Structures Algébriques

Théorie des groupes

Cours Euler 4ème année

Ce cours de structures algébriques reprend les bases de la théorie des groupes et les approfondit. Nous allons reprendre les notions de groupes, découvrir celles de sous-groupes normaux et de quotients, qui permettent de décomposer un groupe en sous "parties". Nous verrons beaucoup d'exemples de groupes qui apparaissent naturellement en mathématiques, mais aussi dans d'autres domaines scientifiques. Nous discuterons la classification des groupes et étudierons les petits groupes. Nous apprendrons ce qu'est une action de groupe, une notion importante tant sur le plan algébrique que pour des outils plus géométriques.
Il s'agit peut-être du premier cours ne contenant presque que des notions algébriques et "abstraites". Le but est de se familiariser avec les méthodes et les preuves qui ne reposent que sur des axiomes (comme ceux d'un groupe par exemple). Même si nos exemples principaux dans ce cours seront des groupes, les méthodes de réflexion et de preuves que vous allez acquérir seront utiles pour le reste de vos études.

Chapitre 1

Groupes et homomorphismes

Pour commencer ce cours, nous allons tout d'abord revoir quelques notions de base sur les relations d'équivalence, qui nous seront utiles pendant les semaines qui suivent. Nous reprendrons ensuite certaines notions de base de théorie des groupes ainsi que des exemples fondamentaux de groupes.

1.1 Relation d'équivalence

Définition 1.1.1 (Rappel)**.**

Une relation d'équivalence $\sim$ *sur un ensemble* E *est une relation*

(i) *réflexive :* $x \sim x, \forall x \in E$ *;*

(ii) *symétrique : si* $x \sim y$ *alors* $y \sim x, \forall x, y \in E$ *;*

(iii) *transitive :* $x \sim y$ *et* $y \sim z$*, implique* $x \sim z$*,* $\forall x, y, z \in E$*.*

Si $x \in E$*, la* classe d'équivalence *de* x *est l'ensemble des éléments équivalents à* x*, c'est-à-dire*

$$[x] = \{y \in E \mid x \sim y\}.$$

La proposition suivante décrit comment un ensemble peut être découpé en parties disjointes : les classes d'équivalence.

Proposition 1.1.2 (Rappel)**.** *Soit* E *un ensemble et* $\sim$ *une relation d'équivalence sur* E*. Alors, l'ensemble des classes d'équivalence (l'ensemble quotient) forme une partition de* E*. C'est-à-dire, si* $[x] \cap [y] \neq \emptyset$ *alors* $[x] = [y]$*.*

Exemple 1.1.3. *Soit $n \in \mathbb{Z}$, on dit que $a, b \in \mathbb{Z}$ sont* congrus modulo n *si n divise leur différence : $n|(b-a)$. La congruence est une relation d'équivalence (Exercice). Combien y-a-t'il de classes d'équivalence pour cette relation ?*

Il y en a n : les classes d'équivalence sont $[0], ..., [n-1]$. Par exemple, pour $n = 6$, la classe de 0 correspond à tous les multiples de 6, la classe de 1 les multiples de 6 auxquels on ajoute 1, etc.

1.2 Groupes et homomorphismes

Nous commençons par rappeler les définitions de base de théorie des groupes ainsi que quelques propriétés qui découlent directement de la définition.

Définition 1.2.1 (Rappel)**.** *Un* groupe $(G, \star)$ *est un ensemble G muni d'une loi de composition $\star : G \times G \to G$ vérifiant les propriétés suivantes :*

Associativité *Pour tout $g, h, k \in G$, $(g \star h) \star k = g \star (h \star k)$.*

Élément neutre *Il existe $1_G \in G$ tel que pour tout $g \in G, 1_G \star g = g \star 1_G = g$. On note parfois l'élément neutre e, Id ou encore I.*

Inverses *Pour tout $g \in G$, il existe $g^{-1} \in G$ tel que $g \star g^{-1} = g^{-1} \star g = 1_G$.*

L'ordre *d'un groupe G, ou sa* cardinalité *est son nombre d'élément (et peut être infini), dénoté $|G|$. Un groupe est dit* abélien*, ou* commutatif*, si tous les éléments du groupe commutent, c'est-à-dire $gh = hg$ pour tout $g, h \in G$.*

Remarque 1.2.2.

1. *L'associativité permet d'omettre les parenthèses.*
2. *L'élément neutre est unique. En effet, si e est aussi un élément neutre, alors on a*
$$1_G = 1_G \star e = e.$$
Cela justifie la notation qui associe a un groupe son unique élément neutre.
3. *L'inverse d'un élément G est unique. En effet, si g' est aussi un inverse de g, alors on a*
$$g' = g' \star (g \star g^{-1}) = (g' \star g) \star g^{-1} = g^{-1}.$$
Cela justifie la notation, qui à un élément du groupe g, associe son unique inverse g^{-1}.
4. $(g \star h)^{-1} = h^{-1} \star g^{-1}$.

5. *Si $g, h, k \in G$, l'équation $h = k$ est équivalente à l'équation $g \star h = g \star k$.*
6. *Lorsqu'il n'y a pas d'ambiguïté sur la loi de composition, on se permet d'écrire gh pour $g \star h$ et G pour le groupe $(G, \star)$, ou $g + h$, si le groupe est abélien.*

Les exemples suivants sont importants pour le reste du cours : ces groupes reviennent dans beaucoup de domaines mathématiques, dont certains que nous mentionnerons au fur et à mesure de ce cours.

Exemples 1.2.3.

1. *$(\mathbb{Z}, +)$ est un groupe, il est abélien et d'ordre infini.*
2. *Soit V un espace vectoriel. Alors, $(V, +)$ forme un groupe abélien.*
3. *Soit K un corps. Alors, $(K \setminus \{0\}, \cdot)$ forme un groupe abélien.*
4. *(Fondamental) Soit X un ensemble. On note*

$$\mathrm{Bij}(X) = \{f : X \to X | \, f \text{ est une fonction bijective}\},$$

l'ensemble des bijections de $X \to X$. Alors, $(\mathrm{Bij}(X), \circ)$ est un groupe, où $\circ$ est la composition usuelle de fonctions. Il n'est pas abélien, sauf si $|X| = 1, 2$. Si $X = \{1, ..., n\}$, il s'agit du groupe S_n.

5. *Soit V un espace vectoriel. On note*

$$\mathrm{GL}(V) = \{T : V \to V | \, T \text{ est une application linéaire bijective}\},$$

l'ensemble des applications linéaires bijectives $V \to V$. Alors, $(\mathrm{GL}(V), \circ)$ est un groupe non abélien si $\dim V \geq 2$.

6. *Soit K un corps et n un entier. On note*

$$\mathrm{GL}_n(K) = \{M | \, M \text{ est une matrice } n \times n \text{ inversible à coefficients dans } K\}.$$

Alors, $(\mathrm{GL}_n(K), \cdot)$ est un groupe, où $\cdot$ est la multiplication usuelle de matrices.

La notion de fonction entre des ensembles satisfaisant une notion de "conservation" de certaines propriétés est fondamentale en mathématique. L'un des premiers exemples que vous avez pu rencontrer est la notion d'application linéaire entre des espaces vectoriels. Une application linéaire conserve la structure d'espace vectoriel et la "transfère" à l'espace d'arrivée. Un homomorphisme de groupe satisfait le même genre de propriété : son but est de conserver la structure de groupe.

Définition 1.2.4. *Soient* $(G, \star)$ *et* $(H, \circ)$ *des groupes. Un* homomorphisme de groupe $\phi : (G, \star) \to (H, \circ)$ *est une application telle que pour tout* $g, g' \in G$,

$$\phi(g \star g') = \phi(g) \circ \phi(g').$$

Un homomorphisme de groupe bijectif est nommé un isomorphisme. *Deux groupes* G, H *sont dits* isomorphes *s'il existe un isomorphisme* $G \to H$.

Deux groupes isomorphes sont considérés comme "les mêmes", dans le sens où leur structure est exactement la même. L'isomorphisme n'est qu'une façon de renommer les éléments, qui satisfont exactement les mêmes propriétés. C'est la base de la classification des groupe : on ne souhaite pas décrire *tous* les groupes, mais toutes les *structures* de groupes possibles. On parle donc de classification *à isomorphisme près*. Nous verrons des exemples en exercice.

Remarque 1.2.5.

1. *Si* $\phi : G \to H$ *et* $\psi : H \to K$ *sont des homomorphismes de groupe, la composée* $\psi \circ \phi : G \to K$ *l'est aussi.*
   En effet, pour $g, g' \in G$

   $$(\psi \circ \phi)(g \cdot g') = \psi(\phi(g) * \phi(g')) = (\psi \circ \phi(g)) \cdot (\psi \circ \phi(g')).$$

2. *Si* $\phi : G \to H$ *est un homomorphisme de groupe,* $\phi(1_G) = 1_H$.
   En effet,

   $$\phi(1_G) = \phi(1_G \cdot 1_G) = \phi(1_G) \cdot \phi(1_G),$$

   et donc $\phi(1_G) = 1_H$.
3. *Si* $\phi : G \to H$ *est un homomorphisme de groupe,* $\phi(g^{-1}) = \phi(g)^{-1}$.
   En effet, pour tout $g \in G$,

   $$\phi(g) \cdot \phi(g^{-1}) = \phi(g \cdot g^{-1}) = \phi(1_G) = 1_H,$$

   et donc, $\phi(g^{-1}) = \phi(g)^{-1}$.
4. *Si* $\phi : G \to H$ *est un isomorphisme, son inverse* $\phi^{-1} : H \to G$ *l'est aussi.*
   Soient $h_1, h_2 \in H$, *alors il existe* $g_1, g_2 \in G$ *tels que* $\phi(g_i) = h_i$ *pour* $i = 1, 2$.
   Alors

$$\begin{aligned}\phi^{-1}(h \cdot h') &= \phi^{-1}(\phi(g) \cdot \phi(g')) \\ &= g \cdot g' \\ &= \phi^{-1}(\phi(g)) \cdot \phi^{-1}(\phi(g')) \\ &= \phi^{-1}(h) \cdot \phi^{-1}(h').\end{aligned}$$

5. *Si $\phi : G \to H$ et $\psi : H \to K$ sont des isomorphismes de groupe, la composition $\psi \circ \phi : G \to K$ l'est aussi.*

Exemples 1.2.6.

1. *Soit V un $\mathbb{K}$-espace vectoriel de dimension n sur $\mathbb{K}$ un corps. Alors $GL(V)$ est isomorphe à $GL_n(\mathbb{K})$ (Exercice). (Il s'agit des exemples 5 et 6 des Exemples 1.2.3).*
2. *Soient V, W des espaces vectoriels et $T : V \to W$ une application linéaire. Alors T est en particulier un homomorphisme de groupe $T : (V, +) \to (W, +)$. Une application linéaire préserve donc plus de structure qu'un homomorphisme de groupe (la multiplication par scalaire).*
3. *Soit K un corps et n un entier. L'application*

$$\det : (GL_n(K), \cdot) \to (K \setminus \{0\}, \cdot)$$

est un homomorphisme de groupe.

4. *Soit S_n le groupe des permutations sur n éléments. Alors l'application de signature*

$$\text{sign} : S_n \to (\{-1, 1\}, \cdot)$$

est un homomorphisme de groupe.

Une notion importante dans un groupe est celle de conjugaison d'un élément par un autre. Pour $g, h \in G$ la *conjugaison* de g par h est définie par hgh^{-1}.

1.3 Sous-groupes

A nouveau, nous rappelons les définitions de base de sous-groupes.

Définition 1.3.1. *Soit $(G, \star)$ un groupe. Un sous-ensemble H de G est un sous-groupe de G si $\star$ se restreint en une loi de composition*

$$\star : H \times H \to H$$

qui munit H d'une structure de groupe.

L'ordre d'un sous-groupe divise toujours l'ordre du groupe. Nous verrons une preuve de ce résultat dans le chapitre suivant. La proposition suivante donne une manière plus simple de vérifier si un sous-ensemble est un sous-groupe.

Proposition 1.3.2 (Rappel)**.** *Soit $(G, \star)$ un groupe. Un sous-ensemble $H \subseteq G$ est un* sous-groupe *de G si et seulement si*

(i) $H \neq \emptyset$,

(ii) $\forall h, h' \in H, h \star (h')^{-1} \in H$.

Une autre condition nécessaire et suffisante pour que H soit un sous-groupe de G est que l'inclusion $H \hookrightarrow G$ définisse un homomorphisme de groupes.

Pour construire un nouveau groupe à partir de plusieurs groupes, on peut considérer leur produit :

Définition 1.3.3. *Soient $(G, \star)$ et $(H, *)$ deux groupes. On définit le* produit direct *de G et H, noté $G \times H$, par*

$$G \times H = \{(g, h) \mid g \in G \text{ et } h \in H\},$$

muni de l'opération $(g_1, h_1) \cdot (g_2, h_2) = (g_1 \star g_2, h_1 * h_2)$ pour tout $g_1, g_2 \in G$ et $h_1, h_2 \in H$.

On vérifie facilement que c'est un groupe (exercice).

Comme pour les applications linéaires, le noyau et l'image d'homomorphismes de groupe sont des notions très importantes. Nous verrons un de leurs intérêts dans le chapitre suivant.

Définition 1.3.4. *Soit $f : G \to H$ un homomorphisme de groupe. Le noyau de f est l'ensemble*

$$\mathrm{Ker}(f) = \{g \in G \mid f(g) = 1_H\}.$$

L'image de f est l'ensemble

$$\mathrm{Im}(f) = \{h \in H \mid \exists g \in G \text{ avec } f(g) = h\}.$$

Proposition 1.3.5. *Soit $f : G \to H$ un homomorphisme de groupe. Alors* $\mathrm{Ker}(f)$ *et* $\mathrm{Im}(f)$ *sont des sous-groupes respectivement de G et H.*

Démonstration. Exercice. □

Proposition 1.3.6. *Soit $f : G \to H$ un homomorphisme de groupe. Alors f est injective si et seulement si* $\mathrm{Ker}(f) = \{1_G\}$.

Démonstration. Supposons que f est injective, et soit $g \in \mathrm{Ker}(f)$.
Alors, $f(g) = 1_H = f(1_G)$ et donc $g = 1_G$.

