2\pi/3} \quad et \quad S_B \circ S_A = r_{-2\pi/3}.$$

— *Chaque transformation de* $\mathrm{Isom}(T)$ *admet une transformation inverse qui est encore dans* $\mathrm{Isom}(T)$.

Exemple 1.2 (Le groupe symétrique) *Le second exemple est de nature plus combinatoire. Si E est un ensemble de n objets, on peut considérer toutes les façons de permuter ces objets, ou plus formellement l'ensemble des bijections de E vers lui-même. Si $E = \{1, \dots, n\}$, on note S_n l'ensemble des bijections associées : le 'S' est pour 'symétrique', on dit que S_n est le "groupe symétrique".*

Par exemple éumérons les éléments de S_3 :



A nouveau, on vérie que S_3 est stable par composition, et que chaque bijection admet un inverse qui est encore dans S_3. En un sens, cet exemple est le même que celui associé au triangle équilatéral : on voit surgir la même "structure algébrique" dans deux contextes distincts. Ce sera un des objectifs de ce cours de pouvoir donner un sens précis à cette remarque (notion "d'isomorphisme"...).

Dernière remarque : le groupe symétrique S_n est un exemple important sur lequel on reviendra. La notation lourde avec des flèches sera alors remplacée par une autre bien plus efficace, donc ne pas trop prendre l'habitude de celle-ci !

1.2 Définition et plus d'exemples

Voici la définition formelle de groupe.

Définition 1.3 *Un groupe est un ensemble G muni d'une application (appelée "loi de groupe")*

$$\begin{aligned} * : G \times G &\to G \\ (g, h) &\mapsto g * h \end{aligned}$$

vérifiant les propriétés suivantes :

— *Associativité : Pour tous g, h, k dans G, $(g * h) * k = g * (h * k)$.*

— *Él ément neutre : Il existe un élément e dans G tel que pour tout g dans G, $e * g = g * e = g$.*

— *Inverse (ou symétrique) : Pour tout g dans G, il existe h dans G, tel que $g * h = h * g = e$.*

Exemple 1.4

i) $\mathbb{Z}$ *avec la loi $+$, neutre $= 0$, symétrique = opposé.*

ii) $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$ *avec la loi $\cdot$, neutre $= 1$, symétrique = inverse.*

iii) Si $P \subset \mathbb{R}^2$ est un polygone régulier à n côtés, l'ensemble $\mathrm{Isom}(P)$ *des isométries du plan préservant P est un groupe, muni de la loi de composition $\circ$, neutre = id, symétrique = transformation réciproque. Ce groupe s'appelle le* ***groupe diédral****, et est aussi noté D_n (certains livres notent D_{2n}). Par exemple :*

— *$D_3 = \mathrm{Isom}(T)$ est le groupe vu en début de cours, il contient 6 éléments ;*

— *D_4 est le groupe des isométries préservant un carré, il contient 8 éléments.*

iv) Si E est un ensemble, l'ensemble $\mathrm{Bij}(E)$ *des bijections de E dans E est un groupe pour la loi $\circ$, comme précédemment. Si $E = \{1, \dots, n\}$, on a déjà mentionné qu'on obtenait un groupe appelé le groupe symétrique, et noté S_n.*

Autre exemple : $\mathrm{Bij}(\mathbb{R})$ *est un énorme groupe !*

v) $\mathbb{R}^n$ muni de l'addition vectorielle est un exemple de groupe, et plus généralement tout espace vectoriel E est un groupe pour l'addition (en fait par définition un espace vectoriel est un groupe avec "quelque chose en plus", à savoir une multiplication par les scalaires).

vi) Autre exemple venant du cours d'algèbre linéaire : l'ensemble $\mathrm{GL}_n(\mathbb{R})$ *des matrices $n \times n$ inversibles (c'est-à-dire de déterminant $\neq 0$), pour la multiplication matricielle.*

Il est aussi utile d'avoir en tête des non-exemples :

i) l'ensemble $\mathbb{N}$ des entiers naturels, muni de l'addition, n'est PAS un groupe (il manque les symétriques) ;

ii) l'ensemble $\mathbb{R}$ des réels muni de la multiplication n'est PAS un groupe (0 n'a pas de symétrique) ;

iii) l'ensemble $\mathbb{Z} \setminus \{0\}$ muni de la multiplication n'est PAS un groupe (1 et -1 sont les seuls éléments admettant un symétrique).

Du coup on s'autorisera souvent à écrire par exemple "le groupe $\mathbb{Z}$", la loi $+$ étant sous-entendue, ce qui n'est guère ambigüe vu qu'il n'y pas pas d'autre choix naturel (on vient de voir que la multiplication est exclue). Idem pour $\mathbb{R}^*$ (forcément multiplicatif), $\mathbb{R}^n$ (forcément additif), etc...

Définition 1.5 *On dit qu'un groupe G est* ***commutatif*** *(ou* ***abélien****) si pour tous g, h dans G, on a $g * h = h * g$.*

Exemple 1.6 *Parmi les exemples vus plus haut :*

- $\mathbb{Z}$, $\mathbb{R}^*$, $\mathbb{C}^*$, $\mathbb{R}^n$ *sont abéliens ;*
- S_n, $\mathrm{GL}_n(\mathbb{R})$ *ne sont pas abéliens (le vérifier par des exemples, et préciser à partir de quel n...)*

1.3 Sous-groupes

Définition 1.7 *Soit G un groupe. Un sous-ensemble $H \subset G$ est appelé un sous-groupe si la loi sur G induit une structure de groupe sur H, c'est-à-dire :*

- *Pour tout h_1, h_2 dans H, $h_1 * h_2 \in H$ (on dit que la loi est "interne") ;*
- *L'élément neutre e est dans H ;*
- *Pour tout h dans H, le symétrique h^{-1} est dans H (on dit que H est "stable par passage au symétrique").*

Exemple 1.8

i) L'ensemble $n\mathbb{Z}$ des multiples de n (pour $n \geq 0$ fixé), est un sous-groupe de $\mathbb{Z}, +$.

ii) L'ensemble $\mathbb{R}_{>0}$ des réels positifs est un sous-groupe de $\mathbb{R}^*, \cdot$.

iii) Le cercle unité $U = \{z ;\ |z| = 1\}$ est un sous-groupe de $\mathbb{C}^*$, ainsi que le groupe $U_n = \{z ;\ z^n = 1\}$ des racines de l'unité. On peut noter au passage (on y reviendra...) qu'il y a des éléments de U qui ne sont PAS des racines de l'unité (pour n'importe quel n).

iv) $\mathrm{Isom}^+(P) \subset \mathrm{Isom}(P)$ *le sous-groupe des isométries préservant le polygone* P *et préservant l'orientation du plan (autrement dit, on ne garde que les rotations, et on oublie les symétries).*

v) $\mathrm{Diff}(\mathbb{R}) \subset \mathrm{Bij}(\mathbb{R})$ *le sous-groupe des bijections de* $\mathbb{R}$ *de classe* $\mathcal{C}^\infty$.

vi) $\mathrm{SL}_n(\mathbb{R}) \subset \mathrm{GL}_n(\mathbb{R})$ *le sous-groupe des matrices de déterminant 1.*

Voici un autre exemple important de groupe, que l'on formalisera précisément un peu plus loin dans le cours.

Exemple 1.9 *Soit* $n > 0$ *un entier fixé. La notation* $\mathbb{Z}/n\mathbb{Z}$ *désignera l'ensemble des entiers* $a \in \mathbb{Z}$ *considérés modulo* n *:* $a \in \mathbb{Z}$ *et* $b \in \mathbb{Z}$ *correspondent au même élément de* $\mathbb{Z}/n\mathbb{Z}$ *si leur différence est un multiple de* n*. On note* $\bar{a}$ *l'élément de* $\mathbb{Z}/n\mathbb{Z}$ *associé à* $a \in \mathbb{Z}$*, ça se lit "a modulo n". Par exemple, dans* $\mathbb{Z}/3\mathbb{Z}$ *:*

$$\bar{1} = \overline{10} = \overline{-5}, \text{ mais } \bar{1} \neq \bar{2}.$$

On définit une addition sur $\mathbb{Z}/n\mathbb{Z}$ *de la façon suivante :*

$$\bar{a} + \bar{b} := \overline{a+b}.$$

On vérifie que la définition est cohérente, au sens où elle ne dépend pas d'un choix de représentants :

$$\bar{a} + \bar{b} = \overline{a+kn} + \overline{b+k'n} := \overline{a+b+(k+k')n} = \overline{a+b}.$$

Noter que sur $\mathbb{Z}/2\mathbb{Z}$*, cela revient à la règle bien connue :*

pair + pair = pair	*pair + impair = impair*
impair + impair = pair	*impair + pair = impair*

Muni de cette loi d'addition, $\mathbb{Z}/n\mathbb{Z}$ *est un groupe.*

Sujet de réflexion : comment définir une multiplication sur $\mathbb{Z}/n\mathbb{Z}$ *? Obtient-on un groupe ?*

La propriété d'associativité peut parfois être pénible à montrer. Dans le cas d'un sous-groupe, elle est héritée automatiquement du groupe ambiant : du coup une bonne recette pour montrer qu'un ensemble est un groupe est de montrer qu'il s'agit d'un sous-groupe d'un groupe déjà connu !

Voici un léger raccourci, d'usage courant, pour montrer qu'un ensemble est un sous-groupe.

Proposition 1.10 *Soit* G *un groupe (noté multiplicativement). Un sous-ensemble* H *de* G *est un sous-groupe si et seulement si les deux conditions suivantes sont satisfaites :*

i) H *n'est pas vide ;*

ii) pour tous h_1, h_2 *dans* H*,* $h_1 h_2^{-1}$ *est dans* H*.*

Démonstration : Un sous-groupe vérifie par définition (i) et (ii), il s'agit de montrer la réciproque.

Supposons donc (i) et (ii). Par (i) il existe $h_0 \in H$. Par (ii) appliqué au couple h_0, h_0, on obtient $e = h_0 h_0^{-1} \in H$. Maintenant si $h \in H$, on applique (ii) au couple e, h pour obtenir $h^{-1} = eh^{-1} \in H$. Enfin, si $h_1, h_2 \in H$, on applique (ii) au couple h_1, h_2^{-1} pour obtenir $h_1 h_2 = h_1 (h_2)^{-1} \in H$. □

1.4 Sous-groupes engendrés par une partie

Proposition 1.11 *i) Soit G un groupe et $H, K \subset G$ des sous-groupes. Alors $H \cap K$ est aussi un sous-groupe de G.*

ii) Plus généralement, si I est un ensemble et $H_i, i \in I$ une famille de sous-groupes de G alors $\bigcap_{i\in I} H_i$ est un sous-groupe de G.

Démonstration : On sait que $e \in H$ et $e \in K$ donc $e \in H \cap K$ qui n'est donc pas vide.

Il reste à vérifier que si $h_1, h_2 \in H \cap K$ alors on a aussi $h_1 h_2^{-1} \in H \cap K$. Comme $h_1, h_2 \in H$ et H est un sous-groupe on a $h_1 h_2^{-1} \in H$, et de même $h_1, h_2 \in K$ implique que $H_1 h_2^{-1} \in K$ et on a donc bien $h_1 h_2^{-1} \in H \cap K$.

La démonstration du point 1.1.11.ii) est exactement semblable. □

On peut utiliser cette proposition pour définir le sous-groupe engendré par une partie via le corollaire suivant.

Corollaire 1.12 *Soient G un groupe et $X \subset G$ une partie quelconque. Il existe un unique sous-groupe H de G tel que $X \subset H$ et H est minimal pour cette propriété, c'est-à-dire que si $G \supset K \supset X$ est un sous-groupe alors $H \subset K$.*

Démonstration : Soit $\mathcal{K}_X$ l'ensemble de tous les sous-groupes de G contenant X. Par la proposition 1.11 le sous-ensemble

$$H = \bigcap_{K\in\mathcal{K}_X} K$$

est un sous-groupe de G. Il contient X puisque $X \subset K$ pour tout $K \in \mathcal{K}_X$, et si $K \supset X$ est un sous-groupe alors $K \in \mathcal{K}_X$ donc $K \supset H$.

Ceci démontre l'existence de H. L'unicité se démontre comme suit : si H_1, H_2 sont tous deux minimaux alors $H_1 \supset H_2$ et $H_2 \supset H_1$ donc $H_1 = H_2$. □

Définition 1.13 *Le sous-groupe minimal de G contenant X est appelé* sous-groupe de G engendré par X. *On le note $\langle X\rangle_G$, ou simplement $\langle X\rangle$.*

On remarque que $\langle\emptyset\rangle = \{e\}$ est le sous-groupe trivial. Une construction plus explicite de $\langle X\rangle$ dans le cas général est donnée par la proposition suivante :

Proposition 1.14 *Soit $X \neq \emptyset$ un sous-ensemble de G. On a*

$$\langle X\rangle = \{g_1^{\varepsilon_1} * \cdots * g_n^{\varepsilon_n} : n \geq 1, g_1, \ldots, g_n \in X, \varepsilon_1, \ldots, \varepsilon_n \in \{1, -1\}\}.$$

Démonstration : Soit H l'ensemble à droite. On vérifie immédiatement que H est un sous-groupe de G. d'autre part il contient X, et si $K \supset X$ est un sous-groupe alors $g_1^{\varepsilon_1} * \cdots * g_n^{\varepsilon_n} \in H$ pour touts n-uplets $g_1, \ldots, g_n \in X$ et $\varepsilon_1, \ldots, \varepsilon_n \in \{1, -1\}$ donc il contient H. □

Définition 1.15 *Soit G un groupe et $X \subset G$. On dit que X* engendre *G, ou que G* est engendré par *X, ou encore que X* est une partie génératrice de *G, si $G = \langle X\rangle_G$. Autrement dit X n'est contenu dans aucun sous-groupe propre de G.*

Exemple 1.16 *i) $\mathbb{Z} = \langle 1\rangle$ ou $\langle -1\rangle$. Le sous-groupe $n\mathbb{Z}$ est engendré par n ou $-n$.*

ii) $\mathbb{R}$ est engendré par $[0, 1]$.

1.5 Groupes cycliques et ordre d'un élément

Définition 1.17 *i) Un groupe G est dit* monogène *s'il est engendré par une partie à un élément, $G = \langle g \rangle$ pour un $g \in G$.*

ii) Soit G un groupe, son ordre *est le cardinal $|G|$ de l'ensemble sous-jacent.*

iii) Soit G un groupe et $g \in G$, l'ordre de g dans G *est le cardinal du sous-groupe $\langle g \rangle_G$.*

iv) Un groupe est dit cyclique *s'il est monogène et fini.*

Exemple 1.18 *i) $\mathbb{Z}$ est monogène puisqu'il est engendré par 1.*

ii) $\mathbb{Z}/n\mathbb{Z}$ est d'ordre n et engendré par $\overline{1}$. Le groupe $\mathbb{Z}/n\mathbb{Z}$ est donc cyclique d'ordre n. C'est aussi le cas du groupe des racines n-ièmes de l'unité (ce dernier est engendré par $e^{2i\pi/n}$).

On peut vérifier que $\overline{3}$ engendre $\mathbb{Z}/4\mathbb{Z}$ (ce qui revient à ce que $\overline{3}$ soit d'ordre 4) mais que ce n'est pas le cas de $\overline{2}$: ce dernier élément est d'ordre 2.

iii) Le groupe D_3 des symétries du triangle est d'ordre 6. Il contient :

- *Des éléments d'ordre 3 : les rotations $r_{2\pi/3}, r_{-2\pi/3}$ (le sous-groupe engendré par l'une d'entre elles est $\{\mathrm{Id}, r_{2\pi/3}, r_{-2\pi/3}\}$) ;*
- *Des éléments d'ordre 2 : les symétries s_A, s_B, s_C (le sous-groupe engendré par s_A est $\{\mathrm{Id}, s_A\}$) ;*
- *l'identité, qui est d'ordre 1.*

Comme ceci est une liste complète des éléments de D_3 on voit qu'il ne contient pas d'élément d'ordre 6, et donc il ne peut pas être cyclique.

1.6 Produit de groupes

Soient G_1, G_2 des groupes. L'ensemble produit

$$G_1 \times G_2 = \{(g_1, g_2) : g_1 \in G_1, g_2 \in G_2\}$$

est alors muni de la loi

$$(g_1, g_2) * (h_1, h_2) = (g_1 h_1, g_2 h_2).$$

On vérifie immédiatement que cette loi satisfait aux axiomes des groupes. Le groupe $(G_1 \times G_2, *)$ est appelé *groupe produit de G_1, G_2*. De même on définit ue loi de groupe sur un produit $\prod_{i \in I} G_i$ facteur par facteur.

On constate immédiatement que si G_1, G_2, G_3 sont trois groupes alors les lois de groupe définies sur $G_1 \times G_2 \times G_3$ par les produits de groupes successifs $G_1 \times (G_2 \times G_3)$ ou $(G_1 \times G_2) \times G_3$, ou sont les mêmes que celle du produit à trois termes.

Exemple 1.19 *i) $\mathbb{Z}^2$ est le groupe $\mathbb{Z} \times \mathbb{Z}$, de même $\mathbb{R}^2$ est $\mathbb{R} \times \mathbb{R}$.*

ii) $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ est cyclique d'ordre 6 : il est engendré par $(\overline{1}, \overline{1})$.

iii) $\mathbb{Z}/2 \times \mathbb{Z}/2$ n'est pas cyclique : il contient exactement trois éléments d'ordre 2 et un d'ordre 1.

1.7 Morphismes

Définition 1.20 *Soient $(G, *)$ et $(H, \star)$ deux groupes. On appelle* morphisme *de groupes de G dans H une application $\varphi : G \to H$ telle que*

$$\forall g, g' \in G : \varphi(g * g') = \varphi(g) \star \varphi(g').$$

*On utilise aussi parfois le terme d'*homomorphisme *pour désigner ces applications.*

(Dans la suite, sauf en présence d'une possible ambiguïté on utilisera la nottaion multiplicative pour toutes les lois de groupe.)

Propriétés

Soit $\varphi : G \to H$ un morphisme de groupe. Les propriétés suivantes sont des conséquences immédiates de la définition.

i) On a $\varphi(e_G) = e_H$;

ii) Si $g \in G$ alors $\varphi(g^{-1}) = \varphi(g)^{-1}$.

iii) Si $g \in G$ et $n \in \mathbb{Z}$ alors $\varphi(g^n) = \varphi(g)^n$.

Pour démontrer 1.1.20.i) on prend $g \in G$ quelconque et on observe que l'on a :

$$\varphi(g) = \varphi(e_G g) = \varphi(e_G)\varphi(g)$$

et il suit de l'égalité du premier et dernier termes que $\varphi(e_G) = \varphi(g)\varphi(g)^{-1} = e_H$.

La démonstration de 1.1.20.ii) est similaire : si $g \in G$ on a :

$$\begin{aligned} \varphi(g)\varphi(g)^{-1} &= \varphi(gg^{-1}) \\ &= \varphi(e_G) = e_H \end{aligned}$$

où la dernière égalité suit de 1.1.20.i). Ceci montre que l'on a bien $\varphi(g^{-1}) = \varphi(g)^{-1}$.

Enfin, la dernière propriété 1.1.20.iii) se démontre pour $n > 0$ par une récurrence immédiate sur n, puis on en déduit $n < 0$ en utilisant le point 1.1.20.ii), et le cas $n = 0$ est 1.1.20.i).

Exemple 1.21

i) Si $n \in \mathbb{Z}$ alore l'application $\mathbb{Z} \to n\mathbb{Z}$ définie par $x \mapsto nx$ est un morphisme de $\mathbb{Z}$ dans le groupe $n\mathbb{Z}$.

ii) L'application dét : $\mathrm{GL}_n(\mathbb{R}) \to \mathbb{R}^\times$ *est un morphisme.*

iii) L'exponentielle $\exp : \mathbb{R} \to \mathbb{R}_{>0}$ *est un morphisme du groupe additif dans le groupe multiplicatif des réels positifs.*

iv) Soit G le groupe des isométries d'un triangle équilatéral de sommets x_1, x_2, x_3. L'application qui à $g \in G$ associe la permutation $\varphi(g) \in S_3$ définie par $g(x_i) = x_{\varphi(g)(i)}$ est un morphisme.

Définition 1.22 *Soient G, H des groupes. Si φ est un morphisme de groupes de G dans H on définit les ensembles suivants :*

— *L'*image *de φ, notée* $\mathrm{im}(\varphi)$*, est :*

$$\mathrm{im}(\varphi) = \{h \in H : \exists g \in G : h = \varphi(g)\} = \{\varphi(g) : g \in G\};$$

— *Le* noyau *de φ, noté* $\ker(\varphi)$*, est :*

$$\ker(\varphi) = \{g \in G : \varphi(g) = e_H\}.$$

On dit que φ est un isomorphisme *si elle est bijective. Si $G = H$ on dit que φ est un* endomorphisme*, et un endomorphisme qui est aussi un isomorphisme est appelé* automorphisme *de G.*

Remarque 1.23 — *Dans les exemples ci-dessus, les morphismes décrits en 1.1.21.i), 1.1.21.iii), 1.1.21.iv) sont des isomorphismes.*

— *Le morphisme* $\det : \mathrm{GL}_n(\mathbb{R}) \to \mathbb{R}^\times$ *n'est pas injectif si $n > 1$.*

Définition 1.24 *Soit G un groupe et $h \in G$. Un* conjugué de h dans G *est un élément de G qui peut sécrire sous la forme ghg^{-1} pour un $g \in G$. On dit aussi que h et ghg^{-1} sont conjugués dans G.*

Un sous-groupe $H \subset G$ est dit distingué dans G *s'il conient tous les conjugués de ses éléments, autrement dit*

$$\forall h \in H : \forall g \in G : ghg^{-1} \in H.$$

On note $H \triangleleft G$ pour signifier que H est distingué dans G.

Proposition 1.25 *Soit $\varphi : G \to H$ un morphisme.*

i) $\mathrm{im}(\varphi)$ *est un sous-groupe de H.*

ii) $\ker(\varphi)$ *est un sous-groupe distingué de G.*

Démonstration : Les deux points sont démontrés indépendamment. Pour 1.1.25.i) il faut vérifier que :

— $\mathrm{im}(\varphi)$ est non-vide : c'est évident puisque G est non-vide et $\varphi(g) \in \mathrm{im}(\varphi)$ pour n'importe quel $g \in G$.

— Si $h \in \mathrm{im}(\varphi)$ alors $h^{-1} \in \mathrm{im}(\varphi)$: il existe $g \in G$ tel que $h = \varphi(g)$ et il suit que $h^{-1} = \varphi(g^{-1})$ (par 1.1.20.ii)) et donc que $h^{-1} \in \mathrm{im}(\varphi)$.

