THÉORIE DES GROUPES

Table des matières

Introduction 2
1. Premières propriétés 2
1.1. Définitions 2
1.2. Exemples et non-exemples 3
2. Sous-groupes, générateurs, ordre d'un élément 4
2.1. Sous-groupes 4
2.2. Exemples 6
2.3. Générateurs 6
2.4. L'ordre d'un élément 8
3. Morphismes de groupes 9
4. Les groupes symétriques 10
4.1. k-Cycles 10
4.2. La signature d'une permutation 13
4.3. Le groupe alterné 14
5. Morphismes et quotients 15
5.1. Rappel : Les relations d'équivalence 15
5.2. Classes modulo un sous-groupe 17
5.3. Théorème de nombre de classes et Théorème de Lagrange 18
5.4. Sous-groupes distinguées et le groupe quotient 19
6. Actions des groupes 22
6.1. Premières définitions et exemples 22
6.2. L'espace des orbites 23
7. Classification des groupes abéliens finis 26
7.1. Décomposition en p-groupes 26
7.2. Décomposition des p-groupes en produit des groupes cycliques. Facteurs invariants. 27

Introduction

En mathématique, un groupe est un ensemble muni d'une opération avec certaines propriétés, mimant l'ensemble des entiers relatifs avec l'additon. Il s'agit d'une structure algébrique fondamentale, qui joue un rôle central dans tous les domaines mathématiques, notamment en algèbre, en géométrie et en théorie des nombres, mais aussi en physique et en chimie par exemple.

Dans son sens mathématique, le terme *groupe* fut employé pour la première fois par le mathématicien français Évariste Galois dans les années 1830 dans son étude des équations polynomiales, pour se référer un certain ensemble de symétries des solutions des équations étudiées.

De façon générale, la principale source des groupes est donnée par les symétries de différents objets, très souvent géométriques. En effet, l'ensemble de transformations qui laissent une forme géométrique invariante, muni de l'opération de composition, forme un groupe. Par exemple le groupe diédral, qu'on va étudier plus tard, est donné par les symétries d'un carré. Un autre exemple d'un groupe est formé par toutes les manipulations possible d'un cube Rubik.

Il y a essentialement deux façons d'étudier les groupes. L'une, plus abstraite, consiste à "fragmenter" les groupes en des objets plus simples, tels que les *générateurs*, les *sous-groupes* et les *groupes quotients*, reliés par des *morphismes*. L'on étudie par la suite ceux-ci et, idéalement, l'on arrive à une classification abstraite de tous les élémenents simples qui participent à la construction d'un groupe. D'ailleurs, la classification des groupes finis dits *simples* a été finalisée en 2004, après des longs travaux dans les années 1950-1980.

Un autre moyen d'étudier les groupes, plus appliqué, consiste en les faire *agir* sur différents espaces, et d'obtenir ainsi différentes réalisations pour un même groupe en tant que groupes de symétries. Cette méthode aide en même temps à mieux comprendre l'espace sur lequel on agit et est à la base de la théorie des représentations.

Dans ce cours, on va donner les notions de base de la théorie des groupes, regarder de plus près les exemples les plus importants et faire les premiers pas vers les deux méthodes d'étude de groupes decrites ci-haut. A la fin, on va donner une esquisse de la classification des groupes abéliens.

1. Premières propriétés

1.1. **Définitions.**

Définition 1.1 — Un *groupe* $(G, \star)$ est la donnée d'un ensemble G et d'une loi de composition interne $\star$, c'est-à-dire d'une application

$$\begin{aligned} G \times G &\to G \\ (x, y) &\to x \star y, \end{aligned}$$

satisfaisant aux propriétés suivantes :

(A) *associativité :* $\forall x, y, z \in G$, on a $(x \star y) \star z = x \star (y \star z)$;

(B) existence d'un *élément neutre* $e \in G$: pour tout $x \in G$, on a $e \star x = x \star e = x$;

(C) tout élément dans G admet *un inverse* : pour tout $x \in G$, il existe $y \in G$ tel que $x \star y = y \star x = e$. On écrit x^{-1} pour l'inverse y de x.

Définition 1.2 — Deux éléments x, y d'un groupe $(G, \star)$ *commutent* si $x \star y = y \star x$. On dit qu'un groupe $(G, \star)$ est *commutatif* ou *abélien* si tous ses éléments commutent, i.e.

$$\forall x, y \in G, \quad x \star y = y \star x.$$

Dans ce cas, on dit aussi alors que la loi $\star$ est commutative (ou abélienne).