Supposons maintenant que $\mathrm{Ker}(f) = \{1_G\}$ et soient $g, g' \in G$. Alors, si $f(g) = f(g')$,

$$f(gg'^{-1}) = f(g)f(g')^{-1} = f(g)f(g)^{-1} = 1_H,$$

et donc $gg'^{-1} = 1_G$. Ceci implique que $g = g'$. □

Il existe plusieurs manières de classifier les groupes selon leurs propriétés. Trouver de nouvelles propriétés pour la classification des groupes est une branche active de recherche en mathématiques. Nous allons présenter l'un des outils les plus basiques pour différencier des groupes. Nous verrons un peu dans ce chapitre, puis plus tard dans le cours, l'utilité de ces notions.

Définition 1.3.7. *Soit G un groupe et $g \in G$. On définit* l'ordre *de g comme le plus petit entier $n \neq 0$ tel que $g^n = g \cdot ...g = e$. L'ensemble $\langle g \rangle = \{g^n \mid n \in \mathbb{Z}\}$ est un sous-groupe de G appelé le* sous-groupe engendré par g. *Un groupe G est dit* cyclique *s'il existe un élément g (pas forcément unique !) tel que $G = \langle g \rangle$. On note généralement un groupe cyclique à n éléments C_n.*

1.4 Le groupe $\mathbb{Z}/n\mathbb{Z}$

Dans cette partie, nous allons discuter un peu d'un groupe cyclique important, $\mathbb{Z}/n\mathbb{Z}$ aussi dénoté $\mathbb{Z}_n$ ou C_n. La notation $\mathbb{Z}/n\mathbb{Z}$ deviendra claire dans le chapitre suivant.

On définit $\mathbb{C}_n$ comme le groupe cyclique à n éléments. Il est unique à isomorphisme près :

Soient G, H deux groupes cycliques à n éléments et soient g, h deux générateurs respectifs. Alors, on peut définir un isomorphisme

$$\phi : G \longrightarrow H : g^i \mapsto h^i$$

pour tout $i \in \{1, ...n\}$. C'est bien un isomorphisme : c'est une bijection et c'est aussi un homomorphisme. Soient $x, y \in G$. Il existe $i, j \in \mathbb{Z}$ tels que $x = g^i$ et $y = g^j$. Alors $\phi(xy) = \phi(g^i g^j) = \phi(g^{i+j}) = h^{i+j} = h^i h^j = \phi(g^i)\phi(g^j) = \phi(x)\phi(y)$. (Attention, ici nous sommes partis du principe que $i + j \leq n$. Si $i + j > n$, que se passe-t-il ?. Il faut soustraire kn à $i + j$ où k est tel que $i + j - kn < n$, car $g^{kn} = e$. Ainsi, on retombe dans le cas $i + j < n$.)

Il y a une manière simple de se représenter ce groupe. Reprenons l'exemple 1.1.3. Considérons les entiers $\{1, ...n\}$. On peut définir une *addition modulo n* : on définit l'addition sur $\{1, ...n\}$ via :

$$a + b = (a + b) \bmod n,$$

où $(a+b) \bmod n$ est l'unique entier entre 1 et n qui est congruent à $a+b$ (ce nombre correspond au reste de la division de $(a+b)$ par n). La preuve de l'unicité est laissée en exercice.

Ce groupe est cyclique, car engendré par 1 : dans $\mathbb{Z}_n$, l'opération du groupe est en fait l'addition modulo n, et donc la puissance devient une multiplication. Nous reviendrons sur cet exemple dans le cours suivant.

1.5 Groupe symétrique et groupe alterné

Définition 1.5.1 (Rappel)**.** *Soit $n \geq 1$. Le groupe symétrique S_n est le groupe de toutes les bijections d'un ensemble à n éléments $\{1, ...n\}$:*

$$S_n = \{f : \{1, ..., n\} \longrightarrow \{1, ..., n\} \mid f \text{ est bijective}\}.$$

Un élément $\sigma \in S_n$ est appelé une permutation*, et on peut l'écrire comme une matrice :*

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

Un point fixe *de σ est un élément $i \in \{1, ..., n\}$ tel que $\sigma(i) = i$. Le* support *de σ est*

$$supp(\sigma) = \{i \in \{1, ..., n\} \mid \sigma(i) \neq i\} = \{1, ..., n\} \backslash \{points\ fixes\ de\ \sigma\}.$$

Remarque 1.5.2. *Le support d'une composition $\sigma\tau$ se comporte comme tel :*

$$supp(\sigma\tau) \subseteq supp(\sigma) \cup supp(\tau).$$

*En conséquence, si $supp(\sigma) \cap supp(\tau) = \emptyset$, alors σ et τ commutent : $\sigma\tau = \tau\sigma$. (*Exercice*).*

On peut décomposer une permutation en produit de permutations à supports disjoints.

Définition 1.5.3. *Pour $l \geq 1$, $i_1, ..., i_l \in \{1, ..., n\}$, un* cycle *de longueur l est une permutation σ définie comme suit : $\sigma(i) = i$ si $i \notin \{i_1, ..., i_l\}$, $\sigma(i_k) = i_{k+1}$ si $1 \leq k \leq l-1$ et $\sigma(i_l) = i_1$. On note un cycle $(i_1...i_l)$. Un cycle de longueur 2 est appelé une* transposition.

Exercice 1.5.4. *Montrer que la conjugaison de $\tau = (i_1...i_l)$ par σ, $\sigma\tau\sigma^{-1}$, est $(\sigma(i_1)...\sigma(i_l))$.*

On rappelle que toute permutation σ peut s'écrire comme un produit de cycles disjoints $\gamma_1, ..., \gamma_r$. Cette écriture est unique si la longueur des cycles est plus grande ou égale à 2. De plus, tout cycle peut se décomposer en produit de transpositions. Par exemple, le cycle (abc), qui transforme a en b, b en c et c en a peut se décomposer en deux transpositions $(abc) = (ab)(bc)$ ou encore en $(abc) = (bc)(ac)$. Ainsi, toute permutation est également un produit de transpositions (de manière non unique). C'est de cette manière qu'on peut définir la signature (vous avez vu une autre manière dans le cours d'Algèbre linéaire) :

$$sign(\sigma) = (-1)^k, \text{ où } k \text{ est le nombre de transpositions de } \sigma.$$

1.5.1 Le groupe alterné

Le groupe alterné A_n est un sous-groupe de S_n comprenant toutes les permutations contenant un nombre pair de transpositions :

$$A_n = \{\sigma \in S_n \mid \sigma \text{ s'écrit comme un nombre pair de transpositions}\}.$$

L'ordre de A_n est $\frac{n!}{2}$. En fait, A_n est le noyau de l'application signature (Exercice).

Exemple 1.5.5. *1. Le groupe $A_3 \leq S_3$ consiste exactement en $A_3 = \{I, (123), (132)\}$.*

2. Le groupe A_4 contient 12 éléments :

$\{I$, (234), (243), (134), (143), (124), (142), (123), (132), (12)(34), (13)(42), (14)(23)$\}$.

C'est un exemple de groupe non abélien. Par exemple, (123) *et* (234) *ne commutent pas.*

1.6 Groupe de matrices

1.
$$\mathrm{GL}(\mathbb{R}^n) = \{M : \mathbb{R}^n \to \mathbb{R}^n | \, T \text{ est une application linéaire bijective}\},$$
l'ensemble des applications linéaires bijectives $\mathbb{R}^n \to \mathbb{R}^n$ est le groupe de matrices n par n de déterminant non nul, appelé le *groupe général linéaire*.

2.
$$\mathrm{SL}(n) = \{M : \mathbb{R}^n \to \mathbb{R}^n | \, \det(M) = 1\}$$
est le groupe des matrices de déterminant 1, le *groupe spécial linéaire*.

3.
$$\mathrm{O}(n) = \{M : \mathbb{R}^n \to \mathbb{R}^n | \, M^{\mathrm{T}}M = MM^{\mathrm{T}} = I\}$$
est le groupe des matrices orthogonales. Notons que $\det(M) = \pm 1$ pour tout $M \in \mathrm{O}(n)$. On l'appelle le *groupe orthogonal*.

4.
$$\mathrm{SO}(n) = \{M : \mathbb{R}^n \to \mathbb{R}^n | \, \det(M) = 1 \text{ et } M^{\mathrm{T}}M = MM^{\mathrm{T}} = I\}$$
est le groupe des matrices orthogonales de déterminant 1. Notons que
$$\mathrm{SO}(n) = \mathrm{SL}(n) \cap \mathrm{O}(n).$$

Chapitre 2

Quotient de groupes

La notion de quotient est fondamentale en mathématiques, en particulier en théorie des groupes. Elle est liée à la notion de classe d'équivalence (il s'agit en fait d'une décomposition en classes d'équivalence bien spécifiques).

2.1 Classes à gauche et à droite

Définition 2.1.1. *Soit G un groupe et $X \subseteq G$ un sous-ensemble de G. Pour $g \in G$, on définit* la classe à gauche de g *par*

$$gX := \{gx \mid x \in X\},$$

l'ensemble des éléments de G qui sont obtenus en multipliant g avec un élément de X. La classe à droite de g est

$$Xg := \{xg \mid x \in X\}.$$

Si $H \leq G$ est un sous-groupe de G, alors gH est aussi appelé un coset *à gauche (et Hg un coset à droite). On dénote G/H l'ensemble des classes à gauche de H dans G :*

$$G/H := \{gH \mid g \in G\} = \{\{gh \mid h \in H\}, g \in G\},$$

(et $H\backslash G$ l'ensemble des classes à droite).

Remarque 2.1.2. *Si $h \in H$, alors $hH = H$, par définition d'un sous-groupe.*

Nous allons maintenant justifier la notation $\mathbb{Z}/n\mathbb{Z}$ du chapitre précédent.

Exemple 2.1.3. *Reprenons l'exemple de $\mathbb{Z}/n\mathbb{Z}$. L'ensemble des multiples de n est un groupe, $n\mathbb{Z}$. C'est en fait un sous-groupe de $\mathbb{Z}$. On peut considérer l'ensemble des cosets à gauche de $n\mathbb{Z}$ dans $\mathbb{Z}$:*

$$\mathbb{Z}/n\mathbb{Z} = \{x + n\mathbb{Z} \mid x \in \mathbb{Z}\} = \{n\mathbb{Z}, n\mathbb{Z} + 1, ..., n\mathbb{Z} + (n-1)\} \cong \{0, ..., n-1\}.$$

Nous allons voir comment déterminer une structure de groupe sur $\mathbb{Z}/n\mathbb{Z}$ dans la section suivante.

Remarque 2.1.4. *La définition 2.1.1 ne considère que les sous-ensembles d'un groupe. Mais c'est en fait une notion plus générale : pour X un ensemble quelconque et $\sim$ une relation d'équivalence sur X, on appelle l'ensemble des classes d'équivalence* l'ensemble quotient *et on le note $X/\sim$. Dans le cas de la définition 2.1.1, la relation d'équivalence en question est la suivante : $x \sim y$ si et seulement s'il y a un $g \in G$ tel que $gx = y$.*

La proposition suivante est très similaire à la décomposition en classes d'équivalence disjointes (en fait, c'est une conséquence directe du fait que les classes à gauche/droite sont des classes d'équivalence).

Proposition 2.1.5. *Si g_1H et g_2H sont deux cosets à gauche de H dans G, alors soit $g_1H = g_2H$, soit $g_1H \cap g_2H = \emptyset$.*

Démonstration. Soient $g_1, g_2 \in G$ un groupe et H un sous-groupe de G. Supposons que $g_1H \cap g_2H \neq \emptyset$. Alors il existe des éléments $h_1, h_2 \in H$ tel que $g_1h_1 = g_2h_2$. Or, dans ce cas, $g_1H = g_1h_1H = g_2h_2H = g_2H$, ce qui prouve la proposition. □

Notons que si $g_1H = g_2H$, alors $g_2^{-1}g_1 \in H$.
Par la proposition ci-dessus, l'ensemble des cosets d'un sous-groupe $H \leq G$ est bien défini, et on peut les compter. Ce nombre s'appelle *l'indice* de H dans G, et on le note $[G : H] := |G/H|$. Le théorème de Lagrange nous donne une relation entre l'indice d'un sous-groupe et le nombre d'élément du groupe et du sous-groupe.

Théorème 2.1.6 (Théorème de Lagrange)**.** *Soit G un groupe fini et $H \leq G$ un sous-groupe. Alors,*

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

Démonstration. Nous allons commencer par montrer que tous les cosets ont la même cardinalité. Soit $g \in G$, alors il existe une bijection

$$H \longrightarrow gH : h \mapsto gh,$$

d'inverse $g^{-1}h' \hookleftarrow h'$. Donc H et gH ont le même cardinal. Notons $d = [G : H]$. Alors $G/H = \{g_1H, ...g_dH\}$, avec $g_i \in G$ et $g_iH \neq g_jH$ si $i \neq j$. On affirme que $G = \bigcup_{g\in G} gH$. La première inclusion $G \supseteq \bigcup_{g\in G} gH$ est évidente. Pour montrer la deuxième, on se donne $g \in G$. Comme $g = g \cdot e$, et que $e \in H$ par définition d'un sous-groupe, on a que $g \in gH$.
Ainsi, $G = \bigcup_{g\in G} gH = \bigcup_{i=1}^{d} g_iH$ qui est en fait une union disjointe par la proposition précédente. On a donc $|G| = \sum_{i=1}^{d} \mid g_iH| = \sum_{i=1}^{d} |H| = d|H| = [G : H] \cdot |H|$. □

Corollaire 2.1.7. *Soit $H \leq G$ un sous-groupe de G fini, $K \leq H$ un sous-groupe de H et $g \in G$. Alors*

1. $|H| \,\Big|\, |G|$
2. $|\langle g\rangle| \,\Big|\, |G|$
3. $[G : K] = [G : H] \cdot [H : K]$.

Démonstration. Les deux premiers points sont évidents. Pour le troisième, on applique plusieurs fois le théorème de Lagrange : $|H| = [H : K] \cdot |K|$ et $|G| = [G : K] \cdot |K|$ donc $|G| = [G : H] \cdot |H| = [G : H] \cdot [H : K] \cdot |K|$. Ainsi,

$$\frac{|G|}{|K|} = [G : K] = [G : H] \cdot [H : K].$$

□

Les conséquences de ce théorème sont nombreuses : par exemple, on sait directement qu'il ne peut pas y avoir de sous-groupe d'ordre 2 ou 3 dans S_5, ou d'élément d'ordre 5 dans $\mathbb{Z}_6$.