— Si $h_1, h_2 \in \mathrm{im}(\varphi)$ alors $h_1 h_2 \in \mathrm{im}(\varphi)$: il eixte $g_1, g_2 \in G$ tels que $h_i = \varphi(g_i)$ et il vient $h_1 h_2 = \varphi(g_1 g_2)$ donc $h_1 h_2 \in \mathrm{im}(\varphi)$.

Pour démontrer 1.1.25.ii) que $\ker(\varphi)$ est un sous-groupe :

— On a $\varphi(e_G) = e_H$ donc $\ker(\varphi)$ est non-vide.

— Si $g \in \ker(\varphi)$ alors

$$\varphi(g^{-1}) = \varphi(g)^{-1} = e_H^{-1} = e_H$$

donc $g^{-1} \in \ker(\varphi)$.

— Si $g_1, g_2 \in \ker(\varphi)$ alors

$$\varphi(g_1 g_2) = \varphi(g_1)\varphi(g_2) = e_H e_H = e_H$$

donc $g_1 g_2 \in \ker(\varphi)$.

Il reste ensuite à voir que $\ker(\varphi)$ est distingué dans G : si $g_0 \in \ker(\varphi)$ et $g \in G$ on a :

$$\begin{aligned}\varphi(gg_0g^{-1}) &= \varphi(g)\varphi(g_0)\varphi(g^{-1}) \\ &= \varphi(g)e_H\varphi(g)^{-1} = \varphi(g)\varphi(g)^{-1} = e_H\end{aligned}$$

et donc $g_0gg_0^{-1} \in \ker(\varphi)$. □

Exemple 1.26 — *Le noyau du morphisme* dét : $\mathrm{GL}_n(\mathbb{R}) \to \mathbb{R}^\times$ *est le groupe spécial linéaire* $\mathrm{SL}_n(\mathbb{R})$. *En particulier celui-ci est distingué :* $\mathrm{SL}_n(\mathbb{R}) \lhd \mathrm{GL}_n(\mathbb{R})$.

— ...

Proposition 1.27 *Soit φ un morphisme de G dans un groupe H. Il est injectif si et seulement si son noyau est trivial, c'est-à-dire* $\ker(\varphi) = \{e_G\}$.

Démonstration : Supposons d'abord que φ est injectif. On a $\varphi(e_G) = e_H$ par 1.1.20.i). Par l'injectivité, il suit que si $\varphi(g) = e_H$ pour un $g \in G$ alors $g = e_G$. C'est-à-dire que $\ker(\varphi) = \{e_G\}$.

Supposons maintenant que $\ker(\varphi) = \{e_G\}$. Si $g, g' \in G$ verifient $\varphi(g) = \varphi(g')$ il vient :

$$\varphi(g^{-1}g') = \varphi(g)^{-1}\varphi(g') = e_H.$$

On a donc $g^{-1}g' \in \ker(\varphi)$, donc $g^{-1}g' = e_G$ et enfin $g = g'$. Ceci démontre que φ est injectif. □

On rappelle que si X, Y sont des ensembles une application $f : X \to Y$ est bijective si et seulement si elle admet une application inverse, c'est-à-dire qu'il existe $h : Y \to X$ vérifiant $h \circ f = \mathrm{Id}_X$ et $f \circ h = \mathrm{Id}_Y$. On utilisera pour cette application inverse la notation $h = f^{-1}$. Noter que f^{-1} est aussi une application bijective.

Proposition 1.28 *i) Soit $\varphi : G \to H$ un isomorphisme. Alors son application inverse φ^{-1} est un morphisme de groupes, donc un isomorphisme.*

ii) Si $\varphi_1 : G_1 \to G_2$ et $\varphi_2 : G_2 \to G_3$ sont des morphismes de groupes alors $\psi = \varphi_2 \circ \varphi_1 : G_1 \to G_3$ est un morphisme de groupes. Si de plus les φ_i sont des isomorphismes alors ψ aussi, et $\psi^{-1} = \varphi_1^{-1} \circ \varphi_2^{-1}$

Démonstration : Soient $h_1, h_2 \in H$ et soient $g_i = \varphi^{-1}(g_i)$. Comme φ^{-1} est l'inverse de φ on a $\varphi(g_i) = h_i$ et comme on sait que φ est un morphisme il suit que :

$$\varphi(g_1g_2) = \varphi(g_1)\varphi(g_2) = h_1h_2.$$

Il vient encore

$$\varphi^{-1}(h_1h_2) = g_1g_2 = \varphi^{-1}(h_1)\varphi^{-1}(h_2).$$

Ceci montre que φ^{-1} est bien un morphisme de groupes.

La démonstration du second point est laissée à la lectrice. □

Définition 1.29 *On dit que deux groupes G, H sont* isomorphes, *et on note $G \cong H$, s'il existe un isomorphisme $G \to H$.*

Avec la proposition ci-dessus on voit que l'isomorphisme est une relation d'équivalence sur les groupes. De manière informelle, deux groupes sont isomorphes s'ils ont « les mêmes » lois de groupes.

Exemple 1.30 *i) Les groupes* $\mathbb{R}, +$ *et* $\mathbb{R}^\times, \times$ *sont isomorphes via le morphisme* exp *(cf. 1.1.21.iii)).*

ii) L'action par permutation sur les sommets 1.1.21.iv) montre que les groupes G *d'isométries du triangle et* S_3 *sont isomorphes l'un à l'autre.*

iii) Les groupes $\mathbb{Z}/n\mathbb{Z}$*,* U_n *(racines n-ièmes de l'unité),* G_n *(isométries positives d'un n-gone régulier) sont deux à deux isomorphes (ce sont des avatars du "groupe cyclique d'ordre n"). Par exemple on a*

$$U_n = \{e^{\frac{2i\pi k}{n}} : k = 0, \dots, n-1\}$$

et on vérifie que l'application $\bar{k} \mapsto e^{2i\pi k/n}$ *définit un isomorphisme* $\mathbb{Z}/n\mathbb{Z} \to U_n$*.*

iv) Les groupes $\mathbb{Z}/6\mathbb{Z}$ *et* $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ *sont isomorphes via l'application*

$$\overline{x}^6 \mapsto (\overline{x}^2, \overline{x}^3)$$

(où $\overline{x}^n$ *désigne la classe de* x *modulo* n*).*

v) Noter que si deux groupes sont isomorphes ils ont des cardinaux égaux. La réciproque n'est pas vraie, cf. par exemple 1.35 ci-dessous.

Proposition 1.31 *Soit* G *un groupe.*

i) Soit $\varphi : \mathbb{Z} \to G$ *un morphisme. Il existe un unique élément* $g \in G$ *tel que pour tout* $n \in \mathbb{Z}$ *on ait* $\varphi(n) = g^n$*.*

ii) Soit $g \in G$*. Il existe un unique morphisme* $\varphi : \mathbb{Z} \to G$ *tel que* $\varphi(1) = g$*.*

Démonstration : Pour démontrer 1.1.31.i) on pose $g = \varphi(1)$. D'après la propriété 1.1.20.iii) il vient pour tout $n \in ZZ$:

$$\begin{aligned}\varphi(n) &= \varphi(\underbrace{1 + \cdots + 1}_{n\ fois}) \\ &= \varphi(1)^n = g^n\end{aligned}$$

Ceci démontre l'existence de g, l'unicité est tautologique puisque $\forall n \in \mathbb{Z}\varphi(g) = g^n$ implique en particulier que $g = \varphi(1)$.

Pour démontrer 1.1.31.ii) on pose

$$\varphi(n) = g^n$$

et il faut vérifier que φ est un morphisme de groupes. C'est immédiat et laissé au lecteur. □

TODO ? réécrire en termes de conditions équivalentes pour clarifier la logique de la démo ?

Théorème 1.32 *Soient* G *un groupe et* $g \in G$*.*

i) g *est d'ordre infini si et seulement si* $\langle g \rangle$ *est isomorphe à* $\mathbb{Z}$ *si et seulement si* $\forall i, j \in \mathbb{Z}$*,* $i \neq j$ *implique* $g^i \neq g^j$*.*

ii) g est d'ordre fini $n \in \mathbb{N}$ si et seulement si les éléments

$$e_G, g, g^2, \ldots, g^{n-1}$$

sont deux à deux distincts et de plus $g^n = e_G$ si et seulement si $\langle g \rangle \mathbb{Z}/n\mathbb{Z}$. On a alors

$$\langle g \rangle = \{e_G, g, \ldots, g^{n-1}\}$$

et $g^k = e_G$ si et seulement si n divise k.

Démonstration : On montre les deux points en même temps. D'après la description explicite du sous-groupe engendré donnée dans la propositoon 1.14 on a

$$\langle g \rangle = \{g^k : k \in \mathbb{Z}\}.$$

Si $\forall i \neq j$ on a $g^i \neq g^j$ alors cet ensemble est infini et donc g est d'ordre infini. Le morphisme défini en 1.1.31.ii) donne alors un isomorphisme $\mathbb{Z} \to \langle g \rangle$.

Sinon il existe $n \in \mathbb{Z}$, $n > 0$ tel que

$$n = \min(k \in \mathbb{Z} : k > 0, g^k = e_G)$$

(en effet si $g^i = g^j$ pour des $i > j$ on a $i - j > 0$ et $g^{i-j} = e_G$ donc l'ensemble sur lequel on prend le minimum est non vide et ce minimum est donc fini). Les éléments $e_G, g, g^2, \ldots, g^{n-1}$ sont deux à deux distincts : si $0 \leq i < j < n$ et $g^i = g^j$ alors $g^{i-j} = e_G$, ce qui contredit la minimalité de n. De plus, si $k \in \mathbb{Z}$ on peut écrire $k = qn + r$ pour des $q, r \in \mathbb{Z}$, $0 \leq r < n$ et il suit que

$$g^k = g^{qn} g^r = (g^n)^q g^r = e_G^q g^r = g^r \in \{e_G, g, \ldots, g^{n-1}\}$$

et on voit donc que $\langle g \rangle = \{e_G, g, \ldots, g^{n-1}\}$. Cet ensemble est de cardinal n et il suit g est d'ordre n. Le calcul ci-dessus montre aussi que $g^k = g^l$ si et seulement si $n|(k-l)$ et il suit que l'on peut définir une application bijective

$$\mathbb{Z}/n\mathbb{Z} \to \langle g \rangle, \ \bar{k} \mapsto g^k$$

qui est alors bijective, et dont on vérifie immédiatement que c'est un morphisme. Ceci implique les deux énoncés restants. □

Remarque 1.33 *La démonstration serait simplifiée par l'usage de la notion de groupe quotient que l'on verra plus tard.*

Proposition 1.34 *Soit $\varphi : G \to H$ un isomorphisme.*

i) Si G est abélien alors H l'est aussi.

ii) Si $g \in G$ est d'ordre n alors $\varphi(g) \in H$ est aussi d'ordre n.

Démonstration : Pour prouver le point 1.1.34.i) on n'utilisera que le fait que φ est un morphisme surjectif. Soient $h_1, h_2 \in H$. Il existe $g_1, g_2 \in G$ tels que l'on ait $\varphi(g_i) = h_i$. Il vient alors :

$$h_1 h_2 = \varphi(g_1)\varphi(g_2) = \varphi(g_1 g_2)$$

et comme G est abélien on a $g_1 g_2 = g_2 g_1$ et il suit que :

$$\begin{aligned} h_1 h_2 &= \varphi(g_2 g_1) \\ &= \varphi(g_2 g_1) = \varphi(g_2)\varphi(g_1) = h_2 h_1. \end{aligned}$$

On a montré que touts éléments $h_1, h_2 \in H$ commutent l'un à l'autre, ce qui veut dire que H est abélien.

Pour démontrer le point 1.1.34.ii) on n'utilisera que le fait que φ est un morphisme injectif. On a vu dans la théorème précédent que l'ordre n de g est donné par :

$$n = \min(k > 0 : g^k = e_G)$$

et de même l'ordre m de $\varphi(g)$ vaut $\min(k > 0 : \varphi(g)^k = e_H)$. On a

$$\varphi(g)^n = \varphi(g^n) = \varphi(e_G) = e_H$$

et il suit que $m \leq n$ (en fait m divise n). D'autre part, pour tout $0 < k < n$ on a $g^k \neq e_G$. Comme φ est injective il suit que $\varphi(g^k) \neq \varphi(e_G) = e_H$ et il suit que $m \geq n$. On a donc finalement $m = n$, c'est-à-dire que g et $\varphi(g)$ on même ordre. □

Exemple 1.35

Les groupes S_3 et $\mathbb{Z}/6\mathbb{Z}$ ne peuvent pas être isomorphes car $\mathbb{Z}/6\mathbb{Z}$ contient un élément d'ordre 6, ce qui n'est pas le cas de S_3. On peut aussi observer que le premier n'est pas abélien mais le second si.

Les groupes $\mathbb{Z}/4\mathbb{Z}$ et $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ ne sont pas isomorphes car le second ne contient pas d'élément d'ordre 4.

Plus généralement, on déduit facilemet du théorème que si G est cyclique alors un groupe H est isomorphe à G si et seulement s'il est cyclique de même ordre.

Chapitre 2

Quotient et actions de groupes

2.1 Classes à droite et à gauche et théorème de Lagrange

2.1.1 Rappels sur les relations et classes d'équivalence

Dans cette section X est un ensemble.

Définition 2.1 — *Une* relation *sur X est un sous-ensemble $R \subset X \times X$. Etant donnée une raltion R sur X et $x, y \in X$ on dit que x* est en relation avec *y si $(x, y) \in R$. On signifiera souvent ceci par la notation $x \sim y$ (ou $x \sim_R y$ s'il y a une ambiguïté à lever), et on utilisera indifférement R ou $\sim$ pour signifier la relation.*

— *Une relation $\sim$ sur X est une* relation d'équivalence *si elle satisfait aux trois conditions suivantes :*

i) Elle est réflexive *: si $x \in X$ alors $x \sim x$.*

ii) Elle est symétrique *: si $x \sim y$ alors $y \sim x$.*

iii) Elle est transitive : si $x, y, z \in X$ et $x \sim y, y \sim z$ alors $x \sim z$.

— *Si $x \in X$ le sous-ensemble $\{y \in X : x \sim y\}$ est alors appelé la* classe d'équivalence *(ou seulement* classe*) de x pour $\sim$. On la notera $[x]$ ou $\bar{x}$.*

Définition 2.2 *Une* partition *de X est une décomposition de X en sous-ensemble disjoints, autrement dit une collection de sous-ensembles $X_i \subset X, i \in I$ tels que $X_i \cap X_j = \emptyset$ si $i, j \in I, i \neq j$ et $X = \bigcup_{i \in I} X_i$. On indiquera cette situation par la notation*

$$X = \dot{\bigcup}_{i \in I} X_i.$$

La démonstration du résultat suivant est laissée à la lectrice.

Proposition 2.3 *Les classes d'une relation d'équivalence sur X forment une partition de X. Réciproquement, si $X = \dot{\bigcup}_{i \in I} X_i$ alors la relation $\sim$ sur X définie par*

$$\forall i \in I : \forall x \in X_i : \forall y \in X, x \sim y \Leftrightarrow y \in X_i$$

(en langage naturel : $x \sim y$ si x, y sont dans le même X_i) est une relation d'équivalence dont les classes sont exactement les X_i.

Définition 2.4 *Si $\sim$ est une relation d'équivalence sur X alors* l'ensemble quotient de X par $\sim$, *que l'on notera $X/\sim$, est l'ensemble des classes de $\sim$:*

$$X/\sim = \{\bar{x} : x \in X\}.$$

L'application $X \to X/\sim$ définie par $x \mapsto \bar{x}$ est appelée application canonique.

2.1.2 Relations d'équivalence associées à un sous-groupe et classes

Proposition 2.5 *Soient G un groupe et $H \subset G$ un sous-groupe. La relation $\sim$ sur G définie par*

$$g \sim g' \Leftrightarrow \exists h \in H : g' = gh$$

est une relation d'équivalence sur G. La relation $\sim'$ définie par

$$g \sim' g' \Leftrightarrow \exists h \in H : hg = g'$$

est aussi une relation d'équivalence, et on a $g^{-1} \sim (g')^{-1}$

Démonstration : On vérifie les trois propriétés définissant une relation d'équivalence l'une après l'autre pour $\sim$:

- Réflexivité : on a $e_G \in H$ donc pour tout $g \in G$ l'égalité $g = ge_G$ montre que $g \sim g$.
- Symétrie : Soient $g, g' \in G$ tels que $g \sim g'$ et $h \in H$ tel que $g' = gh$. On a alors $g = g'h^{-1}$ et comme $h^{-1} \in H$ il suit que $g' \sim g$.
- Transitivité : Si $g_1 \sim g_2$ et $g_2 \sim g_3$ il existe $h_1, h_2 \in H$ tels que $g_2 = g_1h_1$ et $g_3 = g_2h_2$ et il suit que $g_3 = g_1(h_1h_2)$ ce qui montre que $g_1 \sim g_3$.

Une démonstration exactement similaire (laissée au lecteur) montre que $\sim'$ est une relation d'équivalence. Ceci peut aussi se déduire directement du dernier énoncé. On va démontrer ce dernier ici : si $h \in H, g, g' \in G$ on a $hg = g'$ si et seulement si $(hg)^{-1} = (g')^{-1}$ si et seulement si $g^{-1}h^{-1} = (g')^{-1}$. Autrement dit $g \sim' g'$ si et seulement si $g^{-1} \sim g'$. □

Définition 2.6 *Les classes pour la relation $\sim$ de la proposition 2.5 sont appelées* classes à gauche de G modulo H. *On notera*

$$gH = \{gh : h \in H\}$$

la classe à gauche de g modulo H. Les classes de $\sim'$ sont appelées classes à droite de G modulo H *et on note Hg la classe de g.*

Remarque 2.7

- *Les classes à droite où à gauche de G modulo H ne sont pas des sous-groupes, sauf H lui-même qui est égal à la classe de e_G (dans les deux sens)—les autres ne peuvent donc pas contenir e_G.*
- *En général on a $gH \neq Hg$ (voir ci-dessous le calcul des classes à droite et à gauche d'un élément d'ordre 2 dans S_3).*
- *En fait, on a*

$$(\forall g \in G : gH = Hg) \Leftrightarrow H \triangleleft G.$$

Exemple 2.8 — *Soit $G = S_3$, $\tau \in S_3$ l'élément d'ordre 2 défini par $\tau(1) = 1$ et $\tau(2) = 3$, et $H = \langle \tau \rangle = \{\mathrm{Id}, \tau\}$. On note σ l'élément d'ordre 3 défini par $\sigma(1) = 2, \sigma(2) = 3$, τ' et τ'' les éléments d'ordre 2 tel que $\tau'(2) = 2$ et $\tau''(3) = 3$. Les classes à gauche de G modulo H sont alors :*

$$\begin{aligned} \mathrm{Id} \cdot H &= H; \\ \sigma H &= \{\sigma, \tau'\} \\ \sigma^2 H &= \{\sigma^2, \tau''\} \end{aligned}$$

et les classes à droite :

$$\begin{aligned} H \cdot \mathrm{Id} &= H; \\ H\sigma &= \{\sigma, \tau''\} \\ H\sigma^2 &= \{\sigma^2, \tau'\}. \end{aligned}$$

— *Soient $G = \mathbb{R} \times \mathbb{R}$ et $H = \mathbb{R} \times \{0\}$. Les classes (à droite et à gauche, ce sont les mêmes puisque G est abélien et donc $H \triangleleft G$) de H modulo H sont les sous-ensembles*

$$\{(x, a) : x \in \mathbb{R}\}$$

pour $a \in \mathbb{R}$.

2.1.3 Quotients de groupes et théorème de Lagrange

Proposition 2.9 *Soient G un groupe, H un sous-groupe et $g \in H$. Les classes à gauche et à droite gH et Hg sont en bijection avec H. En particulier*

$$|gH| = |H| = |Hg|.$$

Démonstration : On vérifie que l'application

$$\lambda_g : H \to gH,\ h \mapsto gh$$

est une bijection. Elle est surjective par définition de gH : on a $g' \in gH$ si et seulement si $g \sim g'$ si et seulement si $\exists h \in H : g' = gh$. Elle est injective car $gh = gh'$ si et seulement si $h = h'$. Pour les classes à droite on peut faire la même démonstration avec $\rho_g : h \mapsto hg$, ou observer que $x \mapsto x^{-1}$ induit une bijection de gH vers Hg^{-1} (les détails sont laissés à la lectrice). □

Définition 2.10 *Soient G un groupe, H un sous-groupe.*

— *On appelle* quotient à gauche *(respectivement* à droite*) de G par H, et on note G/H (respectivement $H\backslash G$) l'ensemble des classes à gauche (respectivement à droite) de G modulo H.*

— *L'*indice *de H dans G est le cardinal de G/H (ou $H\backslash G$). On le notera $[G : H]$*

Théorème 2.11 *Soient G un groupe et H un sous-groupe. On a*

$$|G| = [G : H] \cdot |H|.$$

Démonstration : Comme G est fini l'indice $[G : H]$ est aussi fini. Soient $X_1, \ldots, X_{[G:H]}$ les classes à gauche de G modulo H. Par la proposition 2.9 on a $|X_i| = |H|$ pour $i = 1, \ldots, [G : H]$ et comme d'autre part $G = \overset{\bullet}{\bigcup}_{i=1}^{[G:H]} X_i = G$ il vient :

$$|G| = \sum_{i=1}^{[G:H]} |X_i| = \sum_{i=1}^{[G:H]} |H| = [G : H] \cdot |H|$$

ce qui termine la démonstration. □

Corollaire 2.12 *(Théorème de Lagrange) Si G est un groupe d'ordre fini et H est un sous-groupe de G alors $|H|$ divise $|G|$.*

Corollaire 2.13 *Si p est un nombre premier et G est un groupe d'ordre p alors c'est un groupe cyclique.*

Démonstration : Soit $g \in G, g \neq e_G$ et soit H le sous-groupe engendré par g. On a $G \neq \{e_G\}$ puisque $g \in G$ et donc $|H| > 1$. D'autre part, par le théorème 2.11 on sait que $|H|$ divise p. Comme p est premier tout diviseur positif de p qui n'est pas égal à 1 est égal à p, et il suit que $|H| = p$ et donc $H = G$. Ceci signifie que g engendre G et qu'il est d'ordre p, autrement dit G est cyclique d'ordre p. □

Exemple 2.14
i) Si $n > 0$ alors les classes (à gauche ou à droite) de $\mathbb{Z}$ modulo $n\mathbb{Z}$ sont $\bar{0}, \bar{1}, \ldots, \overline{n-1}$. En effet, ce sont toutes les classes puisque la classe de x contient le reste de la division euclidienne de x par n, qui est un entier entre 0 et $n-1$. D'autre part elles sont deux à deuxdistinctes : si $y \in x + n\mathbb{Z}$ et $x \neq y$ alors $|x - y| \geq n$ donc si $x \sim y$ avec $0 \leq x < n$ on a $x = y$ ou $y \leq x - n < 0$ ou $y \geq x + n \geq n$.

ii) le sous-groupe trivial $\{e_G\}$ est d'indice $|G|$ dans G : la classe à droite ou à gauche de g est égale à $\{g\}$ et le quotient $G/\{e_G\}$ (ou $\{e_G\}\backslash G$) est identifié à G.