Remarque 1.3. *Un couple $(G, \star)$ formé par un ensemble et une opération satisfaisant seulement aux propriétés (A) et (B) est appelé monoïde. On a donc les relations d'inclusion :*

$$\textit{Groupes commutatifs} \subset \textit{Groupes} \subset \textit{Monoïdes}.$$

Définition 1.4 — Lorsque pour un groupe $(G, \star)$, G est un ensemble fini, le cardinal de G s'appelle l'*ordre* du groupe, noté aussi $|G|$. Si G n'est pas un ensemble fini, on dit que G est d'ordre infini.

Si $(G, \star)$ est un groupe fini et $G = \{e, g_1, \ldots, g_m\}$, on peut donner sa table de multiplication :

$\star$	e	g_1	$\cdots$	g_m
e	e	g_1	$\cdots$	g_m
g_1	g_1			
$\vdots$	$\vdots$		$g_i \star g_j$	
g_m	g_m			

où sur la i-ème ligne se trouvent les éléments de G multipliés par g_i à gauche, donc cette ligne contient chaque élément de G exactement une fois. De même la j-ème colonne contient tous les multiples à droite de g_j, et donc tous les éléments de G apparaissent exactement une fois dans cette colonne.

Proposition 1.5 — Soit $(G, \star)$ un groupe d'élément neutre e. Alors :

i. l'élément neutre est unique, i.e. si $e' \in G$ vérifie $x \star e' = e' \star x = x$ pour tout $x \in G$ alors $e' = e$;

ii. l'inverse d'un élément $x \in G$ est également unique, i.e. si $y', y \in G$ sont deux inverses de x dans G alors $y = y'$.

Démonstration. Pour $i.$: si $e' \in G$ est un élémentneutre, alors $e' = e' \star e = e$, où pour l'égalité de gauche on utilise le fait que e est élément neutre, et pour celle de droite on utilise le fait que e' est élément neutre.

Pour $ii.$: si $y, y' \in G$ sont des inverses de x, alors

$$x \star y = e = x \star y'.$$

En multipliant à gauche par y, on obtient que

$$y \star (x \star y) = y \star (x \star y').$$

Par associativité de la loi $\star$, on en déduit que

$$(y \star x) \star y = (y \star x) \star y',$$

et comme $y \star x = e$, on a

$$e \star y = e \star y',$$

d'où, comme e est élément neutre, $y = y'$. □

Notations et Conventions 1 — On utilise souvent aussi la notation $'\cdot'$ pour l'operation $\star$, et 1_G ou 1 pour l'élément neutre e. Parfois, quand la loi de composition est claire, pour simplifier la notation on parle du groupe G sans spécifier la loi de groupe $\star$, et on va écrire ab au lieu de $a \star b$ pour $a, b \in G$.
Quand le groupe est abélien, en analogie avec $(\mathbb{Z}, +)$ on va utiliser la notation $'+'$ au lieu de $\star$, 0_G ou 0 pour l'élément neutre e de G et $-x$ pour l'inverse x^{-1} d'un élémént $x \in G$.

Pour tout $x \in G$ et $n \in \mathbb{Z}$, $n > 0$, on note x^n l'élément $x^n = x \star \cdots \star x$ n-fois, $x^0 := e$ et pour $n < 0$, $x^n = x^{-1} \star \cdots \star x^{-1}$ $(-n)$-fois.

1.2. **Exemples et non-exemples.** Donnons ici quelques exemples, qu'il est bon de garder en mémoire pour tester des affirmations sur des cas particuliers.

(1) Si $(G, \star_G)$ et $(H, \star_H)$ sont deux groupes, alors le produit cartésien $G \times H$ l'est aussi pour la loi de composition interne donnée par $(g,h)\cdot(g',h') = (g \star_G g', h \star_H h')$ pour tous $((g,h),(g',h')) \in (G\times H)^2$.

(2) $(\mathbb{Z}, +)$ est l'exemple typique d'un groupe. L'élément neutre est 0 et pour tout $n \in \mathbb{Z}$, $-n$ est son inverse par rapport à $'+'$. De plus, $+$ est abélien. Pareil pour $(\mathbb{R}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{C}, +)$. Ceci sont des groupes d'ordre infini.