2.2 Sous-groupes normaux

Les classes à gauche d'un sous-groupe prennent particulièrement d'importance lorsque le sous-groupe a une particularité en plus. Le but de cette particularité est de donner une structure de groupe aux cosets définis dans la définition 2.1.1.

On voudrait, pour avoir une opération bien définie, avoir $g'H * gH = g'gH$. Mais $g'HgH = g'gH$ est équivalent à $gHg^{-1} = H$, ce qui nous mène à la définition suivante.

Définition 2.2.1. *Soit $H \leq G$ un sous-groupe de G. Il est dit* normal *si*

$$gHg^{-1} = H \text{ pour tout } g \in G.$$

On note $H \triangleleft G$. De manière équivalente, un sous-groupe H est normal si $gH = Hg$ pour tout $g \in G$, soit si les classes à gauche et les classes à droite sont les mêmes.

Pour montrer qu'un sous-groupe est normal, il suffit de montrer l'inclusion $gHg^{-1} \subseteq H$. En effet, $H = g(g^{-1}Hg)g^{-1} \subseteq gHg^{-1}$ montre l'autre inclusion.

Exemple 2.2.2.

1. *Les sous-groupes $\{e\}$ et G sont toujours normaux dans G.*
2. *Si G est abélien, tout sous-groupe de G est normal. En effet, $ghg^{-1} = h$ pour tout $g \in G$, $h \in H$.*
3. *L'intersection de sous-groupes normaux est un sous-groupe normal (Exercice).*
4. *Le centre d'un groupe est $Z(G) = \{x \in G \mid gx = xg \text{ pour tout } g \in G\}$, l'ensemble des éléments qui commutent avec tous les autres dans G. Le centre est un sous-groupe normal (Exercice).*

Attention, être normal n'est pas transitif ! (Exercice)

Un groupe G est dit *simple* s'il ne possède que deux sous-groupes normaux : $\{e\}$ et G. L'intérêt des groupes simples est qu'ils servent de "building blocks" à d'autres groupes, car ils ne peuvent pas être réduits à des groupes plus petits.

Proposition 2.2.3. *Le groupe $\mathbb{Z}_n$ est simple si et seulement si n est premier.*

Démonstration. Exercice. □

Le groupe alterné A_5 d'ordre 5 est le premier exemple d'un groupe simple non abélien.

Théorème 2.2.4. *Si n est un entier supérieur ou égal à 5, le groupe alterné de degré n est simple.*

Démonstration. Algèbre II. □

2.3 Quotient

L'intérêt des sous-groupes normaux est de pouvoir donner une structure de groupe aux classes d'équivalence $G/H := \{gH \mid g \in G\}$. Le théorème suivant décrit cette structure de groupe.

Théorème 2.3.1. *Soit $H \triangleleft G$ un sous-groupe normal. Alors G/H muni de l'opération*

$$* : G/H \times G/H \longrightarrow G/H,\ xH * yH \mapsto xyH$$

est un groupe. De plus, l'application quotient

$$\pi : G \twoheadrightarrow G/H : x \mapsto xH$$

est un homomorphisme surjectif de noyau $\mathrm{Ker}(\pi) = H$.

Démonstration. Remarquons d'abord que $xHyH = xyH$. Cela découle du fait que H est un sous-groupe *normal* et que donc $yH = Hy$ (cela n'est pas forcément le cas pour un sous-groupe quelconque). Ainsi,

$$xHyH = xyHH = xyH.$$

Il en découle que l'application π est un homomorphisme.

Il faut ensuite vérifier que l'opération $*$ est bien définie, c'est à dire que si $xH = x'H$ et $yH = y'H$ alors $xH * yH = x'H * y'H$.

Si $xH = x'H$, il existe $h_1 \in H$ tel que $x = x'h_1$. De même, il existe $h_2 \in H$ tel que $y = y'h_2$. Ainsi, $xH* = xyH = xy'h_2H = xy'H = x'h_1y'H = x'y'H = x'H * y'H$, en utilisant que H est normal dans la dernière égalité.

Le fait que G/H est un groupe avec cette opération $*$ découle du fait que G est un groupe :

1. Associativité : $xH * (yH * zH) = x(yz)H = (xy)zH = (xH * yH) * zH$.
2. Elément neutre : $xH * H = xH * eH = xeH = xH$ pour tout $x \in H$.
3. Inverse : $xH * x^{-1}H = xx^{-1}H = eH = H$.

Pour l'application π, le fait qu'elle est surjective est trivial, et on vérifie quel est son noyau :

$$\mathrm{Ker}(\pi) = \{x \in G | \pi(x) = H\}.$$

Soit $x \in \mathrm{Ker}(\pi)$. Alors $\pi(x) = xH = H$, donc $x \in H$. On a montré que $\mathrm{Ker}(\pi) = H$. □

Exemple 2.3.2. *1. On peut toujours quotienter G par ses sous-groupes triviaux $\{e\}$ et G. On a : $G/G = \{e\}$ et $G/\{e\} = G$.*

2. Soit $G = \{e^{ik\pi/6}, k = 0, ...11\}$ les racines 12-ième de l'unité. C'est un groupe abélien (isomorphe au groupe cyclique C_{12} à 12 éléments). On considère le sous-groupes des racines 4-ième de l'unité $N = \{e^{ik\pi/6}, k = 0, 3, 6, 9\}$. Alors N est normal dans G et G/N est :

$$G/N = \{\{e^{ik\pi/6}, k = 0, 3, 6, 9\}, \{e^{ik\pi/6}, k = 1, 4, 7, 10\}, \{e^{ik\pi/6}, k = 2, 5, 8, 11\}\} \cong C_3.$$

3. Le groupe $SL(3)$ est normal dans $GL(3)$. Le quotient de $GL(3)$ par $SL(3)$ est isomorphe à $(\mathbb{R}^*, \cdot)$ (Exercice).

Remarquons que dans le cas de π défini dans le théorème précédent, $\mathrm{Ker}(\pi) \triangleleft G$. C'est le cas pour n'importe quel homomorphisme :

Exercice 2.3.3. *Soit $\phi : G \longrightarrow H$ un homomorphisme de groupe. Alors,* $\mathrm{Ker}(\phi) \triangleleft G$.

En conséquence, pour n'importe quel sous-groupe normal $N \triangleleft G$, il existe un homomorphisme ϕ de G dans un autre groupe H tel que le noyau de cet homomorphisme est N. Il suffit de prendre l'application quotient

$$G \longrightarrow G/N = H.$$

On va utiliser cela dans la prochaine section pour décrire les relations entre le noyau et l'image d'un homomorphisme.

2.4 Premier Théorème d'isomorphisme

Le but de cette section est de décrire le groupe H tel qu'il existe un homomorphisme $\phi : G \longrightarrow H$ dont le noyau est N.

Théorème 2.4.1 (Premier théorème d'isomorphisme)**.** *Soit $\phi : G \longrightarrow H$ un homomorphisme de groupe. Alors,*

$$G/\mathrm{Ker}(\phi) \cong \mathrm{Im}(\phi).$$

Démonstration. On définit

$$\hat{\phi} : G/\operatorname{Ker}(\phi) \longrightarrow \operatorname{Im}(\phi) : g\operatorname{Ker}(\phi) \mapsto \phi(g).$$

Le but est de montrer que $\hat{\phi}$ est un isomorphisme. On montre d'abord que $\hat{\phi}$ est bien définie, c'est-à-dire que si $g\operatorname{Ker}(\phi) = g'\operatorname{Ker}(\phi)$, alors $\hat{\phi}(g\operatorname{Ker}(\phi)) = \hat{\phi}(g'\operatorname{Ker}(\phi))$.

Or, comme avant, si $g\operatorname{Ker}(\phi) = g'\operatorname{Ker}(\phi)$, il existe $k \in \operatorname{Ker}(\phi)$ tel que $g = g'k$. Donc $\hat{\phi}(g\operatorname{Ker}(\phi)) = \phi(g) = \phi(g)e = \phi(g)\phi(k)$, car $k \in \operatorname{Ker}(\phi)$, et donc

$$\hat{\phi}(g\operatorname{Ker}(\phi)) = \phi(g)\phi(k) = \phi(gk) = \hat{\phi}(g'\operatorname{Ker}(\phi)).$$

On montre que $\hat{\phi}$ est un homomorphisme :

$$\hat{\phi}(g\operatorname{Ker}(\phi)g'\operatorname{Ker}(\phi)) = \hat{\phi}(gg'\operatorname{Ker}(\phi)) = \phi(gg') = \phi(g)\phi(g') = \hat{\phi}(g\operatorname{Ker}(\phi))\hat{\phi}(g'\operatorname{Ker}(\phi)).$$

Pour finir, $\hat{\phi}$ est bijective : elle surjective sur son image et injective car son noyau est trivial.

En effet, si $g\operatorname{Ker}(\phi) \in \operatorname{Ker}(\hat{\phi})$, alors $\hat{\phi}(g\operatorname{Ker}(\phi)) = e$, et donc $\phi(g) = e$ ce qui implique que $g \in \operatorname{Ker}(\phi)$. Ainsi, $g\operatorname{Ker}(\phi) = \operatorname{Ker}(\phi)$, l'élément neutre du groupe quotient.

□

Exemple 2.4.2. *Nous allons reprendre l'exemple de $\mathbb{Z}/n\mathbb{Z}$. Juste pour cet exemple, nous allons appeler C_n l'ensemble $\{0, ..., n-1\}$ muni de l'addition modulo n. Le but de cet exemple est de démontrer formellement que $\mathbb{Z}/n\mathbb{Z}$ est isomorphe à C_n. Même si nous avons vu dans le chapitre précédent que tous les groupes cycliques à n éléments sont isomorphes, nous n'avons encore pas formellement vérifié que $\mathbb{Z}/n\mathbb{Z}$ est un groupe cyclique.*

On définit $\phi : \mathbb{Z} \longrightarrow C_n : x \mapsto x \bmod n$. Le noyau de ϕ est exactement $n\mathbb{Z}$: en effet, nx est un multiple de n et donc $nx \bmod n = 0$. De plus, ϕ est surjective (on peut voir que $\phi(\{0, ..., n-1\})$ engendre C_n). En appliquant le premier théorème d'isomorphisme, on obtient $\mathbb{Z}/n\mathbb{Z} \cong C_n$. On vient de montrer formellement que $\mathbb{Z}/n\mathbb{Z}$ a la même structure de groupe que C_n.

Chapitre 3

Actions de groupes

3.1 Actions

Dans ce chapitre, nous allons voir la notion très importante d'action de groupe. C'est une manière d'appliquer une structure de groupe sur un ensemble qui n'en possède pas forcément. Les actions de groupe apparaissent naturellement dans beaucoup de domaines scientifiques, par exemple pour la classification de structures chimiques, où l'on s'intéresse à la forme d'une molécule, quelle que soit sa position dans l'espace à symétrie près.

Définition 3.1.1. *Soit X un ensemble.*

Une action *du groupe $(G, \cdot)$ sur X, ou G-action, est une application $\star : G \times X \to X$ telle que :*

(i) Pour tout $g, h \in G$, $x \in X$, $g \star (h \star x) = (g \cdot h) \star x$;

(ii) Pour tout $x \in X$, $1_G \star x = x$.

Une action d'un groupe G sur un ensemble X est dite fidèle *si pour $g \in G$ satisfaisant $g \star x = x$ pour tout $x \in X$, alors $g = 1_G$ (autrement dit, seul l'identité fixe tous les points de X).*
L'action est dite transitive *si pour tout $x, y \in E$ il existe un $g \in G$ tel que $g \star x = y$.*

Exemples 3.1.2.

1. *L'action triviale d'un groupe G sur un ensemble E, est définie par $g \star x = x$, pour tout $x \in E, g \in G$. Elle n'est évidemment ni transitive, ni fidèle.*

2. *Le groupe des matrices $GL_n(\mathbb{R})$ agit sur $\mathbb{R}^n$ par multiplication matrice-vecteur :* $GL_n(\mathbb{R}) \times \mathbb{R}^n \longrightarrow \mathbb{R}^n : (M, x) \mapsto M \cdot x$.
   Cette action est fidèle mais pas transitive.
   En effet, $M \cdot 0_{\mathbb{R}^n} = 0_{\mathbb{R}^n}, \forall M \in GL_n(\mathbb{R})$.

3. *On considère le groupe $(\mathbb{R}, +)$ et l'ensemble $\mathbb{C}$. L'application $\star : \mathbb{R} \times \mathbb{C} \to \mathbb{C}$ donnée par $t \star z = e^{2\pi i t} z$ est une action de groupe. Cette action n'est ni fidèle ni transitive.*

4. *Soit H un sous-groupe de $(G, \cdot)$. Alors H agit sur G par multiplication à gauche, c'est-à-dire, pour $h \in H$ et $g \in G$, $h \star g = h \cdot g$.*

5. *Soit H un sous-groupe de $(G, \cdot)$. Alors H agit sur G par multiplication par inverse à droite, c'est-à-dire, pour $h \in H$ et $g \in G$, $h \star g = g \cdot h^{-1}$.*
   En effet, soient $h, h' \in H$ et $g \in G$. Alors,

$$\begin{aligned} h \star (h' \star g) &= (g \cdot h'^{-1}) \cdot h^{-1} \\ &= g \cdot (h \cdot h')^{-1} \\ &= (h \cdot h') \star g. \end{aligned}$$

6. *Soit H un sous-groupe de $(G, \cdot)$. Alors H agit sur G par conjugaison, c'est-à-dire, pour $h \in H$ et $g \in G$, $h \star g = h \cdot g \cdot h^{-1}$.*

7. *Soit X un ensemble. Le groupe $\mathrm{Bij}(X)$ agit sur X par évaluation, c'est-à-dire pour $f \in \mathrm{Bij}(X)$ et $x \in X$, $f \star x = f(x)$.*

8. *Soit $\star$ une action de G sur X. Pour $S \subseteq X$ et $g \in G$, on note*

$$g \star S = \{g \star s \mid s \in S\}.$$

   Notons que cette formule détermine une action $G \times \mathcal{P}(X) \to \mathcal{P}(X)$ de G sur l'ensemble des parties de X (Exercice).

La proposition suivante décrit une relation entre les actions d'un groupe sur un ensemble X et l'ensemble des homomorphismes entre G et le groupe $\mathrm{Bij}(X)$.