2.2 Actions de groupe

2.2.1 Définition

Définition 2.15 *Soient G un groupe et X un ensemble. Une* action à gauche de G sur X *est donnée par une application*

$$\begin{cases} G \times X & \to X \\ (g, x) & \mapsto g \cdot x \end{cases}$$

qui vérifie les deux conditions suivantes :

i) $\forall g, h \in G$, $x \in X$:

$$(gh) \cdot x = g \cdot (h \cdot x);$$

ii) $\forall x \in X$: $e_G \cdot x = x$.

On dit aussi que G opère à gauche sur X.

De manière semblable, une action à droite est définie par une application

$$\begin{cases} X \times G \to X \\ (x,g) \mapsto x \cdot g \end{cases}$$

vérifiant $x \cdot e_G = x$ *et* $x \cdot (gh) = (x \cdot g) \cdot h$ *pour touts* $g, h \in G$ *et* $x \in X$.

On notera $G \curvearrowleft X$ *pour indiquer une action à gaiche de* G *sur* X *et* $X \curvearrowright G$ *pour une action à droite.*

Remarque 2.16 — *La condition* $e_G \cdot x = x$ *est une condition de non-dégénérescence et revient à demander que les applications* $\lambda(g) : x \mapsto g \cdot x$ *pour* $g \in G$ *soient bijectives (voir la démonstration de la proposition 2.18 ci-dessous).*

— *Si on a une action à gauche* $(g,x) \mapsto g \cdot x$ *alors* $(x,g) \mapsto g^{-1} \cdot x$ *définit une action à droite.*

Exemple 2.17 *i) L'application*

$$\mathbb{Z}/3\mathbb{Z} \times \mathbb{C} \to \mathbb{C},\ (\bar{k}, z) \mapsto e^{2i\pi k/3} z$$

définit une action de $\mathbb{Z}/3\mathbb{Z}$ *sur* $\mathbb{C}$.

ii) L'application

$$t \cdot (x_1, x_2) = (x_1 + t, x_2)$$

définit une action de $\mathbb{R}$ *sur* $\mathbb{R}^2$. *De même* $(t_1, t_2) \cdot (v_1, v_2) = (v_1 + t_1, v_2 + t_2)$ *définit une action de* $\mathbb{R}^2$ *sur* $\mathbb{R}^2$.

iii) Soit G *un groupe quelconque. Alors on a deux actions à gauche de* G *sur lui-même :*

*(a) L'*action par translations à gauche*, définie par :*

$$g \cdot h = gh;$$

*(b) L'*action par conjugaison*, définie par :*

$$g \cdot h = ghg^{-1}.$$

On peut définir des actions à droite correspondantes par $h \cdot g = hg$ *et* $h \cdot g = g^{-1}hg$.

iv) Si G, X *sont quelconques on peut toujours définir l'*action triviale *de* G *sur* X *par* $g \cdot x = x$.

Si X est un ensemble on rappelle que $\mathrm{Bij}(X)$ désigne le groupe des bijections $X \to X$. On observe que le concept d'action se ramène à celui de morphisme de groupes vers $\mathrm{Bij}(X)$.

Proposition 2.18 *Si* $F : G \times X \to X$ *définit une action de* G *à gauche sur* X *on note, pour tout* $g \in G$, $\lambda_F(g)$ *l'application de* X *dans lui-même défine par* $\lambda_F(x) = F(g,x)$. *Alors l'application* $F \mapsto \lambda_F$ *est une bijection de l'ensemble des actions de* G *sur* X *vers l'ensemble des morphismes* $G \to \mathrm{Bij}(X)$.

Démonstration : Commençons par vérifier que si F définit une action alors λ_F est un morphisme vers $\mathrm{Bij}(X)$. Tout d'abord $\lambda_F(g)$ est bien une bijection : en effet d'après les axiomes 2.2.15.i) et 2.2.15.ii) on voit que $\lambda_F(g^{-1})$ est son application inverse :

$$\begin{aligned}\lambda_F(g)(\lambda_F(g^{-1})(x)) &= g \cdot (g^{-1} \cdot x) \\ &= (gg^{-1}) \cdot x = e_G \cdot x = x\end{aligned}$$

donc $\lambda_F(g) \circ \lambda_F(g^{-1}) = \mathrm{Id}_X$ et de même on voit que $\lambda_F(g^{-1}) \circ \lambda_F(g) = \mathrm{Id}_X$.

Il suit alors immédiatement de 2.2.15.i) que λ_F est un morphisme.

Il reste à vérifier la bijectivité. Pour ceci on observe qu'étant donné un morphisme de groupes $\lambda : G \to \mathrm{Bij}(X)$ on peut lui associer l'action à gauche définie par

$$F_\lambda(g, x) = \lambda(g)(x)$$

et on vérifie alors immédiatement que les composées

$$F \mapsto \lambda_F \mapsto F_{\lambda_F},\ \lambda \mapsto F_\lambda \mapsto \lambda_{F_\lambda}$$

sont l'identité de leurs ensembles de définition respectifs, c'est-à-dire que $F \mapsto \lambda_F$ est bijective d'inverse $\lambda \mapsto F_\lambda$. □

2.2.2 Orbites

Définition 2.19 *Soit $G \curvearrowright X$ une action de groupe. Si $X \in X$, l'*orbite de x sous G *est le sous-ensemble*

$$\mathrm{Orb}(x) = \{g \cdot x : g \in G\}.$$

Proposition 2.20 *Soit G un groupe agissant à gauche sur un ensemble X. Soit $\sim$ la relation sur X définie par :*

$$x \sim y \Leftrightarrow \exists g \in G : y = g \cdot x.$$

Alors $\sim$ est une relation d'équivalence sur X, et la classe de $x \in X$ est égale à son orbite sous G.

Démonstration :

□

Exemple 2.21 *i) Les orbites de l'action de $\mathbb{Z}/3\mathbb{Z}$ sur $\mathbb{C}$ décrite en 2.2.17.i) sont les sous-ensembles*

$$\{z, e^{2i\pi/3}z, e^{-2i\pi/3}\}$$

pour $Z \in \mathbb{C}$. Noter que si $z \neq 0$ c'est un ensemble de cardinal 3, alors que l'orbite de 0 est réduite à $\{0\}$.

ii) Les orbites de l'action $\mathbb{R} \curvearrowright \mathbb{R}^2$ décrite en 2.2.17.ii) sont les droites $\{(a, y) : y \in \mathbb{R}\}$ pour $a \in \mathbb{R}$.

iii) L'action par translation à gauche d'un groupe sur lui-même n'a qu'une seule orbite.

Définition 2.22 *Si l'action de G sur X n'a qu'une seule orbite (c'est-à-dire que $\forall x, y \in X \exists g \in Gy = g \cdot x$) on dit qu'elle est* transitive.

Définition 2.23 *i) Soit $x \in X$. Le* stabilisateur de x dans G *est :*

$$\mathrm{Stab}_G(x) = \{g \in G : g \cdot x = x\}.$$

C'est un sous-groupe de G, comme il suit immédiatement des axiomes définissant une action (laissé à la lectrice).

ii) Si $g \in G$ on note $\mathrm{Fix}(g)$ *l'ensemble des points fixes de g dans X :*

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

iii) On dit que $x \in X$ est un point fixe de G si $\forall g \in G : g \cdot x = x$.

Proposition 2.24 *Soit $G \curvearrowright X$ une action à gauche. Soit $x \in X$ et $y \in \mathrm{Orb}(x)$. Les sous-groupes $\mathrm{Stab}_G(x)$ et $\mathrm{Stab}_G(y)$ sont conjugués dans G.*

Démonstration : Par définition de $\mathrm{Orb}(x)$ il existe un $g \in G$ tel que $y = gx$. On va montrer que

$$\mathrm{Stab}_G(y) = g\,\mathrm{Stab}_G(x)g^{-1}.$$

Pour ceci il suffit de voir que

$$g\,\mathrm{Stab}_G(x)g^{-1} \subset \mathrm{Stab}_G(y); \tag{2.2.1}$$

en effet en appliquant ceci avec x remplacé par y et g par g^{-1} on en déduit l'inclusion contraire.

La démonstration de (2.2.1) est une simple vérification : si $k \in \mathrm{Stab}_G(x)$ il vient

$$\begin{aligned}(gkg^{-1}) \cdot y &= (gk) \cdot (g^{-1} \cdot (gx)) \\ &= (gk) \cdot (e_G \cdot x) \\ &= g \cdot (kx) = g \cdot c = y\end{aligned}$$

donc on a bien $gkg^{-1} \in \mathrm{Stab}_G(y)$. □

Théorème 2.25 *Soit G un groupe agissant sur un ensemble X. Si $x \in X$ alors les ensembles $\mathrm{Orb}(x)$ et $G/\mathrm{Stab}_G(x)$ sont en bijection l'un avec l'autre.*

En particulier, si $orb(x)$ est finie alors $\mathrm{Stab}_G(x)$ est d'indice fini dans G, et $[G : \mathrm{Stab}_G(x)] = \mathrm{Orb}(x)$.

Démonstration : Dans toute cette démonstration on notera $K = \mathrm{Stab}_G(x)$. On veut définir une application Φ comme suit :

$$\Phi : \left\{ \begin{array}{rl} \mathrm{Orb}(x) & \to G/K \\ g \cdot x & \mapsto gK \end{array} \right. .$$

Pour vérifier que cette définition a un sens il faut démontrer que si $g, g' \in G$ vérifient $g \cdot x = g' \cdot x$ alors on a $gK = g'K$. On va en fait montrer le résultat suivant.

Lemme 2.26 *Si $g, g' \in G$ on a $gK = g'K$ si et seulement si $g' \cdot x = g \cdot x$.*

Démonstration : On a $g' \cdot x = g \cdot x$ si et seulement si $(g^{-1}g') \cdot x = x$. En posant $k = g^{-1}g'$ on voit que ceci revient à ce qu'il existe $k \in K$ tel que $g^{-1}g' = k$, autrement dit $g' = gk$. Ce qui veut exactement dire que g, g' ont la même classe à gauche modulo K. □

On va maintenant montrer que Φ est une bijection. Pour ceci on va exhiber une application Ψ dont on vérfifie qu'elle est sa bijection réciproque. On voudrait définir cette application par :

$$\Psi : \begin{cases} G/K & \to X \\ gK \mapsto gx & \end{cases}$$

et il faut vérifier que si $gK = g'K$ alors $gx = g'x$, ce qui est une conséquence du lemme ci-dessus. On voit alors immédiatement que

$$\Psi \circ \Phi(g \cdot x) = \Psi(gK) = g \cdot x$$

et

$$\Phi \circ \Psi(gK) = \Phi(g \cdot x) = gK$$

ce qui termine la démonstration que Φ, Ψ sont inverses l'une de l'autre et donc celle du théorème. □

Corollaire 2.27 *Formule des classes Soit G un groupe fini opérant sur X et $x \in X$. On a*

$$|\operatorname{Orb}(x)| \cdot |\operatorname{Stab}_G(x)| = |G|.$$

Exemple 2.28 *Un exemple particulièrement important de stabilisateur est donné par ceux des éléments non-triviaux dans l'action de G sur lui-même par conjugaison 2.2.17.iii)b. Dans ce cadre on introduit la nomenclature suivante :*

i) L'orbite de $h \in G$ est donnée par

$$\{ghg^{-1} : g \in G\}$$

et est appelée classe de conjugaison *de h dans G. On dit que h, h' sont* conjugués *dans G s'ils ont la même classe de conjugaison, autrement dit $\exists g \in G ghg^{-1} = h'$.*

ii) Le stabilisateur de $h \in G$ est :

$$\operatorname{Stab}_G(h) = \{g \in G : ghg^{-1} = h\}$$

et est appelé centralisateur *de h dans G. On note qu'il est aussi égal à $\{g \in G : gh = hg\}$, l'ensemble des éléments de G commutant à h.*

Pour un exemple plus concret on prend $G = \operatorname{Isom}(T)$ le groupe des isométries du triangle équilatéral ABC. Les classes de conjugaison sont alors :

$$C_1 = \{\mathrm{Id}\},\ C_2 = \{s_A, s_B, s_C\},\ C_3 = \{r_{2\pi/3}, r^2_{2\pi/3}\}.$$

Le centralisateur de l'identité est G tout entier (c'est évidemment toujours le cas pour l'élément neutre d'un groupe). Dns les autre cas le centralisateur de g contient toujours au moins le sous-groupe $\langle g \rangle$ engendré par g : le formule des classe permet de vérifier rapidement que pour un élément de C_2 et C_3 le centralisateur est en fait réduit à ce sous-groupe.

Un peu plus de nomenclature pour les actions :

i) Une action $G \curvearrowright X$ est dite *libre* si aucun élément de G distinct du neutre n'a de point fixe, autrement dit :

$$\forall g \in G, g \neq e_G : \forall x \in X g \cdot x \neq x.$$

ii) Elle est dite fidèle si aucun élément non-neutre n'agit trivialement, autrement dit :

$$\forall g \in G, g \neq e_G : \exists x \in X g x \neq x.$$

De manière équivalente le morphisme $G \to \mathrm{Bij}(X)$ est injectif.

Noter qu'une action libre est fidèle mais la réciproque est fausse (voir les exemples ci-dessus.

Chapitre 3

Groupes symétrique et alterné

Soit $n \geq 1$. On rappelle que le *groupe symétrique* sur $\{1, \ldots, n\}$, ou groupe des permutations de $\{1, \ldots, n\}$, est défini par :

$$S_n = \{\text{bijections } \{1, \ldots, n\} \to \{1, \ldots, n\}\}.$$

Un élément de S_n est appelé une *permutation*. Pour désigner une permutation $\sigma \in S_n$ on utilisera la notation :

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}.$$

Les groupes S_n sont des exemples importants de groupes finis. D'autant plus que par le « théorème de Cayley » tout groupe fini G est isomorphe à un sous-groupe d'un groupe S_n.

Proposition 3.1 *On a* $|S_n| = n!$.

Démonstration : On va démontrer ceci par récurrence sur n en utilisant les actions de groupe. Le groupe S_1 est le groupe trivial $\{\mathrm{Id}\}$ et son cardinal est donc égal à $1 = 1!$. On va maintenant montrer que $|S_n| = n|S_{n-1}|$ pour $n \geq 2$. Pour ceci on considère l'action de S_n sur $\{1, \ldots, n\}$: elle est transitive et il suit donc par la formule des classes (Corollaire 2.27) que l'on a

$$|S_n| = n \cdot |\operatorname{Stab}_{S_n}(1)|. \tag{3.0.1}$$

D'autre part, le sous-groupe $\operatorname{Stab}_{S_n}(1)$ est composé de toutes les permutations fixant 1, donc préservant le sous-ensemble $\{2, \ldots, n\}$. Il est donc isomorphe au groupe des bijections de $\{2, \ldots, n\}$ dans lui-même, qui est isomorphe à S_{n-1} et le résultat voulu est donc une conséquence de (3.0.1). □

3.1 Décomposition en cycles

Définition 3.2 *Soient* $n \geq 1$ *et* $1 \leq p \leq n$. *On dit qu'un élément* $\sigma \in S_n$ *est un* p-cycle *(ou simplement un cycle) s'il existe* $a_1, \ldots, a_p \in \{1, \ldots, n\}$ *tels que* $\sigma(a_i) = a_{i+1}$ *pour* $i = 1, \ldots, p-1$, $\sigma(a_p) = a_1$ *et* $\sigma(k) = k$ *si* $k \notin \{a_1, \ldots, a_p\}$.

Un 2-cycle est aussi appelé une transposition.

Exemple 3.3 *i) Dans S_3 les 3-cycles sont les permutations données par :*

$$\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}, \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$$

et les transpositions par :

$$\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}, \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}, \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}.$$

ii) Pour tout n, le seul 1-cycle dans S_n est l'identité.

Définition 3.4 *Soient $n \geq 1$, $\sigma \in S_n$.*

i) Si $i \in \{1, \ldots, n\}$ et $\sigma(i) = i$ on dit que i est un point fixe *de σ.*

ii) Le support *de σ est le complémentaire dans $\{1, \ldots, n\}$ de l'ensemble des points fixes de σ :*

$$\mathrm{Supp}(\sigma) = \{i \in \{1, \ldots, n\} : \sigma(i) \neq i\}.$$

Exemple 3.5 *Soit $\sigma \in S_8$ la permutation donnée par :*

$$\begin{pmatrix}1&2&3&4&5&6&7&8\\2&8&1&5&3&6&7&4\end{pmatrix}$$

on voit que les points fixes de σ sont $6, 7$ et son support est donc $\{1, 2, 3, 4, 5, 8\}$.

Si $\sigma \in S_n$ est le p-cycle associé à $a_1, \ldots, a_p$ comme dans la définition alors son support est exactement $\{a_1, \ldots, a_p\}$. On notera $\sigma = (a_1\, a_2 \cdots a_p)$. Par exemple la permutation $\begin{pmatrix}1&2&3&4&5\\5&4&3&1&2\end{pmatrix}$ est le cycle $(1\,4\,2\,5)$.

On note que si σ est un p-cycle alors σ^{-1} en est aussi un , de même support. En effet on vérifie immédiatement que l'on a :

$$(a_1\, a_2 \cdots a_p)^{-1} = (a_p\, a_{p-1} \cdots a_1).$$

Proposition 3.6 *Soient $n \geq 1$ et $\sigma, \rho \in S_n$.*

i) On a $\mathrm{Supp}(\sigma \circ \rho) \subset \mathrm{Supp}(\sigma) \cup \mathrm{Supp}(\rho)$.

ii) Si $\mathrm{Supp}(\sigma) \cap \mathrm{Supp}(\rho) = \emptyset$ alors $\mathrm{Supp}(\sigma \circ \rho) = \mathrm{Supp}(\sigma) \cup \mathrm{Supp}(\rho)$ et de plus $\sigma \circ \rho = \rho \circ \sigma$.

Démonstration : Pour démontrer le point 3.3.6.i) on va plutôt montrer que $\mathrm{Fix}(\sigma \circ \rho) \supset \mathrm{Fix}(\sigma) \cap \mathrm{Fix}(\rho)$: le résultat suit vu que l'on a

$$\begin{aligned}\mathrm{Supp}(\sigma \circ \rho) &= (\{1, \ldots, n\} \setminus \mathrm{Fix}(\sigma)) \cup (\{1, \ldots, n\} \setminus \mathrm{Fix}(\sigma)) \\ &= \{1, \ldots, n\} \setminus (\mathrm{Fix}(\sigma) \cap \mathrm{Fix}(\rho)).\end{aligned}$$

Soit donc $x \in \mathrm{Fix}(\sigma) \cap \mathrm{Fix}(\rho)$. On a $\sigma \circ \rho(x) = \sigma(x) = x$ donc $x \in \mathrm{Fix}(\sigma \circ \rho)$ et ceci finit la dmonstration.

Pour le point 3.3.6.ii) il faut en plus montrer que l'on a $\sigma \circ \rho(x) \neq x$ si $x \in \mathrm{Supp}(\sigma) \cup \mathrm{Supp}(\rho)$. On voit en fait que l'on a :

— Si $x \in \mathrm{Supp}(\sigma)$ alors $x \notin \mathrm{Supp}(\rho)$ et donc $\sigma \circ \rho(x) = \sigma(x) \neq x$;

— Si $x \in \mathrm{Supp}(\rho)$ alors on a aussi $\rho(x) \in \mathrm{Supp}(\rho)$ et donc $\rho(x) \notin \mathrm{Supp}(\sigma)$ d'où il suit que $\sigma \circ \rho(x) = \rho(x) \neq x$.

On peut de plus montrer pareillement que $\rho \circ \sigma(x) = \sigma(x)$ pour $x \in \mathrm{Supp}(\sigma)$ et $\rho \circ \sigma(x) = \rho(x)$ pour $x \in \mathrm{Supp}(\rho)$. Comme le reste des points est fixé par σ et ρ on constate donc que l'on a bien $\sigma \circ \rho = \rho \circ \sigma$. □

Théorème 3.7 *Toute permutation non-trivial s'écrit de manière unique à l'ordre des facteurs près comme composée de cycles à supports deux à deux disjoints. Autrement dit, si $\sigma \in S_n, \sigma \neq \mathrm{Id}$ il existe $\gamma_1, \ldots, \gamma_r \in S_n$ tel que chaque $\gamma_i \neq \mathrm{Id}$ est un cycle et $\mathrm{Supp}(\gamma_i) \cap \mathrm{Supp}(\gamma_j) = \emptyset$ si $i \neq j$ tels que $\sigma = \gamma_r \circ \cdots \circ \gamma_1$ et l'ensemble $\{\gamma_1, \ldots, \gamma_r\}$ est uniquement déterminé par σ.*

Noter que dans la décomposition énoncée dans le théorème 3.7 ne figurent pas de 1-cycles, qui compromettraient son unicité.

Exemple 3.8 *i) La permutation de l'exemple 3.5 est le 6-cycle* $(1\,2\,8\,4\,5\,3)$.

ii) Si $\sigma \in S_8$ est donnée par

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 5 & 6 & 8 & 1 & 3 & 7 & 4 \end{pmatrix}$$

sa décomposition en cycles est :

$$\sigma = (1\,2\,5)(3\,6)(4\,8).$$

iii) Si $\sigma \in S_9$ est donnée par

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 2 & 9 & 1 & 5 & 8 & 4 & 3 & 6 \end{pmatrix}$$

sa décomposition en cycles est

$$\sigma = (1\,7\,4)(3\,9\,6\,8).$$

Démonstration : La démonstration est par récurrence, et donne l'algorithme utilisé en pratique pour calculer la décomposition en cycles.

Pour $n = 1, 2, 3$ toutes les permutations sont des cycles (vérification laissée à la lectrice). Supposons $n \geq 4$ et soit $\sigma \in S_n$. Soit $X \subset \{1, \ldots, n\}$ le sous-ensemble défini par :

$$X = \{\sigma^k(1) : k \geq 0\}$$

et $m = |X|$. Autrement dit X est l'orbite de 1 sous le groupe $\langle\sigma\rangle$ et il suit que l'on a

$$X = \{1, \sigma(1), \ldots, \sigma^{m-1}(1)\}$$

et que $\sigma^m(1) = 1$. Soit γ_1 le cycle $(1\,\sigma(1)\,\cdots\,\sigma^{m-1}(1))$, on voit que l'on a

$$\forall x \in X : \sigma\gamma_1^{-1}(x) = x.$$

Si $X = \{1, \ldots, n\}$ on a donc montré que $\sigma = \gamma_1$ est un cycle. Si $X \neq \{1, \ldots, n\}$ alors on considère $Y = \{1, \ldots, n\} \setminus X$ et la restricition $\sigma|_Y$ de σ à Y. Comme $|Y| < n$, par l'hypothèse de récurrence

il existe des cycles $\gamma_2, \ldots, \gamma_r$ à supports disjoints tels que $\sigma|_Y = \gamma_r \cdots \gamma_2$. On remarque de plus que comme $\mathrm{Supp}(\gamma) = X$ on a $(\sigma\gamma_1^{-1})|_Y = \sigma|_Y$ par 3.3.6.ii) et il suit que

$$\sigma\gamma_1^{-1} = \gamma_r \cdots \gamma_2$$

et donc σ est le produit des γ_i.