(3) Un **non-exemple** de groupe est $(\mathbb{N}, +)$. Dans ce cas, alors que $'+'$ reste associative est 0 est élément neutre, seul $0 \in \mathbb{N}$ a un inverse dans $\mathbb{N}$. Cependent, $(\mathbb{N}, +)$ est un monoïde.

(4) Pareil, $(\mathbb{Z}, \cdot)$, $(\mathbb{R}, \cdot)$ etc. ne sont pas groupes. Cependent, $(\{\pm 1\}, \cdot)$, $(\mathbb{R}^*, \cdot)$ sont des groupes commutatifs.

(5) $(\mathbb{Z}/n\mathbb{Z}, +)$ est le prototype de groupe abélien d'ordre fini n.

(6) L'ensemble $\mathrm{GL}_n(\mathbb{R})$ des matrices inversibles dans $M_n(\mathbb{R})$ avec la multiplication des matrices forme un groupe non-abélien, appelé *le groupe général linéaire*. Par exemple, pour $n = 2$,
$$\begin{pmatrix} 1 & 2 \\ 0 & 3 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 \\ 0 & 3 \end{pmatrix}.$$

(7) Soit X un ensemble non vide. Notons S_X l'ensemble des fonctions bijectives $f\colon X \to X$. La loi de composition $\circ : S_X \times S_X \to S_X$, $(f,g) \to f \circ g$ définit une loi de composition interne, généralement non-abélienne. L'élément neutre est donné par l'indentité id_X, est pour $f \in S_X$, l'inverse de f est la fonction réciproque $f^{-1} \in S_X$, qui existe puisque f est bijective.

Un cas spécial qu'on va étudier en detail est donné par $X = \{1, \dots, n\}$ pour un certain $n \in \mathbb{N}^*$ fixé. Dans ce cas, on denote le groupe aussi par $S_n = S_{\{1,\dots,n\}}$ (ou parfois même par Σ_n). Les éléments de S_n s'appellent des *permutations*, et le groupe S_n s'appelle le *groupe symétrique* d'ordre n ou bien *groupe des permutations*. On note la permutation σ par un tableau :
$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \cdots & \sigma(n) \end{pmatrix}.$$

Par exemple,
$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 3 & 1 & 4 \end{pmatrix} \in S_5,$$
denote la bijection $\sigma\colon \{1,\dots,5\} \to \{1,\dots,5\}$ définie par
$$\sigma(1) = 2, \sigma(2) = 5, \sigma(3) = 3, \sigma(4) = 1, \sigma(5) = 4.$$
On a
$$\sigma^2 := \sigma \circ \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 3 & 1 & 4 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 3 & 1 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 3 & 2 & 1 \end{pmatrix}$$
et $\sigma^4 = (\sigma^2)^2 = ... = 1$.

L'ordre, c'est-à-dire le cardinal, de S_n est $n!$: c'est le nombre de façons d'ordonner n éléments distincts. En effet, pour l'image de 1 on a n choix, pour l'image de 2 on a $n-1$ choix etc, et donc au total on a $n! = n \cdot (n-1) \cdot \cdots \cdot 2 \cdot 1$ choix.

Comme on va voir plus tard, les groupes d'ordre ≤ 5 sont tous abéliens. En même temps, S_3 est un groupe non-abélian d'ordre 6, c'est donc le "plus petit" exemple possible de groupe non-abélien.

2. Sous-groupes, générateurs, ordre d'un élément

2.1. **Sous-groupes.** Soit $(G, \cdot)$ un groupe d'élément neutre e.

Définition 2.1 — Soit H un sous-ensemble non-vide de G. H est un **sous-groupe** de G si H est stable par multiplication et par inverse, c'est-à-dire :

(A) $e \in H$;

(B) pour tout $x, y \in H$, on a $x \cdot y \in H$;

(C) pour tout $x \in H$, on a $x^{-1} \in H$.

Dans ce cas, on écrit $H < G$. On appelle le cardinal de H, noté par $|H|$, **l'ordre** du sous-groupe H.