Proposition 3.1.3. *Soit G un groupe et X un ensemble. Il existe une bijection entre l'ensemble des actions de G sur X et l'ensemble des homomorphismes de groupe $G \to \mathrm{Bij}(X)$.*

Démonstration. On définit

$$\rho : \{\text{Actions de } G \text{ sur } X\} \longrightarrow \{\text{Homomorphismes de } G \text{ dans } Bij(X)\}$$

$$a \mapsto \rho_a$$

Soit $a : G \times X \to X$ une action de G sur X que l'on note avec le symbole $\star$. On associe à a l'homomorphisme $\rho_a : G \to \mathrm{Bij}(X)$, où, pour $g \in G$, $\rho_a(g)$ est la bijection donnée, pour $x \in X$, par $\rho_a(g)(x) = g \star x$. Son inverse est $\rho_a(g^{-1})$ puisque pour tous $x \in X$, $\rho_a(g^{-1})\rho_a(g)(x) = g^{-1} \star g \star x = x$.

La fonction ρ_a est bien un homomorphisme, puisque pour tout $x \in X$, $g, g' \in G$,

$$\rho_a(gg')(x) = (gg') \star x = g \star (g' \star x) = \rho_a(g) \circ \rho_a(g').$$

Inversement, si $\rho_a : G \to \mathrm{Bij}(X)$ est un homomorphisme de groupe, l'application $a_\rho : G \times X \to X$ donnée par $a_\rho(g, x) = \rho(g)(x)$ est une action. En effet, pour $x \in X$, $a_\rho(1_G, x) = \rho(1_G)(x) = \mathrm{Id}_X(x) = x$. De plus, pour $g, h \in G$ et $x \in X$,

$$a_\rho(g, a_\rho(h, x)) = \rho(g)(\rho(h)(x)) = \rho(gh)(x) = a_\rho(gh, x).$$

On vérifie maintenant facilement que les applications $a \mapsto \rho_a$ et $\rho \mapsto a_\rho$ sont inverses l'une de l'autre. □

Remarque 3.1.4. *Une action a de G sur X est fidèle si et seulement si l'homomorphisme ρ_a définit ci-dessus est injectif. En effet, ρ_a est injectif si et seulement si son noyau est trivial. Or, le noyau de ρ_a est*

$$\mathrm{Ker}(\rho_a) = \{g \in G | \rho_a(g) = Id\} = \{g \in G | g \star x = x, \forall x \in X\}.$$

Donc ρ_a est injectif si et seulement si $\{g \in G | g \star x = x, \forall x \in X\} = \{1_G\}$, i.e. si et seulement si l'action est fidèle.

3.2 Stabilisateur et orbite

Soit $G \times X \to X$ une action de groupe. Il y a une relation sur X donnée par $x \sim y \Leftrightarrow \exists g \in G$ tel que $gx = y$. C'est une relation d'équivalence. En effet, pour tout $x, y, z \in X$, $g, h \in G$,

- $1_G x = x$ donc la relation est réflexive.

- $gx = y$ implique que $x = g^{-1}gx = g^{-1}y$, et donc la relation est symétrique.
- $gx = y$ et $hy = z$, alors $(hg)x = z$, donc la relation est transitive.

Définition 3.2.1.

On appelle la classe d'équivalence de x pour cette relation l'orbite *de x, et on la note* $\mathrm{Orb}(x)$, $G \cdot x$ *ou* Gx *:*

$$Gx = \mathrm{Orb}(x) := \{y \in X | \exists g \in G, gx = y\}.$$

Le stabilisateur *de $x \in X$, noté G_x ou* $\mathrm{Stab}(x)$*, est le sous-groupe de G qui contient les éléments qui fixent x, c'est-à-dire,*

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

Remarque 3.2.2. *Une action est transitive si et seulement si elle admet une unique orbite.*

Définition 3.2.3. *On considère l'action de H sur G par multiplication par inverse à droite. L'ensemble G/H est l'ensemble des orbites de cette action. L'orbite de $g \in G$ est notée gH.*

Observons que g' est dans l'orbite de g si et seulement si l'une des conditions équivalentes suivantes est satisfaite :

(i) il existe $h \in H$ tel que $g' = gh^{-1}$;

(ii) il existe $h \in H$ tel que $g' = gh$;

(iii) $g^{-1}g' \in H$.

Remarque 3.2.4. *On peut aussi définir l'ensemble des orbites d'une action quelconque d'un groupe G sur un ensemble X. On dénote alors aussi cet ensemble X/G.*

Proposition 3.2.5. *Si G agit sur X, alors X est partitionné en ses orbites :*

$$X = \bigsqcup_{x \in S} \mathrm{Orb}(x),$$

où S est un ensemble qui contient un élément de chaque orbite.

On appelle S un *système de représentants* et un élément de S un *représentant.*

Démonstration. Cela découle du fait que les orbites sont les classes d'équivalence de la relation $x \sim y \Leftrightarrow \exists g$ tel que $gx = y$, voir Proposition 1.1.2. □

Exemples 3.2.6.

1. *Pour l'action triviale de G sur X, où $gx = x$ pour tout $x \in X$, $g \in G$, on a $X/G = X$, c'est à dire que les orbites correspondent aux singletons,* $\mathrm{Orb}(x) = \{x\}$ *pour tout $x \in X$.*
2. *L'action de multiplication de matrices vue dans l'exemple 3.1.2 partage $\mathbb{R}^n$ en deux orbites disjointes : l'une pour l'élément $0_{\mathbb{R}^n}$, $\{0_{\mathbb{R}^n}\}$, et l'autre qui contient tout le reste, $\{x \in \mathbb{R}^n | x \neq 0_{\mathbb{R}^n}\}$. En effet, pour $x \neq 0, y \neq 0 \in \mathbb{R}^n$, il existe toujours une matrice $M \in GL_n(\mathbb{R})$ telle que $Mx = y$. Ainsi, $GL(n, \mathbb{R})$ agit sur $\mathbb{R}^n \setminus \{0\}$ de manière transitive.*

On peut utiliser la notion d'action de groupe et d'orbite pour redémontrer la formule de Lagrange vue dans le chapitre précédent.

Proposition 3.2.7 (Lagrange)**.** *Soit G un groupe fini et H un sous-groupe. Alors $|G| = |H| \cdot |G/H|$.*

Démonstration. On observe que gH est en bijection avec H pour tout g dans G. En effet, $h \mapsto g \cdot h$ est une telle bijection, d'inverse $k \mapsto g^{-1} \cdot k$.

Par conséquent, $|H| \cdot |G/H| = |G|$. □

Le stabilisateur d'un élément est en fait un sous-groupe de G. En effet, $e \in \mathrm{Stab}(x)$, si $g \in \mathrm{Stab}(x)$ alors $g^{-1} \in \mathrm{Stab}(x)$ car $g^{-1}x = g^{-1}gx = ex = x$ et si $g, g' \in \mathrm{Stab}(x)$, on a $gx = g'x = x$ et donc $(gg')x = x$ également. La proposition suivante nous montre comment le quotient de G par les stabilisateurs est en lien avec les orbites de l'action.

Proposition 3.2.8. *Soit $G \times X \to X$ une action de G sur X et $x \in X$. Alors, il y a une bijection $G/\mathrm{Stab}(x) \cong \mathrm{Orb}(x)$.*

Démonstration. On définit une fonction $\phi : G/\mathrm{Stab}(x) \to \mathrm{Orb}(x)$ par

$$\phi(g\mathrm{Stab}(x)) = gx.$$

Il faut vérifier que ϕ est bien définie, c'est-à-dire que si $g\mathrm{Stab}(x) = g'\mathrm{Stab}(x)$, alors $gx = g'x$. Or, ceci est le cas si et seulement si $g^{-1}g' \in \mathrm{Stab}(x)$. Ceci implique que $gx = gg^{-1}g'x = g'x$.

On observe que ϕ est surjective par construction. Pour l'injectivité, supposons que $gx = hx$. Alors $g^{-1}hx = x$ et donc $g^{-1}h \in \text{Stab}(x)$. Ceci montre que $g\text{Stab}(x) = h\text{Stab}(x)$. □

Notons que en fait, $\text{Stab}(x)$ est un sous-groupe pour tout $x \in X$ (Exercice). Ce n'est par contre par forcément un sous-groupe normal. Prenons par exemple l'action du groupe symétrique S_3 sur $\{1, 2, 3\}$. Alors $\text{Stab}(1) = \{e, (23)\} \leq S_3$ mais il n'est pas normal : $(12)(23)(12)^{-1} = (13) \notin \text{Stab}(1)$.

La proposition précédente nous donne une relation entre le sous-groupe du stabilisateur d'un élément et l'orbite du même élément. En particulier, l'indice du stabilisateur d'un élément dans G est égal au cardinal de son orbite.

Corollaire 3.2.9 (Formule des orbites)**.** *Pour une action de G fini sur X, on a, pour tout $x \in X$:*

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

Démonstration. Cela découle du théorème de Lagrange et de la proposition précédente, car le stabilisateur de x est un sous-groupe de G. □

Exercice 3.2.10. *(Défi) Montrer que le stabilisateur de x dépend seulement de son orbite. Autrement dit, si x et y sont dans la même orbite, il y a un homomorphisme de groupe bijectif* $\text{Stab}(x) \cong \text{Stab}(y)$.
Indice : Considérer la conjugaison par l'élément $g \in G$ qui "transporte x sur y".

3.3 Formule de Burnside

La formule de Burnside est une formule utilisée pour compter les différentes possibilités d'objets symétriques, par exemple, des colliers de perles de différentes couleurs. Elle établit une relation entre les points fixes d'une action, le nombre d'orbites et le nombre d'éléments dans le groupe G.

Soit G un groupe fini qui agit sur un ensemble fini X. On note les *points fixes* de $g \in G$

$$X^g = Fix(g) = \{x \in X | gx = x\},$$

l'ensemble des points qui sont fixé par g. La formule de Burnside est la suivante :

Théorème 3.3.1. *Le nombre d'orbites $|X/G|$ satisfait :*

$$|X/G| = \frac{1}{|G|} \sum_{g \in G} |X^g|.$$

Démonstration. On va compter les éléments d'un ensemble spécifique de deux manières différentes (argument de double comptage). Soit

$$Y = \{(g, x) \in G \times X | gx = x\}.$$

L'idée est de compter les éléments de Y par rapport à X et par rapport à G.

— Par rapport à G : Par définition,

$$Y = Y \cap (G \times X) = Y \cap \coprod_{g \in G} (\{g\} \times X) = \coprod_{g \in G} Y \cap (\{g\} \times X).$$

Mais

$$Y \cap (\{g\} \times X) = \{(g, x) \in \{g\} \times X \mid gx = x\} = \{g\} \times \{x \in X \mid gx = x\} = \{g\} \times X^g.$$

Ainsi, $Y = \coprod_{g \in G} \{g\} \times X^g$, ce qui nous donne $|Y| = \sum_{g \in G} |X^g|$.

— Par rapport à X :

$$Y = \coprod_{x \in X} Y \cap (G \times \{x\}).$$

Regardons ce qu'est $Y \cap (G \times \{x\})$.

$$Y \cap (G \times \{x\}) = \{(g, x) \in G \times \{x\} \mid gx = x\} = \{g \in G \mid gx = x\} \times \{x\} = \mathrm{Stab}(x) \times \{x\}.$$

Ainsi, $Y = \sum_{x \in X} \mathrm{Stab}(x) \times \{x\}$, et $|Y| = \sum_{x \in X} |\mathrm{Stab}(x)|$. Reste à compter le nombre d'éléments dans le stabilisateur. Comme nous allons le voir en exercice, deux éléments dans la même orbite ont le même nombre d'éléments dans leur stabilisateur. Soit $N = |X/G|$ le nombre d'orbites et soient $x_1, ...x_N$ des représentants de chaque orbite.

Nous avons :

$$|Y| = \sum_{x \in X} |\mathrm{Stab}(x)| = \sum_{x \in X} \frac{|G|}{|\mathrm{Orb}(x)|} = \sum_{i=1}^{N} \sum_{x \in \mathrm{Orb}(x_i)} \frac{|G|}{|\mathrm{Orb}(x)|} = \sum_{i=1}^{N} \sum_{x \in \mathrm{Orb}(x_i)} \frac{|G|}{|\mathrm{Orb}(x_i)|}$$

$$= \sum_{i=1}^{N} \frac{|G| \cdot |\mathrm{Orb}(x_i)|}{|\mathrm{Orb}(x_i)|} = \sum_{i=1}^{N} |G| = N \cdot |G|.$$

De cela nous déduisons $|Y| = N \cdot |G|$.

Ainsi,

$$N = \frac{1}{|G|} \sum_{g \in G} |X^g|.$$

□

Exemple 3.3.2 (Application au comptage d'objets symétriques)**.** *On aimerait compter le nombre de colliers possible contenant* 6 *perles de* k *couleurs différentes. Evidemment, deux colliers sont équivalents si on les tourne ou qu'on regarde la version "miroir".*

Formellement, fixons une numérotation des perles $\{p_1, ..., p_6\}$ *et* $\{1, ..., k\}$ *les couleurs. L'ensemble* X *des représentations de colliers est*

$$X = \{x : \{p_1, ...p_6\} \longrightarrow \{1, ..., k\}\}.$$

Cet ensemble contient k^6 *éléments. Les perles forment un* 6*-gone régulier. Les symétries pour lesquelles nous considérons deux colliers équivalents correspondent au groupe de symétries d'un* 6*-gone, qu'on appelle le* groupe diédral *et qu'on dénote* $D_{2\cdot 6}$ *dans le cas du* 6*-gone. Vous avez déjà vu des exemples de groupes diédraux, comme le groupe* D_8 *que vous avez étudié dans le cadre des isométries de* $\mathbb{R}^2$ *en première année. Nous reviendrons sur ces groupes plus en détails dans le chapitre suivant. Pour le moment, on considère juste*

$$D_{12} = \{Id, r, r^2, 3^3, r^4, r^5, s, rs, r^2s, r^3s, r^4s, r^5s\},$$

où r *est une rotation d'angle* $\pi/3$ *et* s *est une réflexion par l'axe des abscisses.*

Ce groupe D_{12} *agit sur les colliers* X *(puisque les perles forment un* 6*-gone régulier) et deux représentations* x, x' *sont les mêmes si et seulement si il existe* $g \in D_{12}$ *tel que* $gx = x'$ (i.e. *si* x *et* x' *sont dans la même orbite).*
Pour compter le nombre de représentations à symétrie près, il suffit donc de compter le nombre d'orbite de cette action, en utilisant la formule de Burnside :

$$|X/G| = \frac{1}{|G|} \sum_{g \in G} |X^g|.$$

On va donc compter $|X^g|$ *pour chaque* $\in D_{12}$.