Pour démontrer l'unicité on suppose que $\gamma_r \cdots \gamma_1 = \sigma = \delta_s \cdots \delta_1$ où les γ_i sont des cycles à supports disjoints de même que les δ_j. Soit $1 \leq i \leq r$. Si $x \in \mathrm{Supp}(\gamma_i)$ alors $x \in \mathrm{Supp}(\sigma)$ et il existe j tel que $x \in \mathrm{Supp}(\delta_j)$ (sinon il serait fixé par tous les δ_j et donc par σ). On a alors

$$\gamma_i(x) = \sigma(x) = \delta_j(x)$$

et en itérant on voit que $\gamma_i = \delta_j$. □

Définition 3.9 *Soit $\sigma \in S_n$, et soit $\gamma_r \cdots \gamma_r$ sa décomposition en cycles. On suppose que γ_i est de longueur ℓ_i et que $\ell_r \geq \ell_{r-1} \geq \cdots \geq \ell_1$. Le r-uplet $(\ell_1, \ldots, \ell_r)$ est alors appelé le* type *de σ.*

3.2 Propriétés algébriques des permutations

3.2.1 Ordre

Proposition 3.10 *Si σ est de type $(\ell_1, \ldots, \ell_r)$ alors elle est d'ordre* $\mathrm{ppcm}(\ell_1, \ldots, \ell_r)$.

Démonstration : On observe d'abord que si γ est un p-cycle alors pour tout $1 \leq k \leq p-1$ la permutation γ^p a le même support que γ, et $\gamma^p = \mathrm{Id}$. En effet on voit immédiatement que $\gamma^k(x)x$ si $x \in \mathrm{Fix}(\sigma)$, et d'autre part si $\gamma = (a_1 \cdots a_p)$ on a $\gamma^k(a_i) = a_{i+k}$ (où les indices sont pris modulo p). Il suit en particulier que γ est d'ordre p (noter par contre que γ^k n'est pas un cycle en général—seulement si p, k sont premiers entre eux).

Soit maintenant $\sigma = \gamma_r \cdots \gamma_1$ la décomposition en cycles de σ, de sorte que γ_i est d'ordre ℓ_i. On voit d'après ce qui précède et 3.3.6.ii) que l'on a

$$\sigma^k = \gamma_r^k \cdots \gamma_1^k$$

et il suit que $\sigma^k = \mathrm{Id}$ si et seulement si $\gamma_i^k = \mathrm{Id}$ pour $1 \leq i \leq r$, c'est-à dire $\ell_i | k$. Il suit que le plus petit entier k positif pour lequel $\sigma^k = \mathrm{Id}$ est le plus petit commun multiple des ℓ_i. □

Exemple 3.11 *i) Si* $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 5 & 1 & 3 \end{pmatrix}$ *on calcule* $\sigma = (1\,2\,4)(3\,5)$ *et σ est donc d'ordre* 6.

ii) Si $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 5 & 6 & 3 & 1 \end{pmatrix}$ *on a* $\sigma = (1\,2\,4\,6)(3\,5)$ *et il suit que σ est d'ordre 4.*

3.2.2 Classes de conjugaisons

Proposition 3.12 *Deux permutations $\sigma, \rho \in S_n$ sont conjuguées dans S_n si et seulement si elles ont le même type.*

Démonstration : L'élément principal de la démonstration est le lemme suivant :

Lemme 3.13 *Soit $\gamma = (a_1 \cdots a_p)$ un p-cycle et $\alpha \in S_n$. Alors $\alpha\gamma\alpha^{-1}$ est le p-cycle $(\alpha(a_1) \cdots \alpha(a_p))$.*

Démonstration : Pour $A \leq i \leq p-1$ on a :

$$\alpha\gamma\alpha^{-1}(\alpha(a_i)) = \alpha\gamma(a_i) = \alpha(a_{i+1})$$

et de même $\alpha\gamma\alpha^{-1}(\alpha(a_p)) = \alpha(a_1)$. D'autre part on voit immédiatement que si $x \in \mathrm{Fix}(\gamma)$ alors $\alpha(x) \in \mathrm{Fix}(\alpha\gamma\alpha^{-1})$. □

On voit ainsi que si $\rho = \alpha\sigma\alpha^{-1}$ et $\sigma = \gamma_r \cdots \gamma_1$ est la décomposition en cycles de σ alors

$$\rho = (\alpha\gamma_r\alpha^{-1})(\alpha\gamma_{r-1}\alpha^{-1}) \cdots (\alpha\gamma_1\alpha^{-1})$$

est la décomposition en cycles de ρ et les deux ont même profil.

Réciproquement, supposons que $\sigma = \gamma_r \cdots \gamma_1$ et $\rho = \eta_r \cdots \eta_1$ sont les décompositions en cycles respectives de σ, ρ et γ_i, η_i ont la même longueur ℓ_i. On note alors $\gamma_i = (a_{i,1} \cdots a_{i,\ell_i})$ et $\eta_i = (b_{i,1} \cdots b_{i,\ell_i})$ et on définit une permutation α par :

$$\alpha(x) = \begin{cases} b_{i,l} & \text{si } x = a_{i,l} \text{ pour des } 1 \leq i \leq r, 1 \leq l \leq \ell_i \\ x \text{ sinon.} & \end{cases}$$

On voit alors en utilisant le lemme que $\alpha\gamma_i\alpha^{-1} = \eta_i$ pour $1 \leq i \leq r$ et donc :

$$\alpha\sigma\alpha^{-1} = (\alpha\gamma_r\alpha^{-1})(\alpha\gamma_{r-1}\alpha^{-1}) \cdots (\alpha\gamma_1\alpha^{-1}) = \rho$$

et donc σ est conjugué à ρ. □

3.3 Générateurs du groupe symétrique

Lemme 3.14 *Un ℓ-cycle peut s'écrire comme un produit de $(\ell - 1)$ transpositions.*

Démonstration : La démonstration se fait par récurrence sur ℓ. Pour $\ell = 2$ l'énoncé est tautologique. Si $\ell \geq 3$ on note $\gamma = (a_1 \cdots a_\ell)$. On voit alors que

$$(a_1\, a_2)\gamma = (a_2 \cdots a_\ell)$$

et par l'hypothése de récurrence on peut donc écrire $(a_1\, a_2)\gamma$ comme un produit de $(\ell - 2)$ transpositions $\tau_2, \ldots, \tau_{\ell-1}$. Il vient alors :

$$\gamma = (a_1\, a_2)\tau_2 \cdots \tau_{\ell-1}$$

et on voit donc que γ peut s'écrire comme produit de $\ell - 1$ transposition. □

Remarque 3.15 — *En examinant la preuve on voit que l'on montre en fait le résultat plus précis que*

$$(a_1 \cdots a_\ell) = (a_1\, a_2)(a_2\, a_3)\cdots(a_{\ell-1}\, a_\ell).$$

On peut aussi changer légèrement la démonstration pour obtenir la décomposition suivante :

$$(a_1 \cdots a_\ell) = (a_1\, a_\ell)(a_1\, a_{\ell-1})\cdots(a_1\, a_2).$$

— *On ne peut pas faire mieux que $\ell - 1$, en effet si le support d'un porduit de p transpositions est de taille $> p+1$ alors ce produit a au moins deux cycles dans sa décomposition (ceci se voit facilement par récurrence sur p).*

Proposition 3.16 *Le groupe symétrique est engéndré par les transpositions.*

Démonstration : Il suit immédiatement de la décomposition en cycles et du le lemme précédent que toute permutation s'écrit comme produit de transpositions, ce qui prouve cet énoncé. □

3.4 Signature

Le sous-ensemble $\{\pm 1\} \subset \mathbb{C}$ est un sous-groupe du groupe multiplicatif $\mathbb{C}^\times$, et c'est un groupe cyclique d'ordre 2. On dira qu'un morphisme de groupes $\phi : G \to H$ est *trivial* si on a $\varphi(g) = e_H$ pour tout $g \in G$.

Théorème 3.17 *Soit $n \geq 2$. Il existe un unique morphisme de groupes non-trivial $\varepsilon : S_n \to \{\pm 1\}$. Si $\sigma \in S_n$ est de type $(\ell_1, \ldots, \ell_r)$ on a :*

$$\varepsilon(\sigma) = (-1)^{\sum_{i=1}^r \ell_i - r}. \tag{3.4.1}$$

Remarque 3.18 *i) Il n'est pas clair a première vue que l'expression* (3.4.1) *définisse un morphisme de groupes.*

ii) La démonstration que l'on va donner du théorème ci-dessus montre (à quelques modifications près) l'énoncé plus fort suivant : si φ est un morphisme non-trivial de S_n dans un groupe abélien A alors il existe un morphism $\psi : \{\pm 1\} \to A$ tel que $\phi = \psi \circ \varepsilon$.

Démonstration : On commence par démontrer l'unicité de ε, c'est-à-dire qu'il existe au plus un morphisme non-trivial $S_n \to \{\pm 1\}$. Soit donc $\phi : S_n \to \{\pm 1\}$ un morphisme. Soit $\tau_0 = (1\,2)$ et $x_0 = \phi(\tau_0)$. On va montrer que si $x_0 = 1$ alors ϕ est trivial. Si ϕ, ψ sont deux morphismes non-triviaux $S_n \to \{\pm 1\}$ alors $\pi : \sigma \mapsto \phi(\sigma)\psi(\sigma)$ est un morphisme (parce que $\{\pm 1\}$ est abélien) et on a $\phi(\tau_0) = -1 = \psi(\tau_0)$ donc $\pi(\tau_0) = 1$ et $\pi(\sigma) = 1$ pour tout $\sigma \in S_n$. Finalement, on voit que our tout $\sigma \in S_n$ on a $\phi(\sigma)\psi(\sigma) = 1$ donc (comme les éléments de $\{\pm 1\}$ sont tous d'order 1 ou 2) $\phi(\sigma) = \psi(\sigma)$, c'est-à-dire $\phi = \psi$.

On suppose donc que $x_0 = 1$ et on veut montrer que $\phi(\sigma) = 1$ pour tout $\sigma \in S_n$. On commence par les transpositions : si τ est une transposition alors elle est conjuguée dans S_n à τ_0, donc il existe $g \in S_n$ telle que $g\tau_0 g^{-1} = \tau$. Il vient alors :

$$\begin{aligned}\phi(\tau) &= \phi(g\tau_0 g^{-1}) \\ &= \phi(g)\phi(\tau_0)\phi(g^{-1}) \\ &= \phi(g)\phi(g)^{-1} = 1.\end{aligned}$$

On prend ensuite $\sigma \in S_n$ quelconque ; comme S_n est engendré par les transpositions (proposition 3.16) il existe des transpositions $\tau_1, \ldots, \tau_l$ telles que $\sigma = \tau_l \cdots \tau_1$. Il suit que

$$\phi(\sigma) = \phi(\tau_l) \cdots \phi(\tau_1) = 1 \cdots 1 = 1$$

ce qui finit la démonstration du fait que ϕ est trivial, et donc de l'unicité.

On va maintenant montrer qu'il existe bien un morphisme non-trivial $S_n \to \{\pm 1\}$. Plutôt que d'étudier directement l'expression (3.4.1) on va faire un détour en introduisant les définitions suivantes. Si $\sigma \in S_n$ son *nombre d'inversions* est l'entier défini par :

$$\mathrm{Inv}(\sigma) = |\{1 \leq i < j \leq n : \sigma(i) > \sigma(j)\}|.$$

On va vérifier que $(-1)^{\mathrm{Inv}}$ définit un morphisme, pour ceci l'ingrédient proncipal est le lemme suivant.

Lemme 3.19 *Si $\tau_1 \ldots, \tau_l$ sont des transpositions et $\sigma = \tau_l \cdots \tau_1$ alors*

$$\mathrm{Inv}(\sigma) \equiv l \pmod 2.$$

Démonstration : La démonstration se fait par récurrence sur l : si $l = 0$ le résultat est clair. Il faut maintenant montrer que si σ est une permutation quelconque et τ une transposition alors $\mathrm{Inv}(\tau\sigma) - \mathrm{Inv}(\sigma)$ est impair. Pour ceci on considère deux entiers i, j tels que $\sigma(i) < \sigma(j)$ (noter que l'on ne fait aucune hypothèse sur i, j). On écrit $\tau = (a\, b)$ avec $a < b$. Il y a alors trois cas de figure possibles :

i) Si $\sigma(i) < a$ ou $\sigma(j) > b$ ou $a < \sigma(i) < \sigma(j) < b$ alors $\tau\sigma(i) < \tau\sigma(j)$;
ii) Si $a = \sigma(i) < \sigma(j) \leq b$ alors $\tau\sigma(i) > \tau\sigma(j)$;
iii) Si $a < \sigma(i) < \sigma(j) = b$ alors $\tau\sigma(i) > \tau\sigma(j)$.

Pour chaque i, j dans la configuration 3.3.19.ii) ou 3.3.19.iii) on ajoute ou elève donc une inversion, et dans le cas 3.3.19.i) on ne touche pas au nombre d'inversion. Comme $1 \equiv -1 \pmod 2$ on a donc :

$$\mathrm{Inv}(\tau\sigma) - \mathrm{Inv}(\sigma) \equiv |\{i, j : a = \sigma(i) < \sigma(j) \leq b\}| + |\{i, j : a < \sigma(i) < \sigma(j) = b\}| \pmod 2$$

et le côté droit est égal à

$$|\{j : a < \sigma(j) \leq b\}| + |\{i : a < \sigma(i) < b\}| = (b - a) + (b - a - 1) = 2(b - a) - 1$$

et on voit donc que

$$\mathrm{Inv}(\tau\sigma) - \mathrm{Inv}(\sigma) \equiv -1 \pmod 2$$

ce qui finit la preuve. □

On pose maintenant :

$$\varepsilon(\sigma) = (-1)^{\mathrm{Inv}(\sigma)}$$

et on va vérifier que ε est un morphisme non-trivial $S_n \to \{\pm 1\}$. Si $\sigma, \rho \in S_n$ on peut les écrire comme produits de transpositions $\sigma = \tau_l \cdots \tau_1$ et $\rho = \tau'_m \cdots \tau'_1$ et on a alors d'après le lemme :

$$\begin{aligned} \varepsilon(\rho\sigma) &= \varepsilon(\tau'_m \cdots \tau'_1 \tau_l \cdots \tau_1) \\ &= (-1)^{m+l} \\ &= (-1)^m (-1)^l = \varepsilon(\rho)\varepsilon(\sigma) \end{aligned}$$

ce qui montre que ε est un morphisme. Il est non-trivial parce que $\varepsilon(\tau) = -1$ si τ est une permutation.

Il reste à montrer la formule (3.4.1). Soit $\sigma = \gamma_r \cdots \gamma_1$ où γ_i est un ℓ_i-cycle. On peut écrire (lemme 3.14) $\gamma_i = \tau_{i,\ell_i-1} \cdots \tau_{i,1}$ où les $\tau_{i,j}$ sont des transpositions, et il vient alors :

$$\varepsilon(\sigma) = \varepsilon\left((\tau_{r,\ell_r-1} \cdots \tau_{r,1}) \cdots (\tau_{1,\ell_1-1} \cdots \tau_{1,1})\right) = (-1)^{(\ell_r-1)+\cdots+(\ell_1)-1}$$

et comme $(\ell_r - 1) + \cdots + (\ell_1) - 1 = \sum_i \ell_i - r$ ceci termine la démonstration. □

Définition 3.20 *Si $\sigma \in S_n$ on appelle $\varepsilon(\sigma)$ la* signature *de σ. Le morphisme ε est appelé* signature.

Exemple 3.21 *La formule* (3.4.1) *est utilisée en pratique pour calculer la signature d'une permutation σ. On compte le nombre de cycles de longueur paire dans σ, et $\varepsilon(\sigma)$ vaut -1 si ce dernier est impair et* 1 *s'il est pair. Par exemple, soit*

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 6 & 1 & 3 & 2 \end{pmatrix}$$

on a la décomposition en cycles

$$\sigma = (1\,4)(2\,5\,3\,6)$$

et on a donc $\varepsilon(\sigma) = 1$.

3.5 Groupe alterné

Dans cette section n est toujours un entier ≥ 2 et $\varepsilon : S_n \to \{\pm 1\}$ désigne la signature.

Définition 3.22 *Le* groupe alterné *de degré n est le sous-groupe* $\ker(\varepsilon) \subset S_n$. *On le note A_n.*

3.5.1 Propriétés immédiates

Les propriétés suivantes sont des conséquences immédiates de la définition.

i) A_n est un sous-groupe d'indice 2 dans A_n. En particulier

$$|A_n| = \frac{|S_n|}{2} = \frac{1}{2}n!.$$

ii) Une permutation est dans A_n si et seulement si sa décomposition en cycles contient un nombre pair de cycles de longueur paire. En particulier un cycle est dans A_n si st seulement s'il est de longueur impaire.

3.5.2 Groupes alternés de petit degré

Dans ces exemples les démonstrations sont souvent faites en exercice ou laissées à la lectrice.

A_3

Comme S_3 ne contient que des 2- et 3-cycles on voit que S_3 ne contient que les 3-cycles et l'identité. On a donc :

$$A_3 = \{\mathrm{Id}, (1\,2\,3), (1\,3\,2)\}.$$

Ceci correspond bien à $|A_3| = 3!/2 = 6/2 = 3$. On voit de plus que A_3 est un groupe cyclique d'ordre 3.

A_4

Les types possibles pour les permutations de degré 4 sont $(2,1,1), (3,1), (4)$ et $(2,2)$. On voit que seules celles de type $(3,1)$ ou $(2,2)$ sont alternées. On compte qu'il y a huit 3-cycles dans S_4 et 3 permutations de type $(2,2)$, et on a bien $8+3+1 = 12 = 24/2 = 4!/2$. Explicitement, on a :

$$\begin{aligned} A_4 = \{&\mathrm{Id}, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3),\\ &(1\,2\,3), (1\,3\,2), (1\,3\,4), (1\,4\,3), (1\,2\,4), (1\,4\,2), (2\,3\,4), (2\,4\,3)\}. \end{aligned}$$

Finalement, on remarque que A_4 n'est pas abélien (contrairement à A_3) et que les permutations de type $(2,2)$ et l'identité forment un sous-groupe distingué d'ordre 4 dans A_4.

Le groupe A_5

Le groupe A_5 contient les permutations de types $(3,1,1), (5)$ et $(2,2,1)$. Il y a vingt 3-cycles, vingt-quatre 5-cycles et quinze permutations de type $(2,2)$ et on voit bien que $1+20+24+15 = 60 = 5!/2$. Contrairement à A_4 le groupe A_5 n'a pas de sous-groupe distingué propre non-trivial.

Proposition 3.23 *Si $H \lhd A_5$ alors $H = \{\mathrm{Id}\}$ ou $H = A_5$.*

Démonstration : Les classes de conjugaison de A_5 sont de cardinaux respectifs 1 (identité), 20 (3-cycles), 12 et 12 (il y a deux classes de conjugaison de 5-cycles) et 15 (type $(2,2)$). On vérifie à la main qu'aucune somme d'un sous-ensemble de ces cardinaux ne donne un diviseur de 60 autre que 1 ou 60. Par le théorème de Lagrange aucun sous-groupe $\{\mathrm{Id}\} \neq H \subsetneq A_5$ n'est donc une union de classes de conjugaison. Mais un sous-groupe distingué est l'union des classes de conjugaison de ses éléments, donc un tel H ne peut pas être distingué. □

3.5.3 Conséquences de la simplicité du groupe A_n, $n \geq 5$

Définition 3.24 *Un groupe G est dit* simple *si toit sous-groupe distingué est trivial ou G lui même. Autrement dit $H \lhd G$ implique que $H = \{e_G\}$ ou $H = G$.*

On a donc démontré la cas $n = 5$ du résultat suivant. Le cas général sera vu en séance projet plus tard.

Théorème 3.25 *Si $n \geq 5$ alors le groupe alterné A_n est simple.*

On va démontrer ici les conséquences suivantes de ce résultat.

Corollaire 3.26 *Si $n \geq 5$ et $H \triangleleft S_n$ alors $H = \{\mathrm{Id}\}, A_n$ ou S_n.*

Corollaire 3.27 *Si $n \geq 5$, G est un groupe quelconque et $\phi : S_n \to G$ est un morphisme alors on est dans l'un des trois cas suivants :*

i) ϕ est injectif ;

ii) il existe un morphisme $\psi : \{\pm 1\} \to G$ tel que $\phi = \psi \circ \varepsilon$;

iii) ϕ est trivial.

Démonstration : Le second corollaire est une cons'équence immédiate du premier (les cas 3.3.27.i), 3.3.27.ii) et 3.3.27.iii) correspondent respectvement à $\ker(\phi) = \{\mathrm{Id}\}$, A_n et S_n) donc on va montrer celui-ci.

Pour cela on considère $K = H \cap A_n$. On a $K \triangleleft A_n$ et il suit que $K = \{\mathrm{Id}\}$ ou $K = A_n$. Tout sous-groupe contenant A_n est d'indice 1 ou 2 et donc égal à S_n ou A_n respectivement. Il reste donc à montrer que si $K = \{\mathrm{Id}\}$ alors on a aussi $H = \{\mathrm{Id}\}$. Il y a plusieurs façons de montrer ceci, en voici une : soit π le morphisme $\varepsilon|_H$, on a $\ker(\pi) = A_n \cap H = \{\mathrm{Id}\}$. Il suit que π est injectif, donc H est isomorphe à un sous-groupe de $\{\pm 1\}$ et de cardinal 1 ou 2. Il faut montrer que $|H| = 2$ est impossible. Si c'est le cas alors $H = \{\mathrm{Id}, \sigma\}$ où σ est d'ordre 2, et on va montrer qu'il existe $g \in S_n$ tel que $g\sigma g^{-1} \neq g$. Pour ceci on note que la décomposition en cycles de σ ne contient que des 2-cycles. Soit $(a\,b)$ l'un d'entre eux, $c \notin \{a, b\}$ et $g = (b\,c)$, on voit que $g\sigma g^{-1}(a) = c \neq \sigma(a)$ ce qui finit la démonstration (noter que la dernière partie est valable, avec des modifications mineures, pour n'importe quelle σ). □

Chapitre 4

Groupes orthogonaux et sous-groupes

4.1 Groupe orthogonal et spécial orthogonal en toute dimension

On rappelle que $\mathrm{GL}_n(\mathbb{R})$ est l'ensemble des matrices $n \times n$ inversibles (de manière équivalente, de déterminant non nul), qui est un groupe pour la multuplications matricielle. On notera Id la mtrice identité, qui est l'élément neutre de $\mathrm{GL}_n(\mathbb{R})$. On rappelle aussi que si $g = (a_{i,j})_{1 \leq i,j \leq n}$ est une matrice sa *transposée* ${}^t g$ est la matrice $(a_{j,i})_{1 \leq i,j \leq n}$.