On peut encoder les conditions d'être un sous-groupe d'une façon plus synthétique :

Proposition 2.2 — Soit $(G, \cdot)$ un groupe d'élément neutre e et soit H un sous-ensemble de G. Alors H est un sous-groupe de G ssi on a les deux propriétés :

I. $e \in H$;

II. $\forall x, y \in H$ on a $x \cdot y^{-1} \in H$.

Démonstration. □

On a encore une troisième façon de définir les groupes, plus naturelle mais moins pratique :

Proposition 2.3 — Soient $(G, \cdot)$ un groupe et H un sous-ensemble non-vide de G. Alors H est un sous-groupe de $(G, \cdot)$ ssi

(1) H est stable pour la lois $\cdot$, i.e. $\forall x, y \in H$, $x \cdot y \in H$, et

(2) $(H, \cdot)$ forme un groupe.

Démonstration. Notons avec e l'élément neutre de G. Supposons d'abord que H est stable pour $\cdot$ et que $(H, \cdot)$ est un groupe d'élément neutre e_H. On va montrer que celui-ci coincïde avec e, et que prendre les inverse dans G ou dans H revient au même.

Pour tout $x \in H$, puisque $x \in G$, on a, par la définition de e, mais aussi par définition de e_H :

$$x \cdot e = x = x \cdot e_H.$$

Cette relation vaut dans G. En multipliant à gauche par x^{-1} dans G, on obtient donc que $e = e_H$. En particulier, $e \in H$, i.e. on a montré la partie (A) de la définition d'un sous-groupe. La partie (B) est vérifiée par hypothèse. Quant à la partie (C), soient $x \in H$, $y = x^{-1} \in G$ l'inverse de x dans G, et $y' \in H$ l'inverse de x dans H. Alors on a $x \cdot y' = y' \cdot x = e$, donc l'unicité des inverses dans G (Prop. 1.5) implique que $y = y'$, et en particulier donc $y = x^{-1} \in H$, donc on a (C) est H est un sous-groupe.

Supposons maintenant que H est un sous-groupe de G, en particulier on a donc que H est stable pour $\cdot$. Puisque $\cdot$ est associative dans G, ça le reste dans H. Comme $e \in H$ par hypothèse, e est un élément neutre dans H. Comme pour tout $x \in H$, $x^{-1} \in H$, x admet un inverse dans H, donné précisément par x^{-1}. On a donc bien vérifié que $(H, \cdot)$ satisfait les propriétés d'un groupe. □

On a encore la propriété suivante :

Proposition 2.4 — L'intersection de deux sous-groupes de G est un sous-groupe. Plus généralement, une intersection non-vide quelconque $\cap_{i \in I} H_i$ de sous-groupes est encore un sous-groupe.

Démonstration. Soient H_1, H_2 deux sous-groupes de G. Alors $e \in H_1$ et $e \in H_2$ donc $e \in H_1 \cap H_2$. De plus pour $x, y \in H_1 \cap H_2$, on a $x, y \in H_1$ et $x, y \in H_2$ donc $xy^{-1} \in H_1$ et $xy^{-1} \in H_2$ d'où $xy^{-1} \in H_1 \cap H_2$, d'où le résultat. La généralisation se montre de la même manière. □

On a aussi une classe speciale des sous-groupes, dont l'utilité sera claire plus tard :

Définition 2.5 — Un sous-groupe $H < G$ s'appelle *distingué* ou *normal*, noté $H \lhd G$, si

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

Remarque 2.6. *Dans un groupe abelien, tout sous-groupe est normal.*

2.2. **Exemples.**

(1) Le sous-ensemble $\mathbb{Z}$ de $\mathbb{R}$ est un sous-groupe.

(2) Le sous-ensemble $\mathbb{N}$ de $(\mathbb{Z}, +)$ est stable pour $+$, mais n'est pas un sous-groupe.

(3) Pour $k \in \mathbb{Z}$ fixé, les multiples de k $H := \{km \mid m \in \mathbb{Z}\}$ forme un sous-groupe de $(\mathbb{Z}, +)$ -détails en TD.

(4) Pour $1 \leq k < n$, l'ensemble de permutations de S_n qui ne permutent que $\{1, \ldots, k\}$, i.e.
$$H = \{\sigma \in S_n \mid \sigma(l) = l \quad \forall k < l \leq n\}$$
forme un sous-groupe de $(S_n, \circ)$.

(5) Le *groupe special linéaire*
$$\mathrm{SL}_n(\mathbb{R}) := \{A \in \mathrm{GL}_n(\mathbb{R}) \mid \det A = 1\}$$
forment un sous-groupe de $(\mathrm{GL}_n(\mathbb{R}), \cdot)$.