1. *Pour* $g = Id$, $X^{Id} = \{x \in X \mid Id \cdot x = x\} = X$ *et donc* $|X^{Id}| = k^6$.

2. *Lorsque* $g = r$, $X^r = \{x \in X \mid r \cdot x = x\}$, *l'ensemble des représentations invariante par rotation d'une perle. Toutes les perles ont donc la même couleur, et* $|X^r| = k$. *De même pour* $g = r^5$.

3. *Pour* $g = r^2$, *une perle sur deux a la même couleur, donc on a deux choix possibles de couleur et* $|X^{r^2}| = k^2$. *De même pour* $g = r^4$.

4. *Lorsque* $g = r^3$, *Une perle sur trois a la même couleur, on a donc* 3 *choix possibles de couleur,* $|X^{r^3}| = k^3$.

5. *Lorsque* $g = s$ *ou* $g = r^2s$ *ou* $g = r^4s$, *on peut utiliser* 4 *types de perles,* $|X^{r^2s}| = |X^{r^4s}| = k^4$.

6. *Lorsque* $g = rs, r^3s$ *ou* r^5s, *on a une réflexion par un axe qui passe entre les perles. Ainsi, on a besoin de* 3 *couleurs différentes, et* $|X^{rs}| = |X^{r^3s}| = |X^{r^5s}| = k^3$.

On peut maintenant utiliser la formule de Burnside pour compter le nombre de colliers de perles possibles à symétries près. Le nombre de colliers à 6 *perles et* k *couleurs est donc*

$$|X/G| = \frac{1}{12}(k^6 + 2k + k^2 + 4k^3 + 3k^4).$$

Ce type d'étude peut se réveler très utile dans des domaines comme la chimie ou la biochimie, où l'on s'intéresse aux propriétés de certaines molécules ou protéines à symétrie près, par exemple.

Chapitre 4

Eléments de classification des groupes

Dans ce chapitre, nous revenons sur certains principes déjà introduit dans les premiers chapitres du cours. Le but est de classifier les groupes (ici : petits ou abéliens) à isomorphisme près. La classification des groupes est encore un domaine de recherche actif en mathématiques.
Nous avons vu les quotients de groupes, permettant de décomposer un groupe en deux "parties" : un sous-groupe normal et le quotient du groupe par ce sous-groupe. Dans ce chapitre nous verrons une manière "d'étendre" les groupes, en créant de nouveaux groupes à partir de plus petits.

Le théorème de Lagrange, vu dans la première partie du cours, et d'autres propriétés sur l'ordre des éléments et du groupe seront très utilisés dans ce chapitre. Le théorème 4.0.2 donne un bon exemple du type de preuve que nous allons voir. On va utiliser le lemme suivant pour démontrer cette proposition.

Lemme 4.0.1. *Soit G un groupe, $x \in G$ un élément, et soit $a \in \mathbb{Z} \setminus \{0\}$. Alors*

1. *si $|x| = \infty$, alors $|x^a| = \infty$.*
2. *Si $|x| = n$, alors $|x^a| = \frac{n}{pgdc(n,a)}$*
3. *Si $|x| = n < \infty$ et a est positif et divise n, alors $|x^a| = n/a$.*

La démonstration se fera en exercice.
Le théorème suivant donne une sorte de converse du théorème de Lagrange qui dit

que l'ordre d'un sous-groupe divise l'ordre d'un groupe. En général, il existe des groupes d'ordre n avec d un diviseur de n tel que G n'a pas de sous-groupe d'ordre d. Mais d est un nombre premier, alors un tel sous-groupe existe forcément.

Théorème 4.0.2 (Cauchy)**.** *Soit G un groupe fini et p un nombre premier qui divise l'ordre de G. Alors G contient un élément d'ordre p.*

On va démontrer ce théorème dans le cas où G est abélien uniquement.

Démonstration. Pour G abélien. On procède par induction sur l'ordre de G. Si $|G| = p$, comme $|G| > 1$, il existe un élément $x \in G$ tel que $x \neq e$. Par le théorème de Lagrange, l'ordre d'un élément divise l'ordre du groupe et comme $|G| = p$, $|x| = p$. Ainsi, on suppose que $|G| > p$. Si p divise l'ordre de x , on écrit donc $|x| = pn$. Par le lemme précédent (3), $|x^n| = p$, donc on a un élément d'ordre p. Supposons maintenant que p ne divise pas $|x|$. Dans ce cas, on considère le sous-groupe engendré par x : $N = \langle x \rangle$. Puisque G est abélien, N est normal, et par le théorème de Lagrange, $|G/N| \cdot |N| = |G|$. Comme p ne divise pas $|N|$, p divise forcément $|G/N|$. Par induction, comme $N \neq \{e\}$, $|G/N| \leq |G|$, et il existe un élément $\overline{y} = yN \in G/N$ d'ordre p. Comme $\overline{y} \neq e$, $y \notin N$, mais $y^p \in N$ car $\overline{y}^p = \overline{1} = N$. De plus, $\langle y^p \rangle \neq \langle y \rangle$ pour les mêmes raisons que précedemment. Ainsi, $|y^p| < |y|$. Par le lemme (2), p divise $|y|$, et on se retrouve dans la situation précédente où p divisait $|x|$. □

Par le théorème de Lagrange, si l'ordre d'un groupe G est premier, alors ses seuls sous-groupes sont $\{e\}$ et G, et donc G est simple. En fait, tout groupe abélien simple est isomorphe à $\mathbb{Z}_p$ pour un p (Exercice). Le premier groupe simple non abélien est d'ordre 60 et il s'agit de A_5.

Le théorème suivant donne la liste complète des sous-groupes d'un groupe cyclique :

Théorème 4.0.3. *Soit C_n le groupe cyclique d'ordre n fini. Alors :*

(i) Tout sous-groupe de C_n est cyclique d'ordre d qui divise n,

(ii) Réciproquement, si d est un diviseur de n, alors il existe un unique sous-groupe cyclique d'ordre d dans C_n, engendré par $g^{n/d}$ (où g est un générateur de C_n).

Démonstration. On va utiliser la notation $\mathbb{Z}_n$ et considérer le groupe cyclique avec l'addition modulo n. On rappelle que pour G un groupe et N un sous-groupe normal,

il y a une bijection entre les sous-groupes de G contenant N et les sous-groupes de G/N. Les sous-groupes de $\mathbb{Z}_n$ sont donc en bijection avec les sous-groupes de $\mathbb{Z}$ contenant $n\mathbb{Z}$. Or, tous les sous-groupes de $\mathbb{Z}$ sont isomorphes à $\mathbb{Z}$ (Exercice). De plus, $d'\mathbb{Z} \supseteq n\mathbb{Z}$ si et seulement si d' divise n. Donc tout sous-groupe de $\mathbb{Z}_n$ est d'ordre un diviseur d' de n. Et comme $d'\mathbb{Z}_n = \{0, \overline{d'}, \overline{2d'}, ..., \overline{(n/d'-1)d'}\}$ est cyclique d'ordre n/d', on voit que $d' = n/d$. □

Dans la suite de ce chapitre, nous aurons besoin de la définition de p-groupe :

Définition 4.0.4. *Soit p un nombre premier. Un p-*groupe *est un groupe fini d'ordre une puissance p^n de p.*

Exemples 4.0.5. *1. Si G est d'ordre p, alors on a vu que $G \cong \mathbb{Z}_p$.*

2. Le groupe diédral D_8 et le groupe des quaternions Q_8 sont des 2-groupes.

3. Le groupe $\mathbb{Z}/p^{a_1} \times \mathbb{Z}/p^{a_2} \times \cdots \times \mathbb{Z}/p^{a_n}$ pour $a_i \in \mathbb{N}$ est un p-groupe (dont nous reparlerons à la fin de ce chapitre).

Remarque 4.0.6. *Tout sous-groupe et tout groupe quotient d'un p-groupe est un p-groupe. En effet, le théorème de Lagrange, $|G| = p^n = |H| \cdot |G/H|$ implique que l'ordre de H et G/H sont aussi des puissances de p.*

4.1 Théorème de Cayley

Nous faisons un rapide détour avec les actions de groupe pour démontrer le théorème de Cayley, qui dit que tout groupe est isomorphe à un sous-groupe de S_n pour un certain n.

Pour cela, nous avons besoin du théorème suivant :

Théorème 4.1.1. *Soit G un groupe, H un sous-groupe et considérons l'action de G sur G/H par multiplication à gauche par des éléments de G. Considérons ρ la permutation associée à cette action (définie dans la proposition 3.1.3). Alors :*

1. G agit de manière transitive sur G/H ;

2. Le stabilisateur de l'action est H ;

3. Le noyau de ρ est $\bigcap_{x\in G} xHx^{-1}$, et $\mathrm{Ker}(\rho)$ est le plus grand sous-groupe normal de G contenant H.

Rappelons que G/H n'est pas forcément un groupe, si H n'est pas normal. Mais il s'agit d'un ensemble sur lequel G peut agir de toute manière.

Démonstration. Exercice. □

On déduit le théorème de Cayley de ce théorème :

Théorème 4.1.2 (Théorème de Cayley)**.** *Tout groupe fini est isomorphe à un sous-groupe d'un groupe symétrique. Si G est d'ordre n, alors $G \leq S_n$.*

Démonstration. On applique le théorème précédent à $H = \{1\}$, soit on considère l'action de G sur lui même par multiplication à gauche. Cela induit un homomorphisme ρ de G dans $Bij(G)$ dont le noyau est $H = \{1\}$. Ainsi, $G \cong \rho(G) \subseteq S_{|G|}$. □

4.2 Produit semi-direct

Avant de passer à la classification des groupes abéliens, nous faisons un petit détour pour discuter d'une manière de créer de nouveaux groupes à partir de plus petits groupes. Nous avons vu des exemples de produit direct de deux groupes, et nous allons voir un nouveau type de produit sur les groupes : le produit semi-direct. Nous commençons par la définition de produit semi-direct *interne*, où l'on décompose un groupe G en produit (semi-direct) de deux de ses sous-groupes.

Définition 4.2.1. *Soit G un groupe et N, H deux sous-groupes de G, avec N un sous-groupe normal. On dit que G est le produit semi-direct (interne) de N et H, qu'on note $G = N \rtimes H$, si il satisfait l'une des conditions suivantes (qui sont équivalentes) :*

(i) $G = NH$ et $H \cap N = \{e\}$.

(ii) Tout élément $g \in G$ s'écrit de manière unique comme $g = nh$ avec $n \in N$ et $h \in H$.

(iii) Tout élément $g \in G$ s'écrit de manière unique comme $g = hn$ avec $n \in N$ et $h \in H$.

iv) Considérons $i : H \longrightarrow G : h \mapsto h$ et $\pi : G \longrightarrow G/N : g \mapsto gN$. Alors la composition $\pi \circ i$ définit un isomorphisme de H dans G/N.

(v) Il existe un homomorphisme de G dans H dont la restriction à H est l'identité et dont le noyau est N.

Notons que l'application $G \longrightarrow N \times H : g \mapsto (n, h)$, où $g = nh$ de manière unique, est bijective, mais n'est pas un isomorphisme !

Comme N est normal, on a en particulier que pour tout $n \in N$ et $h \in H$, le conjugué de n par h est dans N : $hnh^{-1} \in H$. La loi de composition dans G est entièrement déterminée par celles de N et H et par l'action de conjugaison de H sur N : Soient $g, g' \in G$, on peut écrire $g = nh$ et $g' = n'h'$. On calcule gg' :
$gg' = (nh)(n'h') = nhn'(h^{-1}h)n' = n(hn'h^{-1})hh' = n''h''$,
où $n'' = nhn'h^{-1} \in N$ et $h'' = hh' \in H$.

Dans le cas particulier où $hnh^{-1} = n$, c'est à dire si $nh = hn$ pour tout $n \in N$ et $h \in H$, on a un produit direct $G = N \times H$. Ainsi, le produit semi-direct (interne) est une généralisation du produit direct.

Exemple 4.2.2.
1. *Le groupe diédral (que l'on verra dans les exposés)* $D_{2\cdot 6} = C_6 \rtimes C_2$, *où* C_i *denote le groupe cyclique à* i *éléments. Ici,* $C_6 = \{Id, r, r^2, ..., r^5\}$ *et* $C_2 = \{Id, s\}$.
2. *Le groupe* $O(n)$ *est aussi un produit semi-direct de deux groupes :* $O(n) = SO(n) \rtimes \{Id, s\}$, *où* s *est la symétrie d'axe des abscisses représentée par la matrice de déterminant* -1 *:* $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$.
3. $S_n = A_n \rtimes \langle \tau \rangle$, *où* τ *est une transposition quelconque de* S_n.

Avec le produit semi-direct interne, on peut décomposer G en produit de deux de ses sous-groupes. Le produit semi-direct *externe* est une généralisation du produit direct de deux groupes, où l'on choisit deux groupes N et H et on construit un nouveau groupe G à partir de ces deux groupes. Pour cela, on a besoin d'un homomorphisme $\varphi : H \longrightarrow \mathrm{Aut}(N)$, où $\mathrm{Aut}(N) = \{\rho : N \longrightarrow N \mid \rho \text{ est un isomorphisme}\}$ les homomorphsimes de N dans N. Avec ces informations, on construit un nouveau groupe où les éléments sont ceux de $G = N \times H$ comme **ensemble**, et l'opération dépend de φ :

$$(n, h) * (n', h') = (n\varphi_h(n'), hh').$$

On peut vérifier que cela définit bien une opération de groupe sur $G = N \times H$, où l'inverse de (n, h) est $(\varphi_{h^{-1}}(n^{-1}), h^{-1})$.
Notons que $G \cong N \times H$ comme **groupe** si et seulement si $\varphi_h(n) = n$ pour tout $h \in H, n \in N$.