Lemme 4.1 *L'ensemble*

$$\mathrm{O}_n(\mathbb{R}) = \{g \in \mathrm{GL}_n(\mathbb{R}) : {}^t g \cdot g = \mathrm{Id}\}$$

est un sous-groupe de $\mathrm{GL}_n(\mathbb{R})$.

Démonstration : On a ${}^t\mathrm{Id} = \mathrm{Id}$ donc ${}^t\mathrm{Id}\,\mathrm{Id} = \mathrm{Id}$ et $\mathrm{Id} \in \mathrm{O}_n(\mathbb{R})$ qui n'est donc pas vide. Si $g, h \in \mathrm{O}_n(\mathbb{R})$ il vient :

$$\begin{aligned} {}^t(gh)(gh) &= {}^t h {}^t g g h \\ &= {}^t h\,\mathrm{Id}\,h = \mathrm{Id} \end{aligned}$$

et donc $gh \in \mathrm{O}_n(\mathbb{R})$. Enfin, on a $g^{-1} = {}^t g$ donc $g = {}^t({}^t g) = {}^t(g^{-1})$ et il vient

$$\left((g^{-1})\right)^{-1} = g = {}^t(g^{-1})$$

donc $g^{-1} \in \mathrm{O}_n(\mathbb{R})$. □

Définition 4.2 *Le sous-groupe* $\mathrm{O}_n(\mathbb{R})$ *est appelé* groupe orthogonal *(en dimension n). Le sous-groupe*

$$\mathrm{SO}_n(\mathbb{R}) = \mathrm{SL}_n(\mathbb{R}) \cap \mathrm{O}_n(\mathbb{R})$$

est appelé groupe spécial orthogonal.

Remarque 4.3 *On peut montrer que* $[O_2(\mathbb{R}) : \mathrm{SO}_2(\mathbb{R})] = 2$.

Interprétation géométrique

Si $u, v \in \mathbb{R}^n$, $u = (u_1, \ldots, u_n)$ et $v = (v_1, \ldots, v_n)$ leur produit scalaire est défini par :

$$\langle u, v\rangle = u_1v_1 + \cdots + u_nv_n.$$

Proposition 4.4 *Soit $g \in \mathrm{GL}_n(\mathbb{R})$. On a $g \in \mathrm{O}_n(\mathbb{R})$ si et seulement si*

$$\forall u, v \in \mathbb{R}^n : \langle g(u), g(v)\rangle = \langle u, v\rangle . \tag{4.1.1}$$

Démonstration : Soit $e_1, \ldots, e_n$ la base canonique de $\mathbb{R}^n$. La propriété (4.1.1) est vérifiée si et seulement si elle est vérifiée pour u, v dans la base. D'autre part si $g = (a_{i,j})$ et ${}^tgg = (b_{i,j})$ on a

$$b_{k,l} = \sum_{j=1}^{n} a_{j,k}a_{j,l} = \langle g(e_k), g(e_l)\rangle$$

donc ${}^tgg = \mathrm{Id}$ si et seulement si $\langle g(e_k, g(e_l)\rangle = 0 = \langle e_k, e_l\rangle$ si $k \neq l$ et $\langle g(e_k), g(e_k)\rangle = 1 = \langle e_k, e_k\rangle$, c'est à-dire que (4.1.1) est vérifiée pour les e_k. □

Remarque 4.5 *i) Il est immédiat de vérifier que l'ensemble des transformations linéaires préservant le produit scalaire (c'est-à-dire vérifiant* (4.1.1)*) forment un sous-groupe, ce qui donne une autre démonstration du fait que $\mathrm{O}_n(\mathbb{R})$ est un sous-groupe.*

ii) Si on pose

$$\|u\| = \sqrt{\langle u, u\rangle}$$

on peut voir que $g \in \mathrm{O}_n(\mathbb{R})$ si et seulement si

$$\forall u \in \mathbb{R}^n : \|g(u)\| = \|u\|. \tag{4.1.2}$$

4.2 Les groupes $\mathrm{O}_2(\mathbb{R})$ et $\mathrm{SO}_2(\mathbb{R})$ et leurs sous-groupes finis

4.2.1 Eléments de $\mathrm{O}_2(\mathbb{R})$

Dans cette section on va donner une paramétrisation par une variable du groupe $\mathrm{O}_2(\mathbb{R})$. Soit :

$$g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{O}_2(\mathbb{R}).$$

On voit que :

$${}^tgg = \begin{pmatrix} a & c \\ b & d \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a^2 + c^2 & ab + cd \\ ab + cd & b^2 + d^2 \end{pmatrix}$$

et on a donc

$$a^2 + c^2 = 1 = b^2 + d^2,\ ab + cd = 0$$

Il suit que :

$$\begin{vmatrix} a & -d \\ c & b \end{vmatrix} = ab + cd = 0$$

et il existe donc $\lambda \in \mathbb{R}$ tel que l'on ait

$$\begin{pmatrix} -d \\ b \end{pmatrix} = \begin{pmatrix} \lambda a \\ \lambda c \end{pmatrix}.$$

On obtient par les deux premières équations que l'on a

$$\lambda^2 = \frac{b^2 + d^2}{a^2 + c^2} = 1$$

et donc $\lambda = \pm 1$. On a ainsi :

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

Comme $a^2 + b^2 = 1$ il existe $\theta \in \mathbb{R}$ tel que $a = \cos(\theta)$ et $b = \sin(\theta)$. On obtient ainsi la paramétrisation :

$$\mathrm{O}_2(\mathbb{R}) = \left\{ \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix} : \theta \in \mathbb{R} \right\} \cup \left\{ \begin{pmatrix} \cos(\theta) & \sin(\theta) \\ \sin(\theta) & -\cos(\theta) \end{pmatrix} : \theta \in \mathbb{R} \right\}. \tag{4.2.1}$$

De plus on voit que

$$\begin{vmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{vmatrix} = \cos(\theta)^2 + \sin(\theta)^2 = 1, \quad \begin{vmatrix} \cos(\theta) & \sin(\theta) \\ \sin(\theta) & -\cos(\theta) \end{vmatrix} = -\cos(\theta)^2 - \sin(\theta)^2 = -1$$

et on a donc

$$\mathrm{SO}_2(\mathbb{R}) = \left\{ \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix} : \theta \in \mathbb{R} \right\}. \tag{4.2.2}$$

Interprétation géométrique

L'élément

$$\rho_\theta = \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix}$$

de $\mathrm{SO}_2(\mathbb{R})$ est appelé *rotation d'angle* θ.[1]

Les éléments de $O_2(\mathbb{R})$ restants sont des symétries par rapport à des droites, aussi appelées *réflexions*. Par exemple :

$$\sigma_0 = \begin{pmatrix} 1 & 0 \\ -1 & 0 \end{pmatrix}$$

est la symétrie par rapport à l'axe des abscisses. En général, on vérifie que :

$$\sigma_\theta = \begin{pmatrix} \cos(\theta) & \sin(\theta) \\ \sin(\theta) & -\cos(\theta) \end{pmatrix}$$

fixe le vecteur

$$v_+ = \begin{pmatrix} \cos(\theta/2) \\ \sin(\theta/2) \end{pmatrix}$$

1. Il devrait y avoir une figure ici.

et renverse le vecteur

$$v_- = \begin{pmatrix} -\sin(\theta/2) \\ \cos(\theta/2) \end{pmatrix}.$$

[2] Autrement dit

$$\sigma_\theta = \rho_{\theta/2}\sigma_0\rho_{-\theta/2} = \rho_{\theta/2}\sigma_0\rho_{\theta/2}^{-1}. \tag{4.2.3}$$

Noter que l'on a aussi

$$\sigma_\theta = \rho_\theta\sigma_0.$$

4.2.2 Structure de $\mathrm{SO}(2)$

Proposition 4.6 *i) Soit π l'application $\mathbb{R} \to \mathrm{SO}_2(\mathbb{R})$ définie par*

$$\pi(\theta) = \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix}.$$

Alors π est un morphisme de groupes surjectif, de noyau $2\pi\mathbb{Z}$. En particulier $\mathrm{SO}_2(\mathbb{R})$ est abélien.

ii) Soit

$$U = \{z \in \mathbb{C} : |z| = 1\}\{e^{i\theta} : \theta \in \mathbb{R}\}.$$

Le groupe $\mathrm{SO}_2(\mathbb{R})$ est isomorphe à U.

Démonstration : La démonstration de 4.4.6.i) est une simple application des formule d'addition pour le cosinus et le sinus : si $\theta, \theta' \in \mathbb{R}$ on a

$$\begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix}\begin{pmatrix} \cos(\theta') & -\sin(\theta') \\ \sin(\theta') & \cos(\theta') \end{pmatrix} = \begin{pmatrix} \cos(\theta)\cos(\theta') - \sin(\theta)\sin(\theta') & -\cos(\theta)\sin(\theta') - \sin(\theta)\cos(\theta') \\ \sin(\theta)\cos(\theta') + \cos(\theta)\sin(\theta') & -\sin(\theta)\sin(\theta') + \cos(\theta)\cos(\theta') \end{pmatrix}$$
$$= \begin{pmatrix} \cos(\theta+\theta') & -\sin(\theta+\theta') \\ \sin(\theta+\theta') & \cos(\theta+\theta') \end{pmatrix}$$

c'est-à-dire que $\pi(\theta)\pi(\theta') = \pi(\theta+\theta')$, donc π est un morphisme de groupes. Il est surjectif à cause de (4.2.2), et le calcul de son noyau est immédiat (on a $\cos(\theta) = 1, \sin(\theta) = 0$ si et seulement si $\theta \equiv 0 \pmod{2\pi}$).

Pour démontrer 4.4.6.ii) on peut montrer directement que $e^{i\theta} \mapsto \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix}$ est un isomorphisme, on va procéder de manière différente (mais équivalente). Soit ϕ l'application $\mathbb{R} \to U$, $\theta \mapsto e^{i\theta}$. C'est un morphisme surjectif par les propriétés de l'exponentielle complexe. De plus $\ker(\phi) = 2\pi\mathbb{Z}$. Pour tout $z \in U$ il existe donc $\theta \in \mathbb{R}$ tel que

$$\phi^{-1}(\{z\}) = \theta + 2\pi\mathbb{Z}.$$

On pose alors

$$\psi(z) = \pi(\theta)$$

qui ne dépend que de z puisque $2\pi\mathbb{Z} \subset \ker(\pi)$ et donc si $\theta' = \theta + 2k\pi$ on a $\pi(\theta') = \pi(2k\pi)\pi(\theta) = \pi(\theta)$. De plus ψ est un morphisme puisque π et ϕ le sont. Enfin, il est surjectif puisque π l'est et injectif vu que $\pi(z) = \mathrm{Id}$ si et seulement si $\phi^{-1}(z) \subset \ker(\pi) = 2\pi\mathbb{Z}$, c'est-à-dire $z = 1$. □

2. Ici aussi.

Remarque 4.7 *Le groupe $O_2(\mathbb{R})$ n'est pas abélien : par exemple* (4.2.3) *indique qu'une symétrie ne commute jamais à une rotation ρ_θ, sauf si $\theta \equiv 0$ ou $\pi \pmod{2\pi}$. On peut en fait montrer que les classes de conjugaison de $O_2(\mathbb{R})$ sont les suivantes :*

- $\{\mathrm{Id}\}$ *et* $\{-\mathrm{Id}\}$ *;*
- $\{\rho_\theta, \rho_{-\theta}\}$ *pour* $\theta \in]0, \pi[\cup]\pi, 2\pi[$
- *toutes les réflexions sont dans la même classe de conjugaison.*

Proposition 4.8 *Soit $n \geq 1$. Les éléments d'ordre n dans $\mathrm{SO}_2(\mathbb{R})$ sont exactement les $\rho_{2k\pi/n}$ pour $1 \leq k \leq n$ tel que $\mathrm{pgcd}(k, n) = 1$.*

Démonstration : D'après le résultat 4.4.6.ii) ci-dessus il suffit de montrer que les éléments d'ordre n dans le groupe U sont les $e^{\frac{2ik\pi}{n}}$ pour $1 \leq k \leq n$ tel que $\mathrm{pgcd}(k, n) = 1$. On sait que les éléments $z \in U$ d'ordre divisant n sont les $e^{2ik\pi/n}$ pour $0 \leq k \leq n$. Soit $1 \leq k \leq n$ et $d = \mathrm{pgcd}(k, n)$. On a $\left(e^{2ik\pi/n}\right)^{n/d} = 1$ et donc si $d > 1$ alors $\left(e^{2ik\pi/n}\right)^{n/d}$ est d'ordre strictement plus petit que n. Réciproquement, si $d = 1$ et il existe $0 < m \leq n$ tel que $\left(e^{2ik\pi/n}\right)^m = 1$ il vient $mk/n \in \mathbb{Z}$ donc $n|mk$ et comme $\mathrm{pgcd}(k, n) = 1$ on a forcément $n|m$, donc $m = n$ et $e^{2ik\pi/n}$ est d'ordre n. □

4.2.3 Sous-groupes finis

Proposition 4.9 *Soit G un sous-groupe fini de $\mathrm{SO}_2(\mathbb{R})$. Alors G est cyclique. De plus, pour toit $n \geq 1$ il existe un unique sous-groupe $C_n \subset \mathrm{SO}_2(\mathbb{R})$ cyclique d'ordre n.*

Démonstration : Soit $G \subset \mathrm{SO}_2(\mathbb{R})$ un sous-groupe fini. Soit H le sous-groupe $\pi^{-1}(G)$ dans $\mathbb{R}$ (où π est la surjection introduite en 4.4.6.i)). On va montrer que H est monogène, d'où il suit immédiatement que G est fini (il est monogène—engendré par $\pi(\theta)$ où $H = \langle\theta\rangle$—et fini).

Pour ce faire on remarque que si $G = \{g_1 = \mathrm{Id}, g_2, \ldots, g_n\}$ et $g_i = \pi(\theta_i)$ alors on a

$$H = 2\pi\mathbb{Z} \cup \{\theta_2 + 2\pi\mathbb{Z}\} \cup \cdots \cup \{\theta_n + 2\pi\mathbb{Z}\}.$$

En particulier, si on a choisi $\theta_i \in [0, 2\pi[$ on a $H \cap [0, 2\pi[= \{0, \theta_2, \ldots, \theta_n\}$. On suppose que tous les θ_i ne sont pas nul (dans le cas contraire on a $H = 2\pi\mathbb{Z}$ et donc $G = \{\mathrm{Id}\}$) il existe donc $2 \leq i \leq n$ tel que

$$\theta := \theta_i = \inf(t \in H, t > 0).$$

On va montrer que $H = \langle\theta\rangle$. Pour ceci soit $\alpha \in H$. Il existe $k \in \mathbb{Z}$ tel que $\alpha \in [k\theta, (k+1)\theta[$. On a aussi $k\theta \in H$ et il suit que $\alpha - k\theta \in H$. Mais on a aussi $\alpha - k\theta \in [0, \theta[$ et par définition de θ il suit que l'on doit avoir $\alpha - k\theta = 0$, donc $\alpha = k\theta \in \langle\theta\rangle$.

Pour démontrer la seconde partie on commence par remarquer que le sous-groupe engendré $\rho_{2\pi/n}$ est cyclique d'ordre n. De plus d'après la proposition 4.8 il contient tous les éléments d'ordre n, donc c'est le seul sous-groupe cyclique d'ordre n. □

Proposition 4.10 *Soit $G \subset \mathrm{O}_2(\mathbb{R})$ un sous-groupe fini. Si G n'est pas contenu dans $\mathrm{SO}_2(\mathbb{R})$ alors il existe $n \geq 2$ tel que $C_n \subset G$ et $[G : C_n] = 2$. De plus tous tels les groupes G sont conjugués l'un à l'autre.*

Démonstration : Soit $H = G \cap \mathrm{SO}_2(\mathbb{R})$. Si $[G : H] = 1$ alors $G = H$ et donc G est contenu dans $\mathrm{SO}_2(\mathbb{R})$. Dans le cas contraire on a $[G : H] = 2$ d'après le lemme général suivant (appliqué à $\Gamma = O_2(\mathbb{R})$, $\Lambda = G$ et $\Delta = \mathrm{SO}_2(\mathbb{R})$).

Lemme 4.11 *Si Γ est un groupe et Δ, Λ sont des sous-groupes alors on a*

$$[\Lambda : \Lambda \cap \Delta] \leq [\Gamma : \Delta].$$

Démonstration : On va montrer que $\Lambda/(\Lambda \cap \Delta)$ s'injecte dans Γ/Δ. Pour ceci on commence par voir que si $\lambda \in \Lambda$ alors on a

$$\lambda(\Lambda \cap \Delta) = (\lambda\Delta) \cap \Lambda. \tag{4.2.4}$$

En effet, il est clair que $\lambda(\Lambda \cap \Delta) \subset (\lambda\Delta) \cap \Lambda$ et on va vérifier l'inclusion réciproque. Si $\lambda' \in \lambda\Delta$ alors il existe $\delta \in \Delta$ tel que $\lambda' = \lambda\delta$. Il vient $\delta = \lambda^{-1}\lambda'$ et si on a de plus $\lambda' \in \Lambda$ il suit que l'on a aussi $\delta \in \Lambda$. Donc $\lambda' \in \lambda(\Delta \cap \Lambda$.

On vérifie maintenant que l'application $\Lambda/(\Lambda \cap \Delta) \to \Gamma/\Delta$ définie par

$$\lambda(\Lambda \cap \Delta) \mapsto \lambda\Delta$$

est injective. En effet, d'après (4.2.4) si $\lambda, \lambda' \in \Lambda$ et $\lambda\Delta = \lambda'\Delta$ alors on a aussi

$$\begin{aligned} \lambda(\Lambda \cap \Delta) &= (\lambda\Delta) \cap \Lambda \\ &= (\lambda'\Delta) \cap \Lambda = \lambda'(\Lambda \cap \Delta) \end{aligned}$$

ce qui termine la démonstration du lemme. □

Il suit donc que $[G : H] = 2$. Il suit que G est de cardinal pair, et si on pose $n = |G|/2$ il suit de la proposition 4.9 que l'on a $H = C_n$. Ceci démontre la première partie de la proposition.

Pour démontrer la seconde partie on commence par remarquer que si $\sigma \in \mathrm{O}_2(\mathbb{R})$ et $\sigma \notin \mathrm{SO}_2(\mathbb{R})$ alors le groupe $G_\sigma = \langle \sigma, C_n \rangle$ est de cardinal $2n$. En effet on a

$$\rho_{2k\pi/n}\sigma = \sigma\rho_{-2k\pi/n}$$

et comme tout élément de G s'écrit sous la forme d'un produit d'éléments de la forme $\rho_{2k\pi/n}$ et σ on peut en fait l'écrire de manière unique sous la forme $\rho_{2l\pi/n}\sigma$ pour un $0 \leq l < n$. On a donc :

$$G_\sigma = \{\mathrm{Id}, \rho_{2\pi/n}, \ldots, \rho_{2(n-1)\pi/n}\} \cup \{\sigma, \sigma\rho_{2\pi/n} \ldots, \sigma\rho_{2(n-1)\pi/n}\}.$$

Réciproquement, tout sous-groupe fini G est de cette forme : en effet, si $\sigma \in G$, $\sigma \notin \mathrm{SO}_2(\mathbb{R})$ alors on a en posant $H = G \cap \mathrm{SO}_2(\mathbb{R})$ que

$$G = H \cup \sigma H$$

vu que $[G : H] = 2$.

Il reste à voir que tous les sous-groupes G_σ sont conjugués l'un à l'autre : c'est le cas car les réflexions le sont d'après la remarque 4.7. □

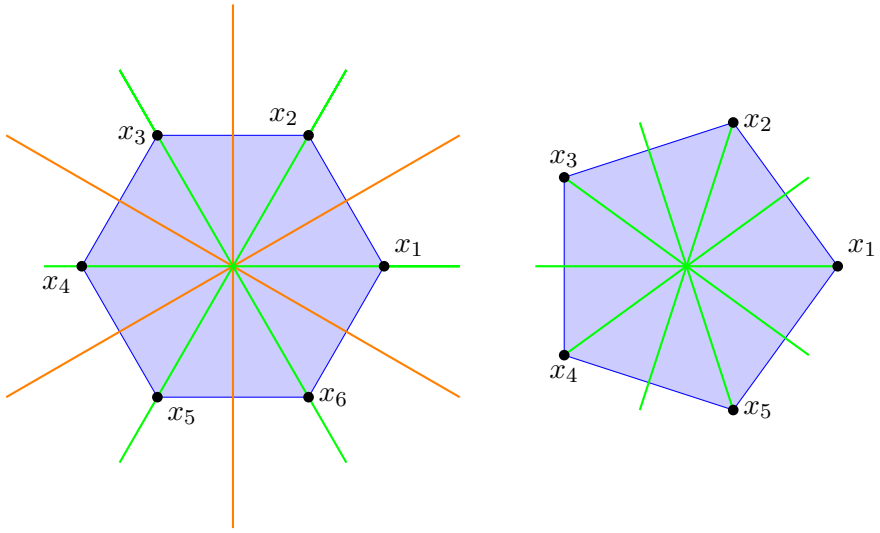
Définition 4.12 *Soit $n \geq 1$. Le groupe $\langle \sigma_0, \rho_{2\pi/n} \rangle$ est appelé* groupe diédral *(d'ordre $2n$) et on le note D_{2n}.*

On a donc montré que les sous-groupes de $\mathrm{O}_2(\mathbb{R})$ sont exactement :

— Les C_n pour $n \geq 1$;

— Les conjugués de D_{2n} pour $n \geq 1$.

Noter que le seul cas où ils sont isomorphes l'un à l'autre est $C_2 \cong \mathbb{Z}/2\mathbb{Z} \cong D_2$ (et que même dans ce cas C_2 et D_2 ne sont pas conjugués dans $O_2(\mathbb{R})$). Les axes des symétries de D_{2n} dans les cas n pair et impair sont illustrés ci-dessous.



4.3 Le groupe $\mathrm{SO}_3(\mathbb{R})$ et ses sous-groupes finis

4.3.1 Eléments de $\mathrm{SO}_3(\mathbb{R})$

Proposition 4.13 *Si $g \in \mathrm{SO}_3(\mathbb{R})$ alors il existe un $v \in \mathbb{R}^3$, $v \neq 0$ tel que $g(v) = v$.*

Démonstration : On admettra cette proposition, une démonstration sera donnée dans le cours d'algèbre linéaire du second semestre (voir aussi l'exercice **??**). □

Proposition 4.14 *Si $\rho \in \mathrm{SO}_3(\mathbb{R})$ alors il existe $g \in \mathrm{SO}_3(\mathbb{R})$ et $\theta \in \mathbb{R}$ tels que*

$$g\rho g^{-1} = \begin{pmatrix} \cos(\theta) & -\sin(\theta) & 0 \\ \sin(\theta) & \cos(\theta) & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Démonstration : Une démonstration complète sera donnée dans le cours du second semestre, on va donner ici les principales idées. Soit v le vecteur donné par la proposition précédente et $e_3 = v/\|v\|$. Alors

$$P = \{u \in \mathbb{R}^3 : \langle u, v\rangle\}$$

est un plan vectoriel de $\mathbb{R}^3$. Soit (e_1, e_2) une base orthonormée de P. On a $\rho(P) = P$: si $u \in P$ on a

$$\langle \rho(u), v\rangle = \langle \rho(u), \rho(v)\rangle = \langle u, v\rangle = 0$$

donc aussi $\rho(u) \in P$. La restriction $\rho|_P^P$ est une isométrie de déterminant 1, et par la description des isométries en dimension 2 donnée dans la sction précédente on a donc

$$\mathrm{Mat}_{(e_1,e_2)}^{(e_1,e_2)}(\rho|_P^P) = \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix}$$

pour un $\theta \in \mathbb{R}$. Si $B = (e_1, e_2, e_3)$ il vient alors

$$\mathrm{Mat}_B^B(\rho) = \begin{pmatrix} \cos(\theta) & -\sin(\theta) & 0 \\ \sin(\theta) & \cos(\theta) & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

ce qui signifie, vu que B est orthonormée, qu'il existe $g \in \mathrm{O}_3(\mathbb{R})$ vérifiant la conclusion de la proposition. En affinant le choix de e_1, e_2 on peut assurer que $g \in \mathrm{SO}_3(\mathbb{R})$. □

4.3.2 Sous-groupes finis

Classification

Théorème 4.15 *Soit $G \subset \mathrm{SO}_3(\mathbb{R})$ un sous-groupe fini. Alors on est dans l'un des cas suivants.*

i) Il existe un vecteur $v \in \mathbb{R}^3 \setminus \{0\}$ tel que

$$\forall g \in G : g(v) = v$$

et G est cyclique.

ii) Il existe un vecteur $v \in \mathbb{R}^3 \setminus \{0\}$ tel que

$$\forall g \in G : g(v) = \pm v$$

et G est diédral.

iii) On a $G \cong A_4$.

iv) On a $G \cong S_4$.

v) On a $G \cong A_5$.

Interprétation géométrique

Dans les deux premiers cas G préserve un prisme dont la base est un n-gone régulier. Dans le cas 4.4.15.i) le n-gone de base peut etre formé en prenant l'orbite de n'importe quel point en-dehors de l'axe commun $\mathbb{R}v$. Dans le cas 4.4.15.ii) les éléments $g \in G$ tels que $gv = -v$ admettent un vecteur fixe $w_g \notin \mathbb{R}v$ et le n-gone de base peut être formé en prenant l'orbite d'un tel w_g.

Dans le cas 4.4.15.iii) G préserve un tétraèdre régulier formé par l'orbite d'un vecteur non-nul fixé par un 3-cycle.

Dans le cas 4.4.15.iv) G préserve un cube formé par l'orbite d'un vecteur non-nul fixé par un 3-cycle. Il préserve aussi l'octaèdre formé par l'orbite d'un vecteur non-nul fixé par un 4-cycle.

Dans le cas 4.4.15.v) G préserve un dodécaèdre formé par l'orbite d'un vecteur non-nul fixé par un 3-cycle. Il préserve aussi un icosaèdre formé par l'orbite d'un vecteur non-nul fixé par un 5-cycle.

Démonstration du théorème

Soit

$$\begin{aligned} X &= \{v \in \mathbb{R}^3 : \|v\| = 1, \exists g \in G, g \neq \mathrm{Id} : g(v) = v\} \\ &= \{v \in \mathbb{R}^3 : \|v\| = 1, \mathrm{Stab}_G(x) \neq \{\mathrm{Id}\}\}. \end{aligned}$$

Alors X est un sous-ensemble fini de $\mathbb{R}^3$ (en effet tout élément de G différent de Id fixe exactement deux vecteurs de norme 1 d'après la proposition 4.14). De plus l'action de G sur $\mathbb{R}^3$ préserve X : en effet, si $g \in G$ et $x \in X$ on a $\|g(x)\| = \|x\|$ vu que $g \in \mathrm{SO}_3(\mathbb{R})$ et de plus on a

$$\mathrm{Stab}_G(g(x)) = g\,\mathrm{Stab}_G(x)g^{-1} \neq \{\mathrm{Id}\}$$

donc $g(x) \in X$.

Soient $O_1, \ldots, O_r$ les orbites de G dans X. Pour $1 \leq i \leq r$ et $x \in O_i$ on note $\nu_i = |\,\mathrm{Stab}_G(x)|$ (qui ne dépend que de i).

Lemme 4.16 *On a*

$$2 - \frac{2}{|G|} = \sum_{i=1}^{r} \left(1 - \frac{1}{\nu_i}\right). \tag{4.3.1}$$

Démonstration : On commence par remarquer que l'on a :

$$\sum_{\substack{g \in G \\ g \neq \mathrm{Id}}} |\,\mathrm{Fix}(g)| = \sum_{x \in X} (|\,\mathrm{Stab}_G(x)| - 1). \tag{4.3.2}$$

En effet les deux côtés sont égaux au cardinal de l'ensemble :

$$\{(g, x) \in G \times X : g \neq \mathrm{Id}, g(x) = x\}.$$

Comme un élément de $\mathrm{SO}_3(\mathbb{R})$ distinct de l'identité a deux vecteurs fixes de norme 1 on voit que $|\,\mathrm{Fix}(g)| = 2$ si $g \in G, g \neq \mathrm{Id}$ et il suit que

$$\sum_{\substack{g \in G \\ g \neq \mathrm{Id}}} |\,\mathrm{Fix}(g)| = 2(|G| - 1). \tag{4.3.3}$$

D'autre part, si $1 \leq i \leq r$ on a $|O_i| \cdot \nu_i = |G|$ et il suit que :

$$\begin{aligned} \sum_{x \in X} (|\,\mathrm{Stab}_G(x)| - 1) &= \sum_{i=1}^{r} \sum_{x \in O_i} (|\,\mathrm{Stab}_G(x)| - 1) \\ &= \sum_{i=1}^{r} |O_i| \cdot (\nu_i - 1) = \sum_{i=1}^{r} |G| \left(1 - \frac{1}{\nu_i}\right). \end{aligned}$$

En remplaçant les deux côtés de (4.3.2) par ce qui est donné ci-dessus et dans (4.3.3) on obtient finalement que

$$2(|G| - 1) = \sum_{i=1}^{r} |G| \left(1 - \frac{1}{\nu_i}\right)$$

et on en déduit la conclusion b=voulue en divisant par $|G|$. □

On va maintenant utiliser ce lemme pour déduire des restrictions sur $|G|$ et les ν_i. Tout d'abord on a $\nu_i \geq 2$ et donc $1 - 1/\nu_i \geq 1/2$, donc il vient

$$r/2 \leq \sum_{i=1}^{r} \left(1 - \frac{1}{\nu_i}\right) = 2 - \frac{2}{|G|} < 2$$

donc $r < 4$. D'autre part si $G \neq \{\mathrm{Id}\}$ on a $2 - 2/|G| \geq 1$ et comme $1 - 1/\nu_i < 1$ il suit que

$$1 \leq 2 - \frac{2}{|G|} = \sum_{i=1}^{r} \left(1 - \frac{1}{\nu_i}\right) < r$$

donc $r > 1$, et on a donc finalement $r = 2$ ou $r = 3$.

Si $r = 2$ alors on a

$$\frac{2}{|G|} = \frac{1}{\nu_1} + \frac{1}{\nu_2}$$

et comme de plus ν_i divise $|G|$ par le théorème de Lagrange on a forcément $\nu_1 = \nu_2 = |G|$ (en effet si $\nu_1 < |G|$ ou $\nu_2 < |G|$ alors $1/\nu_1 + 1/\nu_2 > 1/|G| + 1/|G|$). il suit que $X = \{\pm v\}$ puisque chaque point de X est fixé par tout élément de G. De plus $\mathrm{Stab}_{\mathrm{SO}_3(\mathbb{R})} \cong \mathrm{SO}_2(\mathbb{R})$ et on est donc dans le cas 4.4.15.i).

Si $r = 3$ alors on a

$$\frac{2}{|G|} = \frac{1}{\nu_1} + \frac{1}{\nu_2} + \frac{1}{\nu_3} - 1.$$

On va supposer que $\nu_1 \leq \nu_2 \leq \nu_3$.

Supposons d'abord que $\nu_1 = \nu_2 = 2$. Alors ν_3 peut prendre n'importe quelle valeur et on a

$$\nu_3 = \frac{|G|}{2}$$

et il suit que l'orbite O_3 a deux éléments, qui sont forcément de la forme $\{pmv\}$ pour un $v \in \mathbb{R}^3$, $\|v\| = 1$. On a alors $g(v) = \pm v$ pour tout $g \in G$ et comme l'ensemble des éléments de $\mathrm{SO}_3(\mathbb{R})$ préservant l'ensemble $\{\pm v\}$ est un sous-group isomorphe à $\mathrm{O}_2(\mathbb{R})$ on est dans le cas 4.4.15.ii).

Dans les cas restants on a forcément $\nu_1 = 2, \nu_2 = 3$: en effet on ne peut pas avoir $\nu_1 \geq 3$ car alors il suivrait que :

$$\frac{1}{\nu_1} + \frac{1}{\nu_2} + \frac{1}{\nu_3} - 1 \leq \frac{1}{3} + \frac{1}{3} + \frac{1}{3} - 1 = 0$$

ni $\nu_3 \geq 4$ car on aurait alors :

$$\frac{1}{\nu_1} + \frac{1}{\nu_2} + \frac{1}{\nu_3} - 1 \leq \frac{1}{2} + \frac{1}{4} + \frac{1}{4} - 1 \leq 0$$

ce qui dans les deux cas contredit le fait que $\frac{1}{\nu_1} + \frac{1}{\nu_2} + \frac{1}{\nu_3} - 1 = \frac{2}{|G|} > 0$. On a $1/2 + 1/3 + 1/6 = 1$ et il suit donc par le même raisonnement que l'on a $\nu_3 = 3, 4$ ou 5.

Si $(\nu_1, \nu_2, \nu_3) = (2, 3, 3)$ on voit que $|G| = 12$. Il suit que l'orbite O_2 est de cardinal 4. Le groupe G agit fidèlement sur O_2 (aucun élément ne peut fixer plus de 2 points) et on obtient donc un morphisme injectif

$$\iota : G \to \mathrm{Bij}(O_4) \cong S_4.$$

L'image $\iota(G)$ est un sous-groupe d'indice 2 vu que $|S_4| = 24 = 2|G|$. Un tel sous-groupe est forcément distingué et il suit donc par le corollaire **??** que $\iota(G) = A_4$, donc ι donne un isomorphisme $G \cong A_4$.

Si $(\nu_1, \nu_2, \nu_3) = (2, 3, 4)$ on voit que $|G| = 24$ et que $|O_2| = 8$. De plus O_2 est de la forme

$$\{\pm v_1, \pm v_2, \pm v_3, \pm v_4\}$$

(en effet les points de O_2 sont exactement les points de X stabilisés par un élément d'ordre 3 de G, et si v est un tel point alors $-v$ l'est également). On peut alors définir un morphisme $\iota : G \to S_4$ par la formule

$$g(v_i) = \pm v_{\iota(g)(i)}.$$

On voit que ι est injectif, en effet les v_i ne peuvent pas être deux à deux orthogonaux et ils ne peuvent donc pas tous être fixés par un même élément de $\mathrm{SO}_3(\mathbb{R})$. Comme $|G| = |S_4|$ il suit que ι est un isomorphisme.

Enfin, si $(\nu_1, \nu_2, \nu_3) = (2, 3, 5)$ on voit que $|G| = 60$. On va montrer que les classes de conjugaison de G ont les même cardinaux que celles de A_5 d'où il suit que G est simplé par la même démonstration que pour A_5 ; on concluera en utilisant le résultat qui sera démontré à la fin du cours : *Tout groupe simple d'ordre 60 est isomorphe à* A_5.

Pour ceci on commence par remarquer que tous les éléments d'ordre 2 sont conjugués l'un à l'autre : en effet si $\sigma; \sigma' \in G$ sont d'ordre alors ils stabilisent respectivement des points de $x, x' \in O_1$ (en effet les stabilisateurs d'utres points de x ont des cardinaux impairs). Vu que $\nu_1 = 2$ on a en fait

$$\mathrm{Stab}_G(x) = \{\mathrm{Id}, \sigma\} \text{ et } \mathrm{Stab}_G(x') = \{\mathrm{Id}, \sigma'\}$$

et il suit qu'en prenant $g \in G$ tel que $g(x) = x'$ on a $g\sigma g^{-1} =_s igma'$. Il y a donc une seule classe de conjugaison d'éléments d'ordre 2, contenant $30/2 = 15$ éléments puisque chaque élément d'ordre 2 fixe exactement 2 points de O_1.

De même les éléments d'ordre 3 sont conjugués l'un à l'autre : en effet si $\rho \in G$ est d'ordre 3 et il fixe $x \in X$ alors il fixe aussi $-x$. L'élément $g \in G$ tel que $g(x) = -x$ conjugue alors ρ à son inverse (en effet g einduit une réflexion dans le plan de rotation de ρ). Il suit que deux éléments d'ordre 3 fixant le même plan sont conjugués l'un à l'autre, et par le même argument que ci-dessus on voit que tous les éléments d'ordre 3 de G sont conjugués l'un à l'autre. Il y a $|O_2|/2 \times 2 = |O_2| = 20$ tels éléments.

Enfin, le même argument que ci-dessus appliqué aux éléments d'ordre 5 montre qu"un tel élément ρ est conjugué à ρ^{-1} mais pas à ρ^2 et ρ^3. Il suit qu'il y a deux classes de conjugaison de tels éléments, chacune comptant $|O_3|/2 \times 2| = 12$ tels éléments.

Chapitre 5

Groupes quotients et produits

5.1 Groupes quotients

Etant donnés un groupe G et un sous-groupe H on a défini l'ensemble G/H des classes à gauche de G modulo H. Dans cette section on se pose le problème de définir sur G/H une loi de groupe « naturelle ». Pour ceci on utilise le calcul élémentaire suivant.

Lemme 5.1 *Soit $g \in G$. On a :*

$$\forall g' \in G \, \forall h \in H : g'hgH = g'gH$$

si et seulement si $g^{-1}Hg = H$.

Démonstration : On a

$$g'hg = (g'g)g^{-1}hg$$

et il suit que

$$g'hgH = g'gH \Leftrightarrow (g'g)^{-1}(g'hg) \in H \Leftrightarrow g^{-1}hg \in H$$

et on voit donc que ceci est vrai pour tout $h \in H$ si et seulement si $g^{-1}Hg = H$. □

Proposition 5.2 *Soit G un groupe et H un sous-groupe. Les conditions suivantes sont équivalentes :*

i) Il existe une loi de groupe sur G/H telle que l'application $\pi : G \to G/H$, $g \mapsto gH$ est un morphisme de groupes.

ii) Le sous-groupe H est distingué dans G.

De plus, si ces conditions sont vérifiées alors la loi de groupe sur G/H vérifiant 5.5.2.i) est uniquement déterminée.

Démonstration : Supposons G/H muni d'une loi de groupe $\star$. Si H n'est pas distingué dans G alors il existe $g \in G$ et $h \in H$ tels que $ghg^{-1} \notin H$. Supposons que π soit un morphisme, il vient alors

$$\begin{aligned} \pi(ghg^{-1}) &= \pi(gh) \star \pi(g^{-1}) = ghH \star g^{-1}H \\ &= gH \star g^{-1}H = \pi(gg^{-1}) = \pi(e_G) = H. \end{aligned}$$

Mais on a aussi $\pi(ghg^{-1}) = ghg^{-1}H \neq H$ ce qui donne une contradiction, et il suit que π ne peut pas être un morphisme.

Réciproquement, supposons $H \triangleleft G$. D'après le lemme ci-dessus, si $g, g' \in G$ alors la classe $gg'H$ ne dépend que de gH et $g'H$ et on peut donc définir une loi sur G/H par :

$$(gH) \star (g'H) = gg'H. \tag{5.1.1}$$

On vérifie immédiatement que $\star$ est associative, de neutre $e_G H = H$ et que tout $gH \in G/H$ admet $g^{-1}H$ comme inverse. De plus on a $\pi(gg') = gg'H = (gH) \star (g'H)$ et π est donc un morphisme.

L'unicité de la loi vérifiant 5.5.2.i) suit immédiatement du fait que π est surjective : si $*$ vérifie 5.5.2.i) et $gH, g'H \in G/H$ on a

$$gH * g'H = \pi(g) * \pi(g') = \pi(gg') = gg'H = gH \star g'H$$

donc $* = \star$. □

Définition 5.3 *Soit G un groupe et H un sous-groupe distingué. Le groupe donné par G/H muni de la loi 5.1.1 est appelé* groupe quotient *de G par H.*

Dans la suite, si $H \triangleleft G$ on utilisera implicitement la structure de groupe sur G/H.

Exemple 5.4 *i) Le sous-groupe trivial $\{e_G\} \subset G$ est toujours distingué. LE quotient $G/\{e_G\}$ s'identifie à G (la classe de g est le singleton $\{g\}$) et la loi de groupe est donnée par celle de G.*

ii) Le groupe G est distingué dans lui-même, le quotient G/G n'a qu'un élément et s'identifie donc au groupe trivial.

iii) Soient A, B des groupes et $G = A \times B$. On pose :

$$H = A \times \{e_B\} = \{(a, e_B) : a \in A\}.$$

Le sous-groupe H est distingué dans G (le vérifier) et on peut définir une application $\phi : G/H \to B$ par :

$$\phi((a, b)H) = b$$

qui est alors un isomorphisme de groupe.

Remarque 5.5 *De manière exactement similaire on voit que $H\backslash G$ a une structure de groupe telle que $g \mapsto Hg$ est un morphisme si et seulement si $H \triangleleft G$. Sous cette condition l'application $gH \mapsto Hg$ (qui est bien définie puisque si $H \triangleleft G$ alors les classes à droite et à gauche coïncident) est un isomorphisme de groupes.*

5.2 Factorisation de morphismes

Lemme 5.6 *Soient G, Q des groupes et $\pi : G \to Q$ un morphisme surjectif. Soient G' est un groupe et $\phi : G \to G'$ un morphisme. Les conditions suivantes sont équivalentes :*

i) Il existe un morphisme $\psi : Q \to G'$ tel que $\phi = \psi \circ \pi$.

ii) On a $\ker(\pi) \subset \ker(\phi)$.

De plus le morphisme ψ *donné le cas échéant par 5.5.6.i) est uniquement déterminé.*

Démonstration : S'il existe $\psi : Q \to G'$ tel que $\phi = \psi \circ \pi$ et $g \in \ker(\pi)$ il vient

$$\phi(g) = \psi(\pi(g)) = \psi(e_Q) = e_{G'}$$

donc $g \in \ker(\phi)$ et on a bien $\ker(\pi) \subset \ker(\phi)$.

Réciproquement, supposons que $\ker(\pi) \subset \ker(\phi)$. Soient $q \in Q$ et $g, g' \in \pi^{-1}(\{q\})$. On a alors $g^{-1}g' \in \ker(\pi)$, donc $g^{-1}g' \in \ker(\phi)$ et finalement $\phi(g) = \phi(g')$. On définit une application $\psi : Q \to G'$ en posant

$$\psi(q) = \phi(g) \text{ pour n'importe quel } g \in G \text{ tel que } \pi(g) = q. \tag{5.2.1}$$

On a alors évidemment $\psi(\pi(g)) = \phi(g)$. On vérifie de plus que ψ est un morphisme : en effet si $q_1, q_2 \in Q$ soient $g_1, g_2 \in G$ tels que $\pi(g_i) = q_i$. Il vient $\psi(q_1)\psi(q_2) = \phi(g_1)\phi(g_2)$ et comme $\pi(g_1g_2) = q_1q_2$ on a d'autre part $\psi(q_1q_2) = \phi(g_1g_2)$ d'où il suit finelement que $\psi(q_1q_2) = \psi(q_1)\psi(q_2)$.

L'unicité de ψ est alors immédiate : en effet, pour tout élément dans l'image de π on a forcément (5.2.1) et comme π est surjective ceci détermine $\psi(q)$ pour tout $q \in Q$. □

Remarque 5.7 *Si* π *n'est pas surjective alors il n'est pas garanti qu'un tel* ψ *puisse exister. Par exemple soient* $G = \mathbb{Z}$, $Q = \mathbb{Z}/9\mathbb{Z}$ *avec* π *définie par* $\pi(x) = \overline{3x}$ *(de sorte que* $\mathrm{im}(\pi) = \{\bar{0}, \bar{3}, \bar{6}\}$*) et* $\phi : G \to \mathbb{Z}/3\mathbb{Z}$ *définie par* $\phi(x) = \bar{x}$*. Supposons qu'un* ψ *vérifiant 5.5.6.i) existe, alors il vient :*

$$3\psi(\bar{1}) = \psi(\bar{3}) = \phi(\pi(1)) = \bar{1}$$

mais il n'existe pas de $\bar{x} \in \mathbb{Z}/3\mathbb{Z}$ *tel que* $3\bar{x} = \bar{1}$ *et ceci est donc une contradiction.*

Proposition 5.8 *i) Soient* G *un groupe et* $H \triangleleft G$ *un sous-groupe distingué. Si* $\phi : G \to G'$ *est un morphisme alors il existe un morphisme* $\psi : G/H \to G'$ *tel que* $\psi(gH) = \phi(g)$ *si et seulement si* $H \subset \ker(\phi)$.

ii) Si $\phi : G \to G'$ *est un morphisme alors* $\bar{\phi} : G/\ker(\phi) \to G'$ *donné par 5.5.8.i) est un morphisme injectif. En particulier, si* ϕ *est surjectif alors* $\bar{\phi}$ *est un isomorphisme.*

Démonstration : L'énoncé 5.5.8.i) est une conséquence directe du lemme ci-dessus appliqué au morphisme $\pi : G \to G/H$. Il reste à démontrer l'injectivité de $\bar{\phi}$ pour terminer la démonstration de 5.5.8.ii). Pour ceci on suppose que $\bar{g} = g\ker(\phi) \in G/\ker(\phi)$ vérifie $\bar{\phi}(\bar{g}) = e_{G'}$. Comme $\bar{\phi}$ est défini par (5.2.1) il vient que $\phi(g) = e_{G'}$ donc $g \in \ker(\phi)$ et on a $\bar{g} = \ker(\phi) = e_{G/\ker(\phi)}$. Donc $\ker(\bar{\phi}) = \{e_{G/\ker(\phi)}\}$ et $\bar{\phi}$ est injectif. □

5.3 Produit semi-direct

On a vu que si $G = Q \times H$ alors $G/(\{e_Q\} \times H) \cong Q$. La réciproqie est fausse, comme on le voit par les exemples suivants :

— Si $G = \mathbb{Z}/4\mathbb{Z}$ et $H = \langle \bar{2} \rangle$ alors $G/H \cong \mathbb{Z}/2\mathbb{Z}$ et $H \cong \mathbb{Z}/2\mathbb{Z}$ mais $G \ncong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ (par exemple parce que G a un élément d'ordre 4 mais pas $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$).