Notons également qu'on retombe sur le cas du produit semi-direct *interne* en considérant $\varphi_h : n \mapsto hnh^{-1}$, la conjugaison.
Pour chaque homomorphisme $\varphi : H \longrightarrow \mathrm{Aut}(N)$, on a une structure de groupe différente sur $G = N \times H$. Remarquons que par la proposition 3.1.3, un tel homomorphisme est équivalent à une action de groupe de H sur N via l'action $h * n = \varphi_h(n)$!

4.3 Classifications des groupes abéliens

4.3.1 Théorème fondamental des groupes abéliens finiment engendrés

Le théorème fondamental des groupes abéliens finiment engendrés donne un moyen de classifier les (comme le nom l'indique) groupes abéliens finiment engendrés.
Un groupe G est *engendré* par un ensemble d'éléments $\{g_1, g_2, ...\}$ si tout élément $g \in G$ peut s'écrire comme produit des g_i, noté $G =< g_1, ... >$. C'est une généralisation d'un groupe engendré par un seul élément comme nous avons vu dans le Chapitre 1. Un groupe G est *finiment engendré* s'il existe un ensemble fini qui génère G.
Tout produit de groupes abéliens est abélien. En particulier, tout produit de groupes de type $\mathbb{Z}_n$ est abélien. Le théorème fondamental des groupes abéliens finiment engendrés nous dit qu'en fait, tout groupe abélien finiment engendré est un produit (direct) de groupes cycliques et de groupes isomorphes à $\mathbb{Z}$. La preuve que nous allons voir se base sur un théorème de Cauchy vu dans la section précédente.

Théorème 4.3.1 (Cauchy, rappel du théorème 4.0.2)**.** *Soit G un groupe fini et p un premier qui divise l'ordre de G. Alors, G possède un élément d'ordre p (de manière équivalente : G a un sous-groupe d'ordre p).*

Dans un groupe cyclique, tout sous-groupe est uniquement déterminé par son ordre. Le lemme suivant donne une sorte de converse pour les p-groupes.

Lemme 4.3.2. *Si G est un p-groupe abélien et que G a un unique sous-groupe H d'ordre p, alors G est cyclique.*

Démonstration. Par induction sur l'ordre de G : si $|G| = p$, c'est évident. On définit $\phi : G \longrightarrow G : \phi(g) = pg$. Soit K le noyau de ϕ, qui consiste exactement en les éléments d'ordre p ou 1. Comme $H \leq K$, K n'est pas trivial. Pour tout élément $g \neq e \in K$, $\langle g \rangle$ est d'ordre p et donc est contenu dans H. Donc $K = H$. Si $K = G$, alors G est cyclique et on a fini. Si $K \neq G$, alors $\phi(G)$ est un sous-groupe propre et non trivial de G isomorphe à G/K par le premier théorème d'isomorphisme. Ainsi, par le théorème de Cauchy, $\phi(G)$ a un sous-groupe d'ordre p. Comme tout sous-groupe de $\phi(G)$ est aussi un sous-groupe de G, il y en a un unique, $H = K$. Par hypohèse de récurrence sur $\phi(G) \cong G/K$, on conclut que ce groupe est cyclique. En notant G/K comme $\langle g + K \rangle$, on va montrer que g génère aussi G. Il suffit de montrer que $K \leq \langle g \rangle$. Par Cauchy, $\langle g \rangle \leq G$ a un sous-groupe d'ordre p, qui par unicité doit être K. □

Ce corollaire combiné avec le théorème de Cauchy implique qu'un p-groupe abélien non-cyclique possède nécessairement plus d'un sous-groupe d'ordre p, ce qui nous mène au lemme suivant.

Lemme 4.3.3. *Soit G un p-groupe abélien et C un sous-groupe cyclique de G maximal, c'est à dire qu'il n'y a pas de sous-groupe de G contenant C. Alors $G \cong C \times H$ pour un sous-groupe H.*

Démonstration. Par récurrence sur l'ordre de G. Si G est cyclique, alors $G = C$ et $H = \{e\}$. Si G n'est pas cyclique, on vient de voir que G possède plus d'un sous-groupe d'ordre p, alors que C qui est cyclique en possède un unique. Soit K un sous-groupe d'ordre p non contenu dans C, alors K est d'ordre premier et $(K \cap K = \{e\}$. Ainsi, $(C \times K)/K \cong C$.
Soit $g \in G$. L'ordre de $g + K$ dans G/K divise $|g|$, qui est au plus $|C|$. Donc le sous-groupe cyclique $(C \times K)/K \cong C$ est d'ordre maximal dans G/K et on applique l'hypothèse de récurrence pour avoir la décomposition :

$$G/K \cong (C \times K)/K \times H',$$

pour $H' \leq G/K$. La préimage de H par l'application $G \longrightarrow G/K$ est un sous-groupe H tel que $K \leq H \leq G$. Mais comme $G/K = (C \times K)/K \times H/K$, on a $G = (C \times K) \times H = C \times (K \times H) \cong C \times H$ (car $H \cap C = \{e\}$). □

Grâce à ce travail, nous pouvons finalement démontrer le théorème de classifications des groupes abéliens finiment engendrés.

Théorème 4.3.4 (Théorème de classifications des groupes abéliens finis)**.** *Soit G un groupe abélien fini. Alors G est un produit direct de sous-groupes cycliques de puissance de premiers :*

$$G \cong \bigotimes_i \mathbb{Z}_{p_i^{n_i}},$$

où les p_i sont des premiers et $n_i \in N$.

Démonstration. Pour tout p premier divisant l'ordre de G, on pose $G_p = \{g : |g| = p^k\}$ et $G_{p'} = \{g : p \nmid |g|\}$. Par le théorème de Cauchy, G_p est un p-groupe non trivial. Si g a ordre $p^k m$ avec $p \nmid m$, alors $p^k g \in G_{p'}$ et $mg \in G_p$. Puisque p^k et m sont premiers entre eux, il existe r, s tels que $rp^k + sm = 1$ (Bezout). Ainsi, on peut écrire $g = rp^k g + smg$ comme une somme d'éléments dans G_p et $G_{p'}$. Cela montre que $G \cong G_p \times G_{p'}$.
On répète le même processus pour les nombres premiers restant qui divisent l'ordre de $G_{p'}$. On peut ainsi décomposer G en produit direct de p-groupes pour différents p. Il suffit donc de montrer le théorème pour les p-groupes.
Supposons donc que G est d'ordre p^k. Par récurrence sur k, soit C un groupe cyclique inclut dans G maximal. Alors, par le lemme précédent, $G \cong C \times H$ avec $|H| < |G|$. Par hypthèse de récurrence, H est un produit direct de sous-groupes cycliques, et la preuve est finie. □

Exemples 4.3.5.

1. *Soit G un groupe abélien d'ordre 4. On peut écrire 4 comme $2 \cdot 2$ ou comme 4. Ainsi, les seuls groupes abéliens d'ordre 4 sont $\mathbb{Z}_2 \times \mathbb{Z}_2$ et $\mathbb{Z}_4$.*
2. *Soit G un groupe abélien d'ordre 6. On peut écrire 6 comme $2 \cdot 3$ ou comme 6. Ainsi, les seuls groupes abéliens d'ordre 6 sont $\mathbb{Z}_2 \times \mathbb{Z}3$ et $\mathbb{Z}_6$, sauf que ces deux groupes sont isomorphes. Ainsi, il n'y a qu'un seul groupe abélien d'ordre 6.*
3. *On peut classifier de la même manière de plus gros groupes : par exemple, les groupes d'ordre 48. Soit G un groupe abélien d'ordre 48. On a $48 = 2^4 \cdot 3$. On peut décomposer 48 de plusieurs manières différentes : $48 = 3 \cdot 16$; $48 = 3 \cdot 8 \cdot 2$; $48 = 3 \cdot 4 \cdot 4$; $48 = 3 \cdot 4 \cdot 2 \cdot 2$; $48 = 3 \cdot 2 \cdot 2 \cdot 2 \cdot 2$. Les 5 groupes abéliens d'ordre*

48 *sont donc :* $\mathbb{Z}_{16} \times \mathbb{Z}_3$ *;* $\mathbb{Z}_8 \times \mathbb{Z}_2 \times \mathbb{Z}_3$ *;* $\mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_3$ *;* $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$ *et* $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$.

Pour G un groupe et $g \in G$, on dit que g est de *torsion* si l'ordre de g est fini. La *torsion* T *de* G est l'ensemble des éléments de torsion de G, et il s'agit d'un sous-groupe (Exercice). On dit que G est sans torsion si $T = \{e\}$ et on appelle G un *groupe de torsion* si $G = T$.

Exemple 4.3.6. *Le groupe* $\mathbb{Q}/\mathbb{Z}$ *vu en exercice est un groupe de torsion et le groupe* $\mathbb{Z}$ *est un groupe sans torsion.*

Théorème 4.3.7. *Soit* G *un groupe abélien sans torsion et finiment engendré. Alors* $G \cong \mathbb{Z}^d$ *pour un certain* d.

Démonstration. L'idée de la preuve repose sur la construction d'un homomorphisme $\phi : \mathbb{Z}^d \longrightarrow G$, avec d le nombre de générateurs de G. Soient $g_1, ...g_d$ les d générateurs de G et on définit $\phi(a_1, ...a_n) = a_1g_1 + ...a_ng_n$. On montre ensuite que le noyau de ϕ est forcément trivial, prouvant l'isomorphisme. Pour cela, on suppose qu'il existe un élément$(a_1, ..., a_n) \in \mathbb{Z}^d$ tel que $a_1g_1 + ...a_ng_n = 0$ et on montre que cela implique qu'il existe un élément de torsion, contredisant l'hypothèse. Ce n'est pas trop compliqué mais nous ne donnerons pas les détails ici. □

On peut enfin combiner les deux théorèmes de classification des groupes en le théorème final :

Théorème 4.3.8 (Théorème de classifications des groupes abéliens finiment engendrés)**.** *Soit* G *un groupe abélien finiment engendré. Alors*

$$G \cong \mathbb{Z}^r \times \bigotimes_i \mathbb{Z}_{p_i^{n_i}},$$

où les p_i *sont des premiers,* $n_i \in N$ *et* $r \in \mathbb{N}$.

La preuve de ce théorème repose sur la décomposition entre la partie de torsion de G et la partie sans torsion. Comme G est abélien, la torsion T est un sous-groupe normal et il suffit donc de décomposer G/T, qui est un sous-groupe de G sans torsion.

Pour trouver cette décomposition, il existe une technique basée sur des méthodes d'algèbre linéaire : la forme normale de Smith. C'est une sorte d'élimination de Gauss avec des coefficients dans $\mathbb{Z}$ (qui n'est pas un corps).

Définition 4.3.9. *Soient $A, B \in M_{n\times m}(\mathbb{Z})$. On dit que A et B sont* équivalentes *s'il existe $P \in M_{m\times m}(\mathbb{Z})$ et $Q \in M_{n\times n}(\mathbb{Z})$, inversibles sur $\mathbb{Z}$, i.e. de déterminant ± 1, tel que $B = Q^{-1}AP$.*

Théorème 4.3.10 (Forme normale de Smith)**.** *Soit $A \in M_{n\times m}(\mathbb{Z})$. Alors A est équivalente à une matrice D où $d_{ij} = 0$ si $i \neq j$ et si $d_i = d_{ii}$, on a*

- *$d_i \neq 0$ pour $1 \leq i \leq r = rang(A)$,*
- *$d_k = 0$ pour $k > r$,*
- *$d_i | d_{i+1}$ pour $1 \leq i \leq r-1$.*

$$D = \begin{pmatrix} d_1 & & & & & & \\ & d_2 & & & & & \\ & & \ddots & & & & \\ & & & d_r & & & \\ & & & & 0 & & \\ & & & & & \ddots & \\ & & & & & & 0 \end{pmatrix}$$

Démonstration. Si $A = 0$ on peut prendre Q, P les matrices identités. Supposons $A = (a_{kl})$ non nuls. Soient i, j tel que $0 \neq |a_{ij}|$ est minimal. Les opérations élémentaires sur les lignes et les colonnes de A qui sont inversibles sur $\mathbb{Z}$ sont :

- les matrices qui permutent lignes/colonnes (car elles sont de déterminant ± 1).
- les matrices qui additionnent un multiple d'une ligne/colonne à une autre ligne/colonne (car elles sont de déterminant 1).

On permute les lignes et colonnes de A pour placer a_{ij} dans la composante $(1,1)$. On a $(a_{11}) \neq 0$ et de valeur absolue minimale. Pour $k > 1$, si $a_{1k} \neq 0$, par l'algorithme d'Euclide, il existe $b_k, b_{1k} \in \mathbb{Z}$ tel que $a_{1k} = a_{11}b_k + b_{1k}$ et $|b_{1k}| < |a_{11}|$. On multiplie à droite par une matrice élémentaire pour soustraire de la k-ième colonne $a_{11}b_k$. Si $b_{1k} \neq 0$ on recommence le processus. On obtient finalement une matrice de la forme

$$\left(\begin{array}{cccc} a'_{11} & b'_{12} & \cdots & b'_{1m} \\ \hline * & * & \cdots & * \\ * & * & \cdots & * \\ * & * & \cdots & * \\ * & * & \cdots & * \\ * & * & \cdots & * \end{array}\right)$$

avec $a'_{11} \mid b'_{1k}$, pour tout k. Ensuite on utilise a'_{11} pour éliminer b'_{1k}. On fait de même pour la première colonne et on obtient la forme suivante :

$$\left(\begin{array}{c|ccc} p_{11} & 0 & \cdots & 0 \\ \hline 0 & & & \\ \vdots & & C & \\ 0 & & & \end{array}\right)$$

Si $p_{11} \mid c_{ij}$, pour tout i, j, on repète la procédure avec la matrice C. Si p_{11} ne divise pas c_{ij} pour un certain c_{ij}, on remplace la ligne 1 par ligne 1 + ligne i. On répète, on obtient une matrice

$$\left(\begin{array}{c|ccc} f_{11} & 0 & \cdots & 0 \\ \hline 0 & & & \\ \vdots & & D & \\ 0 & & & \end{array}\right)$$

où f_{11} divise tous les d_{ij}. On repète la procédure avec la matrice D.