— Si $G = S_3$, $H = A_3 \cong \mathbb{Z}/3\mathbb{Z}$ alors $G/H \cong \mathbb{Z}/2\mathbb{Z}$ mais $S_3 \ncong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ parce que S_3 n'est pas abélien.

On va introduire ici une notion plus générale de produit qui s'appliquera au second exemple mais pas au premier.

Produit semi-direct interne

Soit G un groupe. Si $H \triangleleft G$ est un sous-groupe distingué de G et $N \subset G$ est un sous-groupe on dit que G est le produit semi-direct de N et H si on a :

i) $N \cap H = \{e_G\}$;

ii) Pour tout $g \in G$ il existe $h \in H$ et $n \in N$ tels que $g = nh$.

On peut noter la seconde condition comme $G = NH$.

On remarque que si 5.5.8.i) et 5.5.8.ii) sont vérifiées alors si on fixe $g \in G$ la paire $(n, h) \in N \times H$ donnée par la seconde est unique. Il suit que l'application entre ensembles définie par :

$$\delta : N \times H \to G,\ (n, h) \mapsto nh$$

est une bijection. En revanche ce n'est pas un morphisme de groupes si $N \times H$ est muni de la loi produit, comme le montre l'exemple de S_3 examiné ci-dessus. Par contre, si on définit une loi $*$ sur $N \times H$ par :

$$(n_1, h_1) * (n_2, h_2) = (n_1 n_2, n_2^{-1} h_1 n_2 h_2)$$

alors δ est un morphisme de $(N \times H, *)$ dans G. En effet on a alors

$$\begin{aligned} \delta((n_1, h_1) * (n_2, h_2)) &= (n_1 n_2)(n_2^{-1} h_1 n_2 h_2) \\ &= n_1 h_1 n_2 h_2 = \delta(n_1, h_1)\delta(n_2, h_2). \end{aligned}$$

5.3.1 Produit semi-direct

Proposition 5.9 *Soient Q, H des groupes et φ une action à droite par automorphismes de Q sur H, autrement dit φ est une application de Q vers* $\mathrm{Aut}(H)$ *et si $q_1, q_2 \in Q$ alors $\varphi(q_1 q_2) = \varphi(q_2) \circ \varphi(q_1)$.*

La loi définie sur l'ensemble $Q \times H$ par :

$$(q_1, h_1)(q_2, h_2) = (q_1 q_2, \varphi(q_2)(h_1) h_2)$$

est une loi de groupe.

Définition 5.10 *Le groupe donné par $Q \times H$ muni de la loi donnée dans la proposition 5.9 est appelé* produit semi-direct de Q par H (par rapport à φ). *On le note $Q \rtimes_\varphi H$.*

Démonstration : Il est clair que (e_Q, e_H) est un neutre (noter que comme φ définit une action on a bien $\varphi(e_Q) = \mathrm{Id}_H$). On va vérifier l'associativité, et expliciter un inverse pour tout élément. On a :

$$\begin{aligned}((q_1,h_1)(q_2,h_2))\,(q_3,h_3) &= (q_1q_2, \varphi(q_2)(h_1)h_2)(q_3,h_3)\\ &= (q_1q_2q_3, \varphi(q_3)(\varphi(q_2)(h_1)h_2)h_3)\\ &= (q_1q_2q_3, \varphi(q_3)(\varphi(q_2)(h_1))\varphi(q_3)(h_2)h_3)\\ &= (q_1q_2q_3, \varphi(q_2q_3)(h_1)(\varphi(q_3)(h_2)h_3))\\ &= (q_1,h_1)(q_2q_3, \varphi(q_3)(h_2)h_3) = (q_1,h_1)\,((q_2,h_2)(q_3,h_3))\end{aligned}$$

ce qui démontre l'associativité. On va maintenant vérifier que $(q^{-1}, \varphi(q)(h^{-1})$ est un inverse à droite et à gauche pour (q,h). On a :

$$\begin{aligned}(q,h)(q^{-1}, \varphi(q^{-1})(h^{-1})) &= (qq^{-1}, \varphi(q^{-1})(h)\varphi(q^{-1})(h^{-1}))\\ &= (e_Q, \varphi(q^{-1})(hh^{-1}))\\ &= (e_Q, \varphi(q^{-1})(e_H)) = (e_Q, e_H).\end{aligned}$$

De même on a :

$$\begin{aligned}(q^{-1}, \varphi(q^{-1})(h^{-1}))(q,h) &= (q^{-1}q, \varphi(q)(\varphi(q^{-1})(h^{-1}))h)\\ &= (e_Q, \varphi(q^{-1}q)(h^{-1})h)\\ &= (e_Q, h^{-1}h) = (e_Q, e_H)\end{aligned}$$

ce qui termine la démonstration. □

Exemple 5.11 *i) Si φ est trivial (c'est-à-dire $\varphi(q) = \mathrm{Id}_H$ pour tout $q \in Q$) alors on voit que $Q \rtimes_\varphi H$ est le groupe produit.*

ii) On a $S_3 \cong \mathbb{Z}/2\mathbb{Z} \rtimes_\varphi \mathbb{Z}/3\mathbb{Z}$ où $\varphi : \mathbb{Z} : 2\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/3\mathbb{Z})$ est défini par $\varphi(\bar{1})(\bar{k}) = -\bar{k}$. Pour obtenir un isomorphisme on peut poser

$$\delta(\bar{x}, \bar{y}) = (1\,2)^x (1\,2\,3)^y$$

(ceci marche avec n'importe quelle paire (transposition, 3-cycle)).

iii) Le groupe $\mathbb{Z}/2\mathbb{Z} \rtimes_\varphi \mathbb{Z}$ où $\varphi(\bar{1})(k) = -k$ est isomorphe au sous-groupe de $\mathrm{GL}_2(\mathbb{R})$ engendré par les matrices $\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}$ et $\begin{pmatrix}1 & 1\\ 0 & -1\end{pmatrix}$. Un isomorphisme est donné par

$$(\bar{x}, k) \mapsto \begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}^x \left(\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}\begin{pmatrix}1 & 1\\ 0 & -1\end{pmatrix}\right)^k.$$

iv) On a $\mathrm{O}_2(\mathbb{R}) \cong \mathbb{Z}/2\mathbb{Z} \rtimes_\varphi \mathrm{SO}_2(\mathbb{R})$ avec $\varphi(\bar{1})(\rho) = \rho^{-1}$.
On a $\mathrm{O}_3(\mathbb{R}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathrm{SO}_3(\mathbb{R})$ (en envoyant $(\bar{x}, \rho)$ sur $(-1)^x\rho$) mais aussi $\mathrm{O}_3(\mathbb{R}) \cong \mathbb{Z}/2\mathbb{Z} \rtimes_\varphi \mathrm{SO}_3(\mathbb{R})$ où on a posé

$$\varphi(\bar{x})(\rho) = \sigma_0\rho\sigma_0^{-1},\ \sigma_0 = \begin{pmatrix}1 & 0 & 0\\ 0 & 1 & 0\\ 0 & 0 & -1\end{pmatrix}$$

(dans ce cas l'isomorphisme est donné par $(\bar{x}, \rho) \mapsto \sigma_0^x\rho$).

Le dernier exemple montre que l'on peut avoir $Q \rtimes_\varphi H \cong Q \rtimes_\psi H$ sans que $\varphi = \psi$.

Exemple 5.12 *i) Il n'existe pas de φ tel que $\mathbb{Z}/4\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \rtimes_\varphi \mathbb{Z}/2\mathbb{Z}$ (en effet le groupe de droite n'a jamais d'élément d'ordre 4).*

ii) Soit $G = \mathrm{SL}_2(\mathbb{Z})$, $Q = \mathrm{SL}_2(\mathbb{Z}/5\mathbb{Z})$, π le morphisme $G \to H$ obtenu en réduisant les coefficients d'une matrice modulo 5 et $H = \ker(\pi)$. Alors on ne peut jamais avoir $G = Q \rtimes_\phi H$, par exemple parce que G ne contient pas d'élément d'ordre 5.

En général si $G = Q \rtimes_\varphi H$ on a un morphisme $\pi : G \to Q$ défini par $\pi(q, h) = q$. De plus le sous-groupe $Q \times \{e_H\}$ est isomorphe à Q via π. On note que dans les deux non-exemples ci-dessus le fait qu'ils ne soient pas de la forme $Q \rtimes_\varphi H$ vient du fait qu'il existe un élément de Q qui ne se "relève" pas à G.

Proposition 5.13 *Soient G, Q des groupes, $\pi : G \to Q$ un morphisme et $H = \ker(\pi)$. S'il existe un sous-groupe $N \subset G$ tel que $\pi|_N$ soit un isomorphisme de N vers Q alors il existe un φ tel que l'on a $G \cong Q \rtimes_\varphi H$.*

Démonstration : On définit $\varphi : Q \to \mathrm{Aut}(H)$ par :

$$\varphi(q)(h) = n^{-1}hn,\ n = (\pi|_N)^{-1}(q).$$

Ceci vérifie les conditions pour définir un produit semi-direct et l'application $Q \rtimes_\varphi H \to G$, $q \mapsto (\pi|_N)^{-1}(q)h$ est un isomorphisme de groupes. □

Produit semi-direct à gauche

Si au lieu de demander que $\varphi : Q \to \mathrm{Aut}(H)$ vérifie $\varphi(q_1q_2) = \varphi(q_1) \circ \varphi(q_2)$ alors on peut définir une loi de groupe sur $H \times Q$ en posant

$$(h_1, q_1)(h_2, q_2) = (h_1\varphi(q_1)(h_2), q_1q_2)$$

(la vérification est complétement semblable à celle faite ci-dessus). Le groupe obtenu est aussi appelé produit semi-direct de Q par H et on le note $H_\varphi \ltimes Q$. On a un isomorphisme

$$\delta : H_\varphi \ltimes Q \to Q \rtimes_{\varphi'} H$$

où $\varphi'(q) = \varphi(q)^{-1}$, défini par

$$\delta(h, q) = (q^{-1}, h^{-1}).$$

Le critère donné par la proposition 5.13 est aussi valide pour les produits semi-directs à gauche.

Exemple 5.14 *Soient $Q = \mathrm{GL}_2(\mathbb{R})$ et $H = \mathbb{R}^2$. On a $Q \subset \mathrm{Aut}(H)$ et on peut donc définir le produit semi-direct $G = H_{\mathrm{Id}} \ltimes Q$.*

Si $g \in \mathrm{GL}_2(\mathbb{R})$ et $x \in \mathbb{R}^2$ alors en voyant x comme un vecteur colonne la produit matriciel gx est bien défini. Soit $\mathrm{Aff}(\mathbb{R}^2)$ le sous-ensemble des bijections $\mathbb{R}^2 \to \mathbb{R}^2$ de la forme

$$F_{v,g}(x) = v + gx$$

pour $g \in \mathrm{GL}_2(\mathbb{R})$ *et* $v \in \mathbb{R}^2$ *(ce sont bien des bijections car le système linéaire* $y = v + gx$ *a pour unique solution* $x = g^{-1}(y - v)$*). Alors* $\mathrm{Aff}(\mathbb{R}^2)$ *est un sous-groupe et il est isomorphe à* G*. En effet on voit que l'on a :*

$$\begin{aligned} F_{v,g} \circ F_{u,h}(x) &= F_{v,g}(u + hx) \\ &= v + g(u + hx) = (v + gu) + (gh)x \end{aligned}$$

donc $F_{v,g} \circ F_{u,h} = F_{v+gu,gh}$ *et on voit donc que* $(v, g) \mapsto F_{v,g}$ *est un morphisme de groupes* $G \to \mathrm{Bij}(\mathbb{R}^2)$ *d'image* $\mathrm{Aff}(\mathbb{R}^2)$*. Il est injectif, en effet on peut vérifier que* $F_{g,v} = \mathrm{Id}$ *si et seulement si* $g = \mathrm{Id}$ *et* $v = \mathrm{Id}$ *(si* $v \neq 0$ *alors* $v + gv \neq v$ *et si* $v = 0$ *et* $g \neq \mathrm{Id}$ *il existe* $x \in \mathbb{R}^2, x \neq 0$ *tel que* $F_{0,g}(x) = gx \neq x$*).*

Si on voit $x \in \mathbb{R}^2$ *comme un vecteur ligne alors la produit matriciel* xg *est bien défini pour* $g \in \mathrm{GL}_2(\mathbb{R})$*. On peut alors définir pour* $g \in \mathrm{GL}_2(\mathbb{R}), v \in \mathbb{R}^2$ *une bijection :*

$$E_{g,v} : x \mapsto xg + v$$

et on obtient ainsi un morphisme injectif $Q \rtimes_{\mathrm{Id}} H \to \mathrm{Bij}(\mathbb{R}^2)$ *d'image* $\mathrm{Aff}(\mathbb{R}^2)$*.*

Chapitre 6

Structure des groupes finis

6.1 Groupes abéliens

Théorème 6.1 *Soit A un groupe abélien fini. Il existe $r \geq 0$, des nombres premiers $p_1 \leq \ldots \leq p_r$ et des entiers $\alpha_1, \ldots, \alpha_r$ avec $\alpha_i \geq 1$ et si $p_i = p_{i+1}$ alors $\alpha_i \leq \alpha_{i+1}$, tels que*

$$A \cong \frac{\mathbb{Z}}{p_1^{\alpha_1}\mathbb{Z}} \times \cdots \times \frac{\mathbb{Z}}{p_r^{\alpha_r}\mathbb{Z}}.$$

De plus, si $p_1, \ldots, p_r$, $\alpha_1, \ldots, \alpha_r$ et $q_1, \ldots q_s$, $\beta_1, \ldots, \beta_s$ vérifient les conditions ci-dessus alors les groupes $\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z} \times \cdots$ et $\mathbb{Z}/q_1^{\beta_1}\mathbb{Z} \times \cdots$ sont isomorphes si et seulement si $r = s$ et $p_i = q_i$, $\alpha_i = \beta_i$ pour tout $i = 1, \ldots, r$.

Exemple 6.2
i) Le groupe abélien $\mathbb{Z}/6\mathbb{Z}$ est isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ qui est de la forme décrite dans le théorème.

ii) On a observé auparavant que les groupes $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ et $\mathbb{Z}/4\mathbb{Z}$ ne sont pas isomorphes.

iii) De même $\mathbb{Z}/24\mathbb{Z} \times \mathbb{Z}/22\mathbb{Z}$ est isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/11\mathbb{Z}$.

Un cas particulier du théorème, que l'on redémontrera et utilisera dans la démonstration, est le résultat suivant (parfois appelé « théorème des restes chinois »).

Corollaire 6.3 *Soient n, m deux entiers premiers entre eux. Alors on a un isomorphisme*

$$\mathbb{Z}/nm\mathbb{Z} \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}.$$

La démonstration du théorème est assez longue. Elle a essentiellement deux étapes, dont la première est la plus compliquée.

— On commence par démontrer le résultat voulu dans le cas où $|A| = p^\alpha$ pour un p premier (proposition 6.6).

— On en déduit le cas général en utilisant une généralisation (que l'on établira) du corollaire 6.3 : si $|A| = q_1^{\beta_1} \cdots q_u^{\beta_u}$ pour des nombres premiers $q_1 < \cdots < q_u$ (noter que contrairement à l'énoncé du théorème il sont deux à deux distincts) alors on a $A \cong A_1 \times \cdots A_u$ où A_i est un groupe de cardinal $q_i^{\beta_i}$ (proposition 6.9).

6.1.1 Lemmes sur les groupes abéliens

On aura à plusieurs reprises besoin des faits suivants dans la démonstration du théorème 6.1.

Lemme 6.4 *Si A est un groupe abélien fini et m un entier premier à $|A|$ alors l'application $A \to A$ définie par $x \mapsto x^m$ est un automorphisme de A.*

Démonstration : Comme A est abélien $x \mapsto x^m$ est un morphisme. Si $y \in A$, $y \neq e_A$ alors son ordre divise $|A|$ par le théorème de Lagrange et en particulier il est premier à m. Donc $y^m \neq e_A$ et il suit que le noyau de $x \mapsto x^m$ est nul et que cette application est donc injective. Comme A est fini on en déduit finalement que c'est un automorphisme. □

Lemme 6.5 *Si $B \cong \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_r\mathbb{Z}$, A est un groupe abélien et π est un morphisme $A \to B$ tel que pour tout $x \in B$ il existe $\tilde{x} \in A$ tel que $\pi(\tilde{x}) = x$ et $\mathrm{ord}(\tilde{x}) = \mathrm{ord}\, x$ alors $A \cong B \times \ker(\pi)$*

Démonstration : On note x_i un générateur du i-ème facteur, de sorte que x_i est d'ordre n_i. D'après l'hypothèse il existe des $\tilde{x}_i \in A$ tels que $\pi(\tilde{x}_i) = x_i$ et $\mathrm{ord}(\tilde{x}_i) = n_i$. Soit $\widetilde{B}$ le sous-groupe de A engendré par les $\tilde{x}_i$, on va montrer que $\pi|_{\widetilde{B}}$ est un isomorphisme. Pour ceci on note $\eta : B \cong \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_r\mathbb{Z} \to \widetilde{B}$ le morphisme défini par $\eta(x_i) = \tilde{x}_i$. On voit que η est surjectif (son image contient la famille génératrice $(\tilde{x}_i)$ de $\widetilde{B}$) et on a $\pi|_{\widetilde{B}} \circ \eta = \mathrm{Id}_B$ (en effet $\pi|_{\widetilde{B}} \circ \eta(x_i) = x_i$ et les x_i engendrent B). Il suit que η doit être injectif.

Par le critère 5.13 il suit que $A \cong B \rtimes_\varphi \ker(\pi)$ pour un $\varphi : B \to \mathrm{Aut}(\ker(\pi)$. Mais comme A est abélien φ est forcément trivial et il suit que $A \cong B \times \ker(\pi)$. □

6.1.2 Première étape : p-groupes abéliens

Soit p un nombre premier. On dit qu'un groupe fini est un p-groupe s'il est de cardinal p^α pour un $\alpha \geq 1$. On va démontrer ici le cas particulier du théorème où A est un p-groupe.

Proposition 6.6 *Soit p un nombre premier et A un p-groupe abélien. Il existe $\alpha_1 \geq \cdots \geq \alpha_r \geq 1$ tels que*

$$A \cong \mathbb{Z}/p^{\alpha_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{\alpha_r}\mathbb{Z}.$$

Les α_i sont uniquement déterminés par A.

Démonstration : La démonstration se fait par récurrence sur le cardinal de A. Si $|A| = p$ alors A est cyclique. Supposons maintenant que $|A| = p^\alpha$ pour un $\alpha > 1$ et que le résultat est vrai pour tout groupe d'ordre p^β avec $\beta < \alpha$.

Soit $x_1 \in A$ d'ordre maximal, c'est-à-dire que $\mathrm{ord}(x_1) \geq \mathrm{ord}(y)$ pour tout $y \in A$ (un tel x_1 existe car A est fini). On note p^{α_1} l'ordre de x (c'est une puissance de p car il divise $|A| = p^\alpha$ par le théorème de Lagrange). Soient $C = \langle x \rangle$, $B = A/C$ et $\pi : A \to B$ le morphisme quotient. On a $|B| < |A|$ et par l'hypothèse de récurrence il suit que l'on peut supposer que

$$B = \mathbb{Z}/p^{\alpha_2}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{\alpha_r}\mathbb{Z}$$

pour des $\alpha_1 \geq \alpha_2 \geq \cdots \geq \alpha_r \geq 1$. L'élément essentiel de la démonstration est alors le lemme suivant.

Lemme 6.7 *Soit $x \in B$ d'ordre p^β. Il existe $\tilde{x} \in A$ d'ordre p^β tel que $\pi(\tilde{x}) = x$.*

Démonstration : On fixe $1 \leq i \leq r$ et on choisit arbitrairement un $\tilde{z} \in A$ tel que $\pi(\tilde{z}) = x$. On a alors $\pi(\tilde{z}^{p^\beta}) = x^{p^\beta} = e_B$ et il suit que $\tilde{z}^{p^\beta} \in \ker(\pi) = C$. Il existe donc un $k \geq 1$ tek que

$$\tilde{z}^{p^\beta} = x_1^k.$$

On écrit $k = p^\gamma m$ avec $p \not| m$. Par le lemme 6.4 il existe un unique $\tilde{y}$ tel que $\tilde{z} = \tilde{y}^m$ et il suit que

$$\tilde{y}^{p^\beta} = x_1^{p^\gamma}.$$

Si $\gamma = \alpha_1$ on a $\tilde{y}^{p^\beta} = e_A$, donc $\tilde{z}^{p^\beta} = e_A$ et $\tilde{x} = \tilde{z}$ convient.

Si $\beta \leq \gamma < \alpha_1$ alors on a $\gamma - \beta \geq 0$ et il vient

$$\left(\tilde{y} x_1^{-p^{\gamma-\beta}}\right)^{p^\beta} = \tilde{y}^{p^\beta} \left(x_1^{p^\gamma}\right)^{-1} = e_A$$

et on pose alors $\tilde{x} = \left(\tilde{y} x_1^{-p^{\gamma-\beta}}\right)^m$ de sorte que $\pi(\tilde{x}) = x$ et, par le lemme 6.4 $\tilde{x}$ a le même ordre que $\tilde{y} x_1^{-p^{\gamma-\beta}}$, c'est-à-dire p^β.