□

Une matrice équivalente à A dans une forme "diagonale" comme dans le résultat précédent est une *forme normale* pour A et les éléments $d_1, \ldots, d_r$ s'appellent un

ensemble de facteurs invariants de A. Ils sont en fait déterminés au signe près.
On peut maintenant re-énoncer le théorème de classification des groupes abéliens finiment engendrés :

Théorème 4.3.11. *Soit G un groupe abélien de type fini. Alors*

$$G \cong \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_s\mathbb{Z}$$

où $d_1\mathbb{Z} \subseteq d_2\mathbb{Z} \subseteq \cdots \subseteq d_s\mathbb{Z}$ *et* $d_i\mathbb{Z} \neq \mathbb{Z}$ *pour tout i. Si* $d_i = \{0\}$ *pour* $t < i \leq s$, *et* $d_i \neq \{0\}$ *pour* $i \leq t$, *on a*

$$G \cong \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_t\mathbb{Z} \times \mathbb{Z}^{(s-t)}$$

Démonstration. Soient $x_1, \ldots, x_n$ un ensemble de générateurs pour G. On a un homomorphisme surjectif

$$\begin{array}{rccc} \varphi : & \mathbb{Z}^n & \to & G \\ & (a_1, \ldots, a_n) & \mapsto & a_1x_1 + \cdots + a_nx_n. \end{array}$$

Par le premier théorème d'isomorphisme, $G \cong \mathbb{Z}^n / \operatorname{Ker}(\varphi)$.

Posons $K = \operatorname{Ker}(\varphi)$. Soient $\{f_1, \ldots, f_m\}$ un ensemble de générateurs de K et $\{e_1, ..., e_n\}$ des générateurs de $\mathbb{Z}^n$ où $e_i = (0, \ldots 0, 1, 0, \ldots 0)$. On a $f_j = \sum_{i=1}^n a_{ij}e_i$. Soit $A = (a_{ij}) \in M_{n\times m}(\mathbb{Z})$. Soient $Q \in M_{n\times n}(\mathbb{Z}), P \in M_{m\times m}(\mathbb{Z})$ inversibles sur $\mathbb{Z}$ tel que $Q^{-1}AP$ soit une forme normale de A.

$$Q^{-1}AP = \begin{pmatrix} d_1 & & & & & & \\ & d_2 & & & & & \\ & & \ddots & & & & \\ & & & d_r & & & \\ & & & & 0 & & \\ & & & & & \ddots & \\ & & & & & & 0 \end{pmatrix}$$

On "remplace" $\{e_1, \ldots, e_n\}$, $\{f_1, \ldots, f_m\}$ par $\{e'_1, \ldots, e'_n\}$, $\{f'_1, \ldots, f'_m\}$ donnés par $e'_j = \sum_{i=1}^n q_{ij}e_i$, $f'_j = \sum_{i=1}^m p_{ij}f_i$ et on a $f'_j = \sum_{i=1}^n (Q^{-1}AP)_{ij}e'_i$. Donc on a que $f'_j = d_je'_j$ pour tout$j \leq r$ et $f'_k = 0$ pour $k \geq r + 1$.

Revenons à $G \cong \mathbb{Z}^n / \operatorname{Ker}(\varphi)$. Posons $y_i = \varphi(e'_i) \in G, 1 \leq i \leq n$. On montre que $G \cong \mathbb{Z}y_1 \times \cdots \times \mathbb{Z}y_n$. Il faut montrer que

— $G = \langle \mathbb{Z}y_1, \ldots, \mathbb{Z}y_n \rangle$

— $\mathbb{Z}y_j \cap \langle y_i \mid i \neq j \rangle = \{0\}$

Les $\{y_i \mid 1 \leq i \leq n\}$ engendrent G car Q est une matrice inversible. Supposons que $\sum b_i y_i = 0$ pour certains $b_i \in \mathbb{Z}$, alors

$$\sum_{i=1}^{n} b_i \varphi(e'_i) = 0 \Rightarrow \varphi(\sum_{i=1}^{n} b_i e'_i) = 0 \Rightarrow \sum b_i e'_i \in \operatorname{Ker}(\varphi) = K$$

donc

$$\sum_{i=1}^{n} b_i e'_i = \sum_{j=1}^{m} c_j f'_j = \sum_{j=1}^{m} c_j d_j e'_j \Rightarrow b_i = c_i d_i, i \leq r \text{ et } b_i = 0$$

pour $i > r$. Pour $i \leq r$, on a $b_i y_i = c_i d_i y_i$ et

$$d_i y_i = d_i \varphi(e'_i) = \varphi(d_i e'_i) = \varphi(f'_i) = 0$$

car $f'_i \in \operatorname{Ker}(\varphi)$. On a ainsi que $b_i y_i = 0$. Ceci montre que $\mathbb{Z}y_j \cap \langle y_i \neq j \rangle = \{0\}$ et ainsi $G \cong \mathbb{Z}y_1 \times \cdots \times \mathbb{Z}y_r$. Il reste à voir que pour chaque $i \leq r, \mathbb{Z}y_i \cong \mathbb{Z}/d_i\mathbb{Z}$. On définit pour tout i

$$\begin{array}{rccc} \psi : & \mathbb{Z} & \to & \mathbb{Z}y_i \\ & l & \mapsto & ly_i. \end{array}$$

ψ est un homomorphisme surjectif. Par définition $\operatorname{Ker}(\psi) = \{l \in \mathbb{Z} | ly_i = 0\}$.

— Si $i \leq r$: soit $l \in \operatorname{Ker}(\psi)$, alors

$$0 = ly_i = l\varphi(e'_i) = \varphi(le'_i)$$

et donc $le'_i \in \operatorname{Ker}(\varphi)$. Comme avant on déduit que $d_i | l$. Donc $\operatorname{Ker}(\psi) \subseteq d_i\mathbb{Z}$. On avait déjà vu que $d_i y_i = 0$. Donc $d_i\mathbb{Z} \subseteq \operatorname{Ker}(\psi)$. Ainsi $\operatorname{Ker}(\psi) = d_i\mathbb{Z}$ et $\mathbb{Z}/d_i\mathbb{Z} \cong \mathbb{Z}y_i$.

— Si $i \geq r+1$, soit $l \in \operatorname{Ker}(\varphi)$ et on obtient $le'_i \in \operatorname{Ker}(\varphi)$ mais $\operatorname{Ker}(\varphi) = \langle d_1 e'_1, \ldots, d_r e'_r \rangle$ et donc $l = 0$. Ainsi $\operatorname{Ker}(\psi) = \{0\}$ et $\mathbb{Z} \cong \mathbb{Z}y_i$.

Par conséquent on a $G \cong \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_r\mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z}$.

□

Remarque 4.3.12. *La suite d'entiers strictement plus grand que 1,* $|d_1|, \ldots, |d_s|$ *est uniquement déterminée, c'est à dire, si* G_1, G_2 *sont des groupes abéliens de type fini avec*

$$G_1 \cong \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_s\mathbb{Z}$$

où $d_1\mathbb{Z} \supseteq d_2\mathbb{Z} \supseteq \cdots \supseteq d_s\mathbb{Z}$*, et*

$$G_2 \cong \mathbb{Z}/a_1\mathbb{Z} \times \cdots \times \mathbb{Z}/a_t\mathbb{Z}$$

où $a_1\mathbb{Z} \supseteq a_2\mathbb{Z} \supseteq \cdots \supseteq a_t\mathbb{Z}$*, alors* $G_1 \cong G_2$ *si et seulement si* $t = s$ *et* $|d_i| = |a_i|$ *pour tout* i *(découle de l'unicité des facteurs invariants dans la matrice). Les entier* $|d_i| > 1$ *s'appellent les* facteurs invariants *du groupe* G*.*

Chapitre 5

Groupes et isométries

Dans ce dernier chapitre, nous allons aborder la théorie des groupes dans un contexte plus géométrique : les isométries. En fait, l'étude de toute géométrie, comme par exemple la géométrie euclidienne que vous avez déjà étudiée, revient à analyser les actions d'un groupe G sur un ensemble X et les propriétés invariantes de cette action. Par exemple, en géométrie euclidienne on considère $X = \mathbb{R}^2$ et $G = \mathsf{Isom}(\mathbb{R}^2)$, l'ensemble des isométries euclidiennes (les applications qui préservent la distance euclidienne). En géométrie sphérique, on considère $X = S^2$, la sphère, et $G = O(3)$, les matrices orthogonales dans $\mathbb{R}^3$. Une géométrie correspond donc une action de groupe G sur un ensemble X. Plus le groupe est gros, moins il a de notions invariantes, qui correspondent aux notions géométriques. La théorie des groupes est donc très importante en géométrie aussi.

5.1 Isométries

On va commencer par rappeler des notions de base sur les distances.

5.1.1 Espaces métriques

Définition 5.1.1. Un ensemble non vide E est un *espace métrique* s'il est muni d'une application symétrique $d : E \times E \to \mathbb{R}_+$ telle que $d(x, y) = 0$ si et seulement si $x = y$ et qui vérifie l'inégalité triangulaire

$$d(x, y) \leq d(x, z) + d(y, z) \text{ pour tout } x, y, z \in E.$$

On appelle cette application une *distance* ou une *métrique*.

Exemple 5.1.2. *On prend un ensemble quelconque $E \neq \emptyset$. On définit : $d(a,b) = 0$ si $a \neq b$ et $d(a,b) = 1$ si $a = b$. Alors (E,d) est un espace métrique, appelé l'espace métrique discret. (Exercice)*

Il y a diverses manières de définir des distances. L'une est de définir la distance directement, comme la distance euclidienne que nous connaissons déjà. Une autre manière de définir une distance à partir d'une norme :

Définition 5.1.3. *Soit E un espace vectoriel sur $\mathbb{R}$. Une application $\| \cdot \| : E \longrightarrow \mathbb{R}$ est une* norme *si elle satisfait les conditions suivantes :*

- $\| a \| \geq 0$ *si et seulement si* $a = 0$ *(positivité),*
- $\| \lambda a \| = | \lambda | \| a \|$ *(homogénéité absolue),*
- $\| a + b \| \leq \| a \| + \| b \|$ *(inégalité triangulaire),*

pour tout $\lambda \in \mathbb{R}, a, b \in E$.

La fonction $d : E \times E \longrightarrow \mathbb{R} : d(a,b) = \| a - b \|$ définit une distance sur E, on a donc un espace métrique (Exercice). Notons qu'une norme est définie sur un espace vectoriel, alors qu'une distance peut être définie sur un ensemble quelconque.

Nous connaissons déjà quelques normes : par exemple, la norme euclidienne dans $\mathbb{R}^2$, $\| x \| = \sqrt{x_1^2 + x_2^2}$. Nous allons voir maintenant que certaines normes viennent d'un *produit scalaire*, dont on rappelle la définition :

Définition 5.1.4. *Soit E un espace vectoriel. Un produit scalaire $\langle \cdot, \cdot \rangle : E \times E \longrightarrow \mathbb{R}$ est une application qui symétrique, positive et linéaire en chacune de ces composantes :*

- $\langle a, b \rangle = \langle b, a \rangle$ *(symétrie),*
- $\langle a, b \rangle \geq 0$ *(positivité),*
- $\langle \lambda a + \mu b, c \rangle = \lambda \langle a, c \rangle + \mu \langle b, c \rangle$ *(linéarité),*

pour tout $a, b, c \in E, \lambda, \mu \in \mathbb{R}$. Un espace vectoriel E muni d'un produit scalaire est appelé un espace préhilbertien.

Vous étudierez les produits scalaires plus en détails dans le cours d'Algèbre linéaire II.

Remarque 5.1.5. *On peut remarquer que la linéarité de la deuxième composante découle de la symétrie et de la linéarité en la première composante.*

Exemple 5.1.6. *Nous connaissons déjà le produit scalaire usuel sur $\mathbb{R}^n$, défini de la manière suivante : $\langle u, v\rangle := \sum_{i=1,...n} u_i v_i$. On rappelle également que*

$$\langle x, y\rangle = \| x \| \| y \| \cos(\theta),$$

où θ est l'angle entre x et y.

Remarque 5.1.7. *Soit A une matrice n par n. On a, par définition du produit scalaire, $\langle Ax, y\rangle = \langle x, A^T y\rangle$.*

A partir d'un produit scalaire, on peut définir une norme de la manière suivante : la norme de $a \in E$ est $\sqrt{\langle a, a\rangle}$. Cela nous définit donc également une métrique sur E.

Pas toutes les distances viennent de normes (par (contre-)exemple : la métrique discrète), et pas toutes les normes sont engendrées par des produits scalaires. Nous allons également voir un contre-exemple mais ne le démontrerons pas.

On a : Produit scalaire $\rightsquigarrow$ Norme $\rightsquigarrow$ Distance, mais pas les réciproques.

Dans $\mathbb{R}^n$, on peut définir plusieurs types de normes, dont certaines se révèlent utiles pour certains types d'applications (en optimisation par exemple).

Définition 5.1.8. *Soit $p \in \mathbb{N}$. On définit la norme $\| \cdot \|_p$ comme :*

$$\| x \|_p = \sqrt[p]{\sum |x_i|^p}$$

et $\| \cdot \|_\infty$ via

$$\| x \|_\infty = \sup\{|x_i|\},$$

pour $x = (x_1, ...x_n) \in \mathbb{R}^n$.

On remarque que lorsque $p = 2$ on obtient la distance euclidienne. Le cas $p = 1$ définit la distance de Manhattan, aussi appelée en français la "distance du chauffeur de taxi de New-York". Les cas $p = 1$ et $p = \infty$ ne viennent pas d'un produit scalaire. En fait, cette norme $\| \cdot \|_p$ n'est engendrée par un produit scalaire que si $p = 2$.

Définition 5.1.9. *Pour une norme $\| \cdot \|$, on définit la boule de centre x et de rayon r de cette norme comme*

$$B_r(x) = \{y \in E \mid \| x - y \| \leq r\}.$$

5.1.2 Groupes d'isométries d'un espace métrique

Une isométrie est une application qui préserve les distances. Plus formellement,

Définition 5.1.10. *Soit (X, d) un espace métrique. Une isométrie sur X est une application bijective $f : X \longrightarrow X$ telle que $d(f(x), f(y)) = d(x, y)$ pour tout $x, y \in X$. On note $\mathsf{Isom}(X)$ l'ensemble des isométries de X.*

Par définition, $\mathsf{Isom}(X)$ est un sous-groupe de $Bij(X)$. Notons qu'une application qui préserve les distances est nécessairement injective. En effet, $f(x) = f(y) \Leftrightarrow d(f(x), f(y)) = 0 \Leftrightarrow d(x, y) = 0 \Leftrightarrow x = y$.