Enfin, si $\gamma < \beta$ il suit que $\tilde{y}$ est d'ordre $p^\beta p^{\alpha_1 - \gamma}$ et comme

$$\beta + \alpha_1 - \gamma = \alpha_1 + (\beta - \gamma) > \alpha_1$$

ceci contredit le fait que x_1 est d'ordre maximal dans A. Ce cas ne peut donc pas se produire et ceci finit donc la démonstration du lemme. □

D'après la conclusion ci-dessus il est donc possible d'appliquer le lemme 6.5 à $A \to B$ et on obtient donc finalement que

$$A \cong C \times B \cong \mathbb{Z}/p^{\alpha_1}\mathbb{Z} \times \mathbb{Z}/p^{\alpha_2}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{\alpha_r}\mathbb{Z}.$$

Il reste à démontrer l'énoncé d'unicité. Il est plus commode d'utiliser pour ceci une notation légèrement différente de celle de l'énoncé : soit A un p-groupe abélien de la forme

$$A \cong (\mathbb{Z}/p^{a_1}\mathbb{Z})^{b_1} \times \cdots \times (\mathbb{Z}/p^{a_u}\mathbb{Z})^{b_u},$$

avec $a_1 > \cdots > a_r$ et $b_i \geq 1$. On commence par observer que p^{a_1} est l'ordre maximal d'un élément de A et est donc déterminé par la seule structure de groupe sur A. Pour montrer que les a_i, b_i restants sont des invariants d'isomorphisme de A on va utiliser le fait suivant.

Lemme 6.8 *Si D est un groupe abélien et $n \geq 1$ on note $\delta_{n,D}$ le morphisme $D \to D$ défini par*

$$\delta_{n,D}(x) = x^n.$$

Si $E = (\mathbb{Z}/p^a\mathbb{Z})^b$ et $c \geq 0$ on a

$$|\operatorname{im}(\delta_{p^c,E})| = p^{\max(b(a-c),0)}.$$

Démonstration : Si $c \geq a$ alors $\delta_{p^c,E}$ est le morphisme trivial. Si $c < a$ il y a p^{bc} éléments d'ordre divisant p^c dans E donc $|\ker(\delta_{p^c,E})| = p^{bc}$ et il suit que

$$|\operatorname{im}(\delta_{p^c,E})| = |E|/|\ker(\delta_{p^c,E})| = p^{ac}/p^{bc} = p^{b(a-c)}.$$

□

Si $n = p^e$ on note $\log_p(n) = e$. En appliquant le lemme ci-dessus à chacun des facteurs de A on voit que pour $1 \leq l \leq u$ on a :

$$(a_1 - a_l)b_1 + \cdots + (a_{l-1} - a_l)b_{l-1} = \log_p |\operatorname{im}(\delta_{A,p^{a_l}})|,$$
$$(a_1 - a_l + 1)b_1 + \cdots + (a_{l-1} - a_l + 1)b_{l-1} + b_l = \log_p |\operatorname{im}(\delta_{A,p^{a_l-1}})|.$$

Conaissant a_1 et les nombres $\log_p |\operatorname{im}(\delta_{A,p^c})|$ pour $0 \leq c \leq a_1$ on peut donc calculer les a_i, b_i. Comme les permiers sont des invariants de groupe il suit que les seconds le sont aussi. □

6.1.3 Deuxième étape : décomposition d'un groupe abélien en p-groupes

On va démontrer ici le résultat suivant, qui termine la démonstration du théorème 6.1.

Proposition 6.9 *Soit A un groupe abélien fini. Si $p_1, \ldots, p_u$ sont les facteurs premiers distincts de $|A|$ il existe des groupes $A_1, \ldots, A_u$ tels que A_i est un p_i-groupe et $A \cong A_1 \times \cdots \times A_u$.*

Démonstration : On écrit $|A| = p_1^{a_1} \cdots p_u^{a_u}$. On définit un sous-ensemble A_i de A par :

$$A_i = \{x \in A : \exists a \geq 1, x^{p^a} = e_A\}.$$

Alors A_i est un sous-groupe de A : en effet si $x^{p^a} = e_A$ et $y^{p^b} = e_A$ alors en posant $c = \max(a, b)$ on a

$$(xy)^{p^c} = (x^{p^a})^{p^{c-a}}(y^{p^b})^{p^{c-b}} = e_A.$$

On va maintenant utiliser le lemme suivant (un cas particulier du « lemme de Cauchy ») pour montrer que $|A_i| = p^{a_i}$.

Lemme 6.10 *Si B est un groupe abélien et p un nombre premier tel que p divise $|B|$ alors B contient un élément d'ordre p.*

Démonstration : On démontre le résultat par récurrence sur le cardinal de $|B|$. Si $|B| = p^a$ on prend $x \in B$, $x \neq e_B$, par le théorème de Lagrange x est d'ordre p^b pour un $1 \leq b \leq a$ et on voit que $x^{p^{b-1}}$ est d'ordre p.

Si $|B| = p^a n$ avec $p \not| n$ on prend de même $x \in B$, $x \neq e_B$. Soit $m = \operatorname{ord}(x)$. Si $p|m$ alors $x^{m/p}$ est d'ordre p. Sinon on a $m|n$ et on pose $C = \langle x \rangle$, $\overline{B} = B/C$ et π le morphisme quotient $B \to \overline{B}$. On a $|\overline{B}| = p^a(n/m)$ donc par l'hypothèse de récurrence il existe un $\bar{y} \in \overline{B}$ d'ordre p. Soit $y \in B$ tel que $\pi(y) = \bar{y}$, alors $\pi(y^p) = \bar{y}^p = e_{\overline{B}}$ donc $y \in \ker(\pi) = C$ et il existe un $z \in C$ tel que $y^p = z$. Mais comme $p \not| m = |C|$, par le lemme 6.4 il existe un unique $t \in C$ tel que $t^p = z$, et il suit que $(yt^{-1})^p = e_B$. Comme $y \notin \ker(\pi)$ on a $y \neq t$ et il suit que yt^{-1} est d'ordre p. □

Il suit de ce lemme que $|A_i|$ divise $p_i^{a_i}$: en effet, dans le cas contraire il existerait $j \neq i$ tel que p_j divise $|A_i|$, et donc A_i contiendrait un élément d'ordre p_j, ce qui est impossible d'après la définition de A_i.

Le lemme entraîne aussi que p^{a_i} divise $|A_i|$: en effet, si ce n'était pas le cas le groupe abélien A/A_i serait d'ordre divisible par p_i. Il contiendrait donc un élément x d'ordre p_i, et en prenant $\tilde{x} \in A$ tel que $\tilde{x} + A_i = x$ on aurait alors que $\mathrm{ord}(\tilde{x}) = p_i^b k$ pour un $k \geq 1$ premier à p_i et donc $\tilde{x}^k$ serait d'ordre p_i^b. Mais $\tilde{x}^k \notin A_i$ car $\tilde{x}^k + A_i = x^k \neq A_i$, ce qui contredit encore la défintion de A_i.

On a vu que $|A_i| = p^{a_i}$, ceci va suffire à conclure que $A \cong A_1 \times \cdots \times A_u$. On définit un morphisme $\Phi : A_1 \times \cdots \times A_u \to A$ par

$$\Phi(x_1, \ldots, x_u) = x_1 \cdots x_u$$

et on va montrer que Φ est injectif, ce qui suffit pour conclure que Φ est un isomorphisme puisque

$$|A| = p_1^{a_1} \cdots p_u^{a_u} = |A_1| \cdots |A_u| = |A_1 \times \cdots \times A_u|.$$

Soit $(x_1, \ldots, x_u)$ tel que $x_1 \cdots x_u = e_A$. Soit $1 \leq i \leq u$ et soit $m = |A|/p_i^{a_i}$. On a $p_i \not| m$ et il suit par le lemme 6.4 que $x \mapsto x^m$ est un automorphisme de A_i, en particulier si $x_i^m = e_A$ alors $x_i = e_A$. D'autre part si $j \neq i$ on a $p_j^{a_j} | m$ et donc $x_j^m = e_A$, et il suit que :

$$e_A = e_A^m = (x_1 \cdots x_u)^m = x_i^m$$

donc $x_i = e_A$. On a finalement $(x_1, \ldots, x_u) = (e_A, \ldots, e_A)$ et il suit que $\ker(\Phi)$ est trivial, donc Φ est un isomorphisme. □

6.2 Théorèmes de Sylow

Définition 6.11 *Soit p un nombre premier.*

*i) Un groupe H est un p-*groupe *s'il est fini et de cardinal $|H| = p^k$ pour un $k \geq 1$.*

*ii) Si G est un groupe et $H \subset G$ un sous-groupe on dit que H est un p-*sous-groupe *de G si c'est un p-groupe ;*

*iii) Soit G est un groupe fini tel que p divise $|G|$, soit k tel que p^k est la plus grande puissance de p divisant $|G|$. Un sous-groupe $H \subset G$ est un p-*sous-groupe de Sylow *de G si $|H| = p^k$.*

Dans la suitre on abréviera fréquemment « p-sous-groupe de Sylow » en « p-Sylow ».

Exemple 6.12 *i) Si A est un groupe abélien fini et p divise A alors le sous-groupe A_p défini dans la démonstration de la proposition 6.9 est l'unique p-sous-groupe de Sylow de A.*

ii) Si G est un groupe fini et p divise $|G|$ mais pas p^2 alors les p-sous-groupes de Sylow de G sont exactement les sous-groupes cycliques enge,ndrés par les éléments d'ordre p. Par le lemme de Cauchy (Exercice **??***) de tels éléments existent toujours.*

iii) Si $G = S_3$ on a $|G| = 6 = 2 \cdot 3$. L'unique 3-Sylow de G est $\langle (1\,2\,3) \rangle = A_3$. Les 2-Sylow de G sont les sous-groupes engendrés chacun par une transposition (il y en a donc 3).

iv) Si $G = A_4$ on a $|G| = 2^2 \cdot 3$. L'unique 2-Sylow de G est

$$V_4 = \{\mathrm{Id}, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

Les 3-Sylow sont les sous-groupes cycliques engendrés par les 3-cycles, il y en a donc 4 au total.

v) Si $G = S_4$ il y a exactement trois 2-Sylow, qui sont les sous-groupes $\langle \sigma, V_4 \rangle$ ou σ est un 4-cycle. Comme $V_4 \triangleleft S_4$ chacun a la structure $(\mathbb{Z}/2\mathbb{Z}) \rtimes_\varphi V_4$ (où $\varphi(\bar{1})$ est l'unique automorphisme d'ordre 2 de V_4).

Théorème 6.13 (Premier théorème de Sylow) *Soit p un nombre premier. Soit G un groupe fini et p un facteur premier de $|G|$. Il existe un p-sous-groupe de Sylow dans G.*

Démonstration : La démonstration se fait en deux étapes :

i) On construit un p-Sylow explicite dans S_n pour $n \geq p$.

ii) On montre que l'existence d'un p-Sylow « passe aux sous-groupes » et on utilise le fait que pour tout groupe G il existe un sous-groupe $G' \subset S_{|G|}$ isomorphe à G.

Première étape. Soit $n \geq p$, soit $r \geq 1$ le plus grand entier tel que $p^r \leq n$ et soient :

$$a_i = \left\lfloor \frac{n}{p^i} \right\rfloor, \ i = 1, \ldots, r;$$
$$a = a_1 + \cdots + a_r.$$

Alors $n! = p^a m$ où $p \not| m$: en effet pour tout $l \leq r$ il y a exactement $\lfloor n/p^l \rfloor$ entiers divisibles par p^l dans $\{1, \ldots, n\}$. Il faut donc construire un sous-groupe de cardinal p^a dans S_n. La construction est une généralisation de l'exemple $n = 4$ ci dessus 6.6.12.v). Soient $\sigma_1^1, \ldots, \sigma_{a_1}^{(1)}$ des p-cycles dont les supports sont deux à deux disjoints (par exemple $\sigma_1^{(1)} = (1 \ldots p)$, $\sigma_2^{(1)} = (p+1 \ldots 2p)$ etc.). On a alors $\langle \sigma_1, \ldots, \sigma_{a_1} \rangle \cong (\mathbb{Z}/p\mathbb{Z})^{a_1}$. Il existe des éléments $\sigma_1^{(2)}, \ldots, \sigma_{a_2}^{(2)} \in S_n$ d'ordre p tels que $\sigma_i^{(2)} \sigma_j^{(1)} (\sigma_i^{(2)})^{-1} = \sigma_{\tau_i(j)}^{(1)}$ où les τ_i sont des p-cycles à supposrts deux à deux disjoints dans S_{a_1}. On a alors

$$\langle \sigma_1^{(2)}, \ldots, \sigma_{a_2}^{(2)}, \sigma_1^{(1)}, \ldots, \sigma_{a_1}^{(1)} \rangle \cong (\mathbb{Z}/p\mathbb{Z})^{a_2} \rtimes_{\varphi_2} (\mathbb{Z}/p\mathbb{Z})^{a_1}$$

où l'action φ est donnée par $\varphi_2(e_i^{(2)})(e_j^{(1)}) = e_{\tau_i(j)}$, $e_i^{(k)}$ étant les vecteurs de la base caonique de $(\mathbb{Z}/p\mathbb{Z})^{a_k}$. On peut itérer ce procédé, on obtient au final un sous-groupe

$$\langle \sigma_1^{(r)}, \ldots, \sigma_{a_r}^{(r)}, \ldots, \sigma_1^{(1)}, \ldots, \sigma_{a_1}^{(1)} \rangle \cong (\mathbb{Z}/p\mathbb{Z})^{a_r} \rtimes_{\varphi_r} (\cdots \rtimes_{\varphi_2} (\mathbb{Z}/p\mathbb{Z})^{a_1} \cdots)$$

qui a donc le bon cardinal.

Deuxième étape. On va démontrer le lemme suivant.

Lemme 6.14 *Soient $G \subset G'$ des groupes finis, p un nombre premier divisant $|G|$. Soit H' un p-sous-groupe de Sylow de G'. Il existe $g \in G'$ tel que $(gH'g^{-1}) \cap G$ est un p-sous-groupe de Sylow de G, en particulier un tel sous-groupe existe.*

Démonstration : Soient $O_1, \ldots, O_r$ les orbites de G dans G'/H' (où l'action est donnée par $k \cdot (gH') = kgH'$). On a

$$|O_1| + \cdots + |O_r| = |G'/H'| =: m$$

et comme H' est un p-Sylow de G' on sait que m n'est pas divisible par p. Il existe donc au moins un i tel que $|O_i|$ ne soit pas divisible par p. D'autre part si $1 \leq j \leq r$ et le stabilisateur H_j dans G d'un point de O_i n'est pas un p-Sylow de G alors $|O_i| = |G/H_j|$ est divisible par p. Donc H_i est un

p-Sylow de G. On observe d'utre part que si gH' est un point de O_i on a $\mathrm{Stab}_{G'}(gH') = gH'g^{-1}$ donc $H_i = (gH'g^{-1}) \cap G$. □

Soientt finalement $n = |G|$ et ϕ le morphisme injectif $G \to S_n$ défini par l'action de G sur lui-même par translation. Par la première partie et le lemme ci-dessus il existe un p-Sylow de $\phi(G)$ et sa préimage âr ϕ est un p-Sylow de G. □

Théorème 6.15 (Second théorème de Sylow) *Soient G un groupe fini et p un facteur premier de $|G|$.*

i) Si H est un p-sous-groupe de G alors il existe un p-sous-groupe de Sylow H' de G tel que $H \subset H'$.

ii) Si H_1, H_2 sont des p-sous-groupes de Sylow de G il existe $g \in G$ tel que $H_2 = gH_1g^{-1}$.

iii) Si k est le nombre exact de p-sous-groupes de Sylow de G alors $p = 1 \pmod p$.

Remarque 6.16
— *Le point 6.6.15.i) montre que les p-Sylow sont maximaux parmi les p-sous-groupes.*
— *Le point 6.6.15.iii) est un renforcement de l'énoncé du premier théorème de Sylow, mais on va utiliser ce dernier dans sa démonstration.*

Démonstration : La démonstration des deux premiers points se fait de concours, on va en fait montrer l'énoncé suivant :

$$\textit{Si } H \textit{ est un } p\textit{-sous-groupe et } H' \textit{ un } p\textit{-Sylow il existe } g \in G \textit{ tel que } H \subset gH'g^{-1}$$

qui implique directement 6.6.15.i), et implique 6.6.15.ii) en l'appliquant à $H = H_2$ et $H' = H_1$ puisque H_2 et gH_1g^{-1} ont le même cardinal. Les arguments ressemblent à ceux utilisés plus haut. L'énoncé suivant sera utile également pour la démonstration du troisième point.

Lemme 6.17 *Soit K un p-groupe agissant sur un ensemble fini X et X^K l'ensemble des points fixes de l'action :*

$$X^K = \{x \in X : \forall k \in K\ k \cdot x = x\}.$$

On a $|X^K| = |X| \pmod p$.

Démonstration : Si O est une orbite non-réduite à un point fixe on a $|O| = |G|/|H|$ pour un sous-groupe $H \subsetneq G$, donc p divise $|O|$ puisque G est un p-groupe. L'ensemble de ces orbites est exactement $X \setminus X^k$ et on voit donc que p divise $|X \setminus X^k| = |X| - |X^K|$. □

Soient maintenant H un p-sous-groupe et H' un p-Sylow dans G. On cosidère l'action de H sur G/H'. Comme H est un p-groupe le nombre de points fixes est congru à $|G/H'|$ modulo p par le lemme ci-dessus, et comme H' est un p-Sylow p ne divise pas $|G/H'|$. Il suit que le nombre de points fixes est $\neq 0 \pmod p$, en particulier il est non nul et il existe des points fixes. Si gH' est fixé par H on voit que $H \subset gH'g^{-1}$, ce qui finit la démonstration des deux premiers points.

Pour le troisième point on fixe un p-Sylow H_0 dans G et on considère l'action de H_0 sur l'ensemble X des p-Sylow de G. On va démontrer que si H est un p-Sylow et H_0 normalise H alors $H = H_0$. Ceci implique le résultat voulu : en effet une formulation équivalente est que H_0 est le seul

p-Sylow de G fixé par l'action par conjugaison de H_0 dans X, et le lemme ci-dessus donne alors que $|X| = 1 \pmod p$.

Soit donc H un p-Sylow de G, et on suppose que $\forall h \in H_0$, $hHh^{-1} = H$. Soit K le sous-groupe engendré par H_0, H. Alors K est un p-sous-groupe : en effet, comme H_0 normalise H l'application

$$H_0 \rtimes_\varphi H \to K,\ (h, h') \mapsto hh'$$

(où φ est l'action $h \cdot h' = h^{-1}h'h$) est un morphisme de groupes surjectif, donc le cardinal de K divise celui de $H_0 \rtimes_\varphi H$ qui est une puissance de p. Mais comme H_0 est un p-Sylow on a alors forcément $|K| = |H_0|$ donc $K = H_0$ et enfin $H \subset H_0$ donc $H = H_0$ puisque les deux sont des p-Sylow. □

Exemple 6.18 *Si $G = \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ alors $|G| = p(p-1)(p+1)$ donc p est la plus grande puissance de p divisant $|G|$. La matrice*

$$u = \begin{pmatrix} \bar{1} & \bar{1} \\ \bar{0} & \bar{1} \end{pmatrix}$$

est d'ordre p dans G et engendre donc un p-Sylow $H_0 = \langle u \rangle$. Par le point 6.6.15.ii) du théorème tous les p-Sylow de G sont conjugués à H_0. On remarque que dans l'action de G sur $V = (\mathbb{Z}/p\mathbb{Z})^2$ le sous-groupe H_0 est le stabilisateur de $v_0 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$. Comme tous les p-Sylow sont conuugués et que l'action est transitive sur $V \setminus \{0\}$ on voit que les p-Sylow de G sont exactement les stabilisateurs de vecteurs non-nuls de V. On a $\mathrm{Stab}_G(v) = \mathrm{Stab}_G(w)$ si et seulement s'il existe $\lambda \in (\mathbb{Z}/p\mathbb{Z})^\times$ tel que $w = \lambda v$ et il suit qu'il y a donc au total

$$(|V| - 1)/(\mathbb{Z}/p\mathbb{Z})^\times = (p^2 - 1)/(p - 1) = p + 1$$

p-sous-groupes de Sylow dans G. On peut voir que ce sont les sous-groupes de la forme :

$$H_a = \left\{ \begin{pmatrix} 1 + \lambda a & -\lambda \\ \lambda a^2 & 1 - \lambda a \end{pmatrix} : \lambda \in \mathbb{Z}/p\mathbb{Z} \right\}$$

pour $a \in \mathbb{Z}/p\mathbb{Z}$, ainsi que le sous-groupe

$$U_\infty = \left\{ \begin{pmatrix} 1 & 0 \\ \lambda & 1 \end{pmatrix} : \lambda \in \mathbb{Z}/p\mathbb{Z} \right\}.$$

6.3 Applications des théorèmes de Sylow

Les points 6.6.15.ii) et 6.6.15.iii) du second théorème de Sylow permettent souvent de déterminer les possibilités pour le nombre de p-Sylow d'un groupe dont on ne connaît que le cardinal. Une exemple d'application de ce principe est le théorème suivant.

Théorème 6.19 *Soit G un groupe d'ordre 60. Si G est simple alors G est isomorphe à A_5.*

Démonstration : Soit X l'ensemble des 5-Sylow de G. Par le point 6.6.15.ii) du second théorème de Sylow G agit transitivement sur X. Comme le stabilisateur d'un point de cette action contient un 5-Sylow (lui-même) on voit que $|X|$ divise $60/5 = 12$. D'autre part on a $|X| = 1 \pmod 5$ par

le point 6.6.15.iii). Il suit que $|X| = 1$ ou $|X| = 6$. Comme G est simple on a $|X| = 6$. On obtient donc une action non-triviale de G sur un ensemble de cardinal 6, donc un morphisme non-trivial $\phi : G \to S_6$, qui doit être injectif puisque G est simple.

L'image de ϕ doit être contenue dans A_6 : en effet on a $\phi(G) \cap A_6 \neq \{e_G\}$ car $|\phi(G)| = 60 > |S_6/A_6|$ et comme $\phi^{-1}(G \cap A_6)$ est distingué dans G (car A_6 l'est dans S_6) il doit être égal à G, c'est-à-dire que $\phi(G) \subset A_6$.

On considère maintenant l'action de $\phi(G)$ sur $Y = A_6/\phi(G)$. On a $Y = 360/60 = 6$; d'autre part $\phi(G)$ fixe la classe $\mathrm{Id} \cdot \phi(G)$ et l'action sur $Y' = Y \setminus \{\mathrm{Id} \cdot \phi(G)\}$ est fidèle : en effet elle n'est pas triviale car $\phi(G) \not\lhd A_6$ (A_6 est simple) donc il existe $\sigma \in A_6$ tel que $\phi(G) \neq \sigma\phi(G)\sigma^{-1} = \mathrm{Stab}_{A_6}(g\phi(G)$, et elle est donc fidèle car G est simple. Elle doit alors être transitive car s'il existait une orbite de cardinal $k \leq 4$ on aurait un morphisme injectif $G \to S_k$ ce qui est impossible car $|G| > 24 = S_4$.

Comme $|Y'| = 5$ on obtient donc un morphisme injectif $\psi : \phi(G) \to S_5$. L'image est d'indice 2 donc doit être égale à A_5, et par égalité des cardinaux il suit que $\psi(\phi(G)) = A_5$. On conclut que $\psi \circ \phi$ est un isomorphisme $G \to A_5$. □