Pour un espace métrique X quelconque, $\mathsf{Isom}(X)$ forme un groupe qui agit fidèlement sur X (Exercice).

Exemple 5.1.11. *1. Soit X un ensemble quelconque muni de la métrique discrète.*

$$\mathsf{Isom}(X) = \{f : X \longrightarrow X \text{ bijective } \mid d(x, y) = d(f(x), f(y)\ \forall x, y \in X\}$$

$$= \{f : X \longrightarrow X \text{ bijective } \} = Bij(X),$$

car toute application injective préserve la métrique discrète. La seule information conservée par la métrique discrète est "deux points sont-ils confondus".

2. Considérons $X = \{0, 1, 3\} \subseteq \mathbb{R}$ muni de la métrique induite par la distance euclidienne sur $\mathbb{R}$. Alors (Exercice)

$$\mathsf{Isom}(X) = \{f : X \longrightarrow X \text{ bijective } \mid d(x, y) = d(f(x), f(y)\ \forall x, y \in X\} = \{Id_X\}.$$

Malheureusement, la classification complète des isométries de $\mathbb{R}^n$ pour la distance euclidienne nous prendrait trop de temps à couvrir en un seul chapitre. Nous allons donc devoir énoncer quelques propositions sans preuves.
Pour rappel, $M \in O(n)$ satisfait $\det(M) = \pm 1$ et $M^{\mathrm{T}} = M$.

Proposition 5.1.12. *Soit $f : \mathbb{R}^n \longrightarrow \mathbb{R}^n$ une application linéaire de $\mathbb{R}^n$ et A la matrice correspondant à f. Alors f est une isométrie si et seulement si $A^T A = I$.*

Démonstration. Une application linéaire de $\mathbb{R}^n$ préserve les distances si et seulement si elle préserve le produit scalaire. En effet, si f est linéaire et préserve les distances, en particulier

$$d(f(x), 0) = d(f(x), f(0)) = d(x, 0),$$

donc $\| f(x) \| = \| x \|$. De plus,

$$\langle x+y, x+y \rangle = \| x+y \|^2 = \| f(x+y) \|^2 = \| f(x)+f(y) \|^2 = \langle f(x)+f(y), f(x)+f(y) \rangle,$$

car f est linéaire. En développant les deux côtés de cette égalité on obtient

$$\| x \|^2 + 2\langle x, y \rangle + \| y \|^2 = \| f(x) \|^2 + 2\langle f(x), f(y) \rangle + \| f(y) \|^2,$$

d'où $\langle x, y \rangle = \langle f(x), f(y) \rangle$. La réciproque est vraie aussi, si f préserve le produit scalaire, alors forcément elle préserve la distance induite par le produit scalaire.
Pour finir, on montre que f préserve le produit scalaire si et seulement si $A^T A = I$. Supposons donc que $\langle x, y \rangle = \langle f(x), f(y) \rangle = \langle Ax, Ay \rangle = \langle x, A^T Ay \rangle$. En prenant $x = y$, on obtient

$$\| x \|^2 = \| x \| \| A^T Ax \| \cos\theta = \| x \|^2,$$

car si A est une isométrie, alors A^T l'est aussi. Ainsi, l'angle θ entre x et $A^T Ax$ est 0, donc $A^T Ax = x$.
Si $A^T A = I$, alors $\langle x, y \rangle = \langle x, A^T Ay \rangle = \langle Ax, Ay \rangle$, et A est une isométrie. □

On appelle un élément de $O(n)$ une *isométrie linéaire*. Par exemple, dans $\mathbb{R}^2$, $O(2)$ consiste en l'ensemble des rotations et réflexions par un axe passant par l'origine.

Corollaire 5.1.13. *Toute isométrie f de $\mathbb{R}^n$ peut s'écrire de manière unique comme $f = \tau_v \circ \alpha$, où τ_v est une translation par un vecteur $v \in \mathbb{R}^n$ ($\tau_v(x) = x+v$) et $\alpha \in O(n)$ est une isométrie linéaire.*

Si $f = \tau_v \circ \alpha$ avec $\alpha \in SO(n)$, c'est-à-dire que $\det(\alpha) = +1$, on dit que f est une isométrie qui *préserve l'orientation*. L'ensemble de ces isométries est dénoté $\mathsf{Isom}^+(\mathbb{R}^n)$. Par exemple, toute matrice $M \in SO(2)$ peut s'écrire sous la forme

$$\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$

pour $\theta \in [0, 2\pi)$ un angle. Donc l'ensemble des isométries linéaires de $\mathbb{R}^2$ qui préservent l'orientation est l'ensemble des matrices qui s'écrivent comme ci-dessus.

Une application $f : \mathbb{R}^n \longrightarrow \mathbb{R}^n$ telle que $f = \tau_v \circ \alpha$ où τ_v est une translation et $\alpha \in GL_n(\mathbb{R})$ est appelée une *application affine*. Un *sous-espace affine* de $\mathbb{R}^n$ est

un ensemble E de la forme $\tau_v(W)$, où W est un sous-espace vectoriel. La proposition suivante donne une propriété des applications affines qui permettra de décrire explicitement les isométries de $\mathbb{R}^n$.

Proposition 5.1.14. *Soit $f : \mathbb{R}^n \longrightarrow \mathbb{R}^n$ une application affine. Alors son ensemble de points fixes $Fix(f) = \{x \in \mathbb{R}^n \mid f(x) = x\}$ est soit vide, soit un sous-espace affine de $\mathbb{R}^n$.*

Démonstration. Exercice. □

L'ensemble des translations dans $\mathbb{R}^n$, $\{\tau_v \mid v \in \mathbb{R}^n\}$ est isomorphe à $\mathbb{R}^n$, car chaque translation ne dépend que du vecteur v et la structure de groupe est la même (Exercice). Puisque toute isométrie f de $\mathbb{R}^n$ s'écrit comme une composition d'une translation et d'un élément de $O(n)$, on aurait envie d'écrire $\mathsf{Isom}(\mathbb{R}^n) = \mathbb{R}^n \times O(n)$. Malheureusement, ce n'est pas le cas, les translations et les isométries linéaires ne commutent pas (voir l'exemple du groupe diédral dans l'exercice 3.3.2). Par contre, pour $\alpha \in O(n)$ et $\tau_v \in R^n$, on a la relation suivante :

$$\alpha^{-1} \circ \tau_v \circ \alpha = \tau_{\alpha(v)} \in \mathbb{R}^n.$$

Autrement dit, par le corollaire 5.1.13 et le fait que $\alpha^{-1} \circ \tau_v \circ \alpha = \tau_{\alpha(v)} \in \mathbb{R}^n$, on a $\mathsf{Isom}(\mathbb{R}^n) = \mathbb{R}^n \rtimes O(n)$. Le groupe des applications affines de $\mathbb{R}^n$ est isomorphe à $\mathbb{R}^n \rtimes GL_n(\mathbb{R})$.

Nous allons énoncer quelques théorèmes de classification des isométries de $\mathbb{R}$, $\mathbb{R}^2$ et $\mathbb{R}^n$, certains sans preuves. Pour cela, il nous faut d'abord la proposition suivante :

Proposition 5.1.15. *Soit $f : \mathbb{R}^n \longrightarrow \mathbb{R}^n$ une isométrie qui fixe un ensemble de points $E \in \mathbb{R}^n$. Alors f fixe le plus petit sous-espace affine de $\mathbb{R}^n$ contenant E.*

Démonstration. Exercice. □

En conséquence, si deux isométries f et g coincident sur un ensemble de points E, alors elles coincident en fait sur tout l'espace affine engendré par E. En effet, il suffit d'appliquer la proposition précédente à $f^{-1} \circ g$. Avec ce résultat, nous pouvons classifier les isométries de $\mathbb{R}^n$ en fonction de réflexions. Une réflexion dans $\mathbb{R}^n$ est une fonction qui inverse les deux côtés d'un hyperplan (sous-espace affine) de dimension $n - 1$. Par exemple, dans $\mathbb{R}$, une réflexion σ_x par $x \in \mathbb{R}$ (un point) s'écrit comme $\sigma_x(y) = 2x - y$. Dans $\mathbb{R}^2$, une réflexion par une droite l envoie un point x à distance d de l sur le point x' à equidistance de l mais de l'autre côté.

Théorème 5.1.16. *Toute isométrie de $\mathbb{R}$ est la composition d'au maximum deux réflexions. De plus, une isométrie de $\mathbb{R}$ est soit l'identité (aucune réflexion), une réflexion (une réflexion) ou une translation (deux réflexions).*

Démonstration. Si f a au moins 2 points fixes, alors $f = I$ (car f fixe aussi le sous-ensemble engendré par ces deux points, $\mathbb{R}$). Supposons que f a un unique point fixe x, on va vérifier que f est la réflexion σ_x. Soit $y \neq x$, et notons $d = d(x, y)$. Alors, $d(f(y), x) = d(f(y), f(x)) = d(y, x) = d$. Ainsi, $f(y)$ est à distance d de x aussi. Donc $f(y) = y$ ou $f(y) = \sigma_x(y)$. Mais comme f ne fixe qu'un point, $f(y) \neq y$, et donc $f = \sigma_x$.

Si f n'a aucun point fixe, il faut vérifier encore que f est une translation. Soit $x \in \mathbb{R}$ et $y = \frac{x+f(x)}{2}$. Soit $g = \sigma_y \circ f$. C'est une composition d'isométries, donc une isométrie. Puisque $g(x) = x$, g a un point fixe, donc g est soit l'identité, soit σ_x. Si $g = I$, on aurait $f = \sigma_y$ et y serait un point fixe de f. Donc $g \neq I$. Ainsi, $\sigma_y \circ f = \sigma_x$, et $f = \sigma_y \circ \sigma_x$, la composition de deux réflexions. Calculons finalement $\sigma_y \circ \sigma_x(z) = 2y - 2x + z = z + 2(y - x) = \tau_{2(y-x)}(z)$, une translation. □

Théorème 5.1.17. *Toute isométrie de $\mathbb{R}^2$ est une composition d'au maximum trois réflexions. Les isométrie de $\mathbb{R}^2$ sont : l'identité (aucune réflexion), les réflexions (une réflexion), les translations (deux réflexions d'axes parallèles), les rotations (deux réflexions d'axes non parallèles) et les réflexions glissées (troix réflexions), que vous avez appelées "renversements sans point fixe" en première année.*

De manière plus générale, toute isométrie de $\mathbb{R}^n$ est un produit d'au plus $n + 1$ réflexions.

5.2 Groupes de symétrie

La dernière partie de ce cours concerne les groupes de symétrie de sous-ensembles de $\mathbb{R}^n$.

Définition 5.2.1. *Soit $Y \subseteq \mathbb{R}^n$. Le* groupe des symétries *de Y est le groupe*

$$Sym(Y) = \{f \in \mathsf{Isom}(\mathbb{R}^n) \mid f(Y) = Y\},$$

les isométries qui fixent Y. L'ensemble des isométries qui préservent l'orientation et fixe Y est appelé le groupe de symétries propres,

$$Sym^+(Y) = \{f \in \mathit{Isom}^+(\mathbb{R}^n) \mid f(Y) = Y\}.$$

Exemple 5.2.2.
1. *Pour un objet pris "au hasard", les chances sont grandes que $Sym(Y) = \{Id\}$.*
2. *Soit Y une croix de type † dans $\mathbb{R}^2$. Son groupe de symétrie est $Sym(Y) \cong C_2$, car Y ne possède qu'une réflexion par l'axe vertical. Son groupe de symétries propres $Sym(Y) = \{I\}$, car la réflexion ne préserve pas l'orientation.*
3. *Si $Y = S^1$, le cercle unité, alors $Sym(Y) = O(2)$ et $Sym^+(Y) = SO(2)$.*

Pour terminer cette section, nous allons nous intéresser à un type de groupe de symétrie bien spécifique.

5.2.1 Groupes diédraux

Nous l'avons déjà mentionné plusieurs fois dans le cours. Le *groupe diédral* $D_{2\cdot n}$ est le groupe de symétrie d'un polygone régulier P_n à n sommets

$$\{e^{(2i\pi/n)k} \mid k = 0, ..., n\}.$$

Nous allons calculer ce groupe.

Soit $f \in \mathrm{Sym}(P_n)$. Alors $f = \tau_v \circ \alpha$, avec $v \in \mathbb{R}^2$ et $\alpha \in O(2)$ puisque f est une isométrie de $\mathbb{R}^2$. Par calcul, on peut vérifier que si $f(P_n) = P_n$, alors $f(0) = 0$ (il suffit de voir que $v = 0$). Donc toute symétrie de P_n fixe l'origine.
Pour simplifier les notations, appelons r la rotation d'angle $2\pi/n$ et s la réflexion par l'axe horizontal. Notons que $r, s \in O(2)$.
On va calculer l'ordre de $G = \mathrm{Sym}(P_n)$. On définit l'action $G \times P_n \longrightarrow P_n$ par : $g * x = g(x)$. Il s'agit bien d'une action car $I * x = I(x) = x$ et $(fg) * x = f(g(x)) = f(g * x)$, par définition. Elle n'est pas transitive, car tous les points de P_n ne s'ont pas à la même distance de l'origine, et les isométries préservent les longueurs. On ne peut donc pas trouver une isométrie qui envoie un des sommets de P_n sur un point au milieu d'un des côtés.
L'orbite de x correspond aux points de P_n qui sont à la même distance de l'origine

que x. En effet, il n'y a que ces points que l'on peut atteindre, et on les atteint tous à l'aide de rotations et de symétries par les sommets. Le stabilisateur d'un point est l'identité et la réflexion par l'axe passant par ce point, si elle existe (seulement pour les sommets de P_n ou les points au milieu d'une arrête). Par la formule des orbites, $|G| = |Stab(x)| \cdot |Orb(x)|$, pour n'importe quel $x \in P_n$. On choisit $x = 1$, on a vu que son stabilisateur contient 2 éléments (l'identité et la réflexion) et son orbite en contient n (les n sommets). On a donc $|G| = 2n$.
De plus, on vérifie que

$$sr^k s^{-1} = r^{-k}.$$

Ainsi, $\mathrm{Sym}(P_n) = C_n \rtimes C_2$, où $C_n = \{Id, r, ..., r^{n-1}\}$ et $C_2 = \{Id, s\}$.