2.3. **Générateurs.**

Définition 2.7 — Soit $(G, \cdot)$ un groupe et $S \subset G$ un sous-ensemble non-vide. On appèle **sous-groupe engendré par** S, noté $\langle S \rangle$, le plus petit sous-groupe de G qui contient S. Cela veut dire :

$$H < G, \quad S \subset H \Rightarrow \langle S \rangle \subseteq H.$$

Il n'est pas à priori clair que *le plus petit* tel sous-groupe existe, mais la proposition suivante nous donne l'existence, ainsi qu'une description explicite de $\langle S \rangle$.

Proposition 2.8 — Soit S un sous-ensemble non vide d'un groupe G. Alors on a :

$$\langle S \rangle = \bigcap_{\substack{S \subset H \\ H < G}} H.$$

De plus, tous les éléments de $\langle S \rangle$ sont de la forme

$$x_1 x_2 \cdots x_n \text{ avec } n \in \mathbb{N}^*, \text{ et } x_i \in S \text{ ou } x_i^{-1} \in S.$$

Démonstration. Notons avec $\mathcal{F} := \{H < G, S \subset H\}$ la famille des sous-groupes de G contenant S et avec $H_S := \bigcap_{H \in \mathcal{F}} H$. Comme $G \in \mathcal{F}$, l'intersection est non-vide, donc Prop. 2.4 implique que H_S est bien un sous-groupe de G. De plus, chaque sous-groupe dans l'intersection contient S, donc H_S aussi contient S. Finalement, si H_0 est un sous-groupe de G qui contient S, on a que $H_0 \in \mathcal{F}$ et donc

$$H_S = H_0 \cap \bigcap_{H \in \mathcal{F}} H \subset H_0$$

i.e. H_S est bien le plus petit sous-groupe contenant S, et donc $H_S = \langle S \rangle$.

Pour la deuxième partie, soit

$$G_S := \{x_1 x_2 \cdots x_n \mid n \in \mathbb{N}^*, \ x_i \in S \text{ ou } x_i^{-1} \in S\} \subset G.$$

Clairement G_S est stable par multiplication, par passage à l'inverse et contient l'élément neutre $e = gg^{-1}$ pour un $g \in S \neq \emptyset$. G_S est donc un sous-groupe de G et il contient S, on a donc que $\langle S \rangle \subset G_S$.

A son tour, $\langle S\rangle$ contient S par définition et quelque soient $n \in \mathbb{N}^*$ et $x_1, \dots, x_n \in S \subset \langle S\rangle$, on a que $x_1^{-1}, \dots x_n^{-1} \in \langle S\rangle$ et $x_1^{\pm 1} \cdots x_n^{\pm 1} \in \langle S\rangle$. On conclut que tout $g \in G_S$ appartient à $\langle S\rangle$, donc par double inclusion $G_S = \langle S\rangle$. □

Définition 2.9 — — Si $S = \{s_1, \dots, s_m\}$, on note aussi $\langle S\rangle = \langle s_1, \dots, s_m\rangle$.

— Si $G = \langle S\rangle$, on dit que G est **engendré par** S, et on appelle S **système de générateurs** pour G.

— Si il existe $x \in G$ tel que $G = \langle x\rangle$, on dit que G est **monogène**. Si de plus G est fini, on dit que G est **cyclique**.

— On dit que G est **finiment engendré** s'il existe un ensemble fini $S \subset G$ tel que $G = \langle S\rangle$.

Exemple 2.1 — (1) Tout groupe a un système de générateurs : l'ensemble des éléments de G en est un. Les systèmes de générateurs ne sont pas généralement uniques.

(2) $(\mathbb{Z}, +) = (\langle 1\rangle, +)$ est monogène, finiment engendré, mais pas fini. Un autre système de générateurs est donné par $S = \{2, 3\}$ - détails en TD.

(3) $\mathbb{Z} \times \mathbb{Z}$ est engendré par $(1, 0)$ et par $(0, 1)$, mais n'est pas monogène - détails en TD.

(4) $(\mathbb{Z}/n\mathbb{Z}, +) = (\langle \bar{1}\rangle, +)$ est cyclique.

Regardons de plus près le groupe monogène abélien $(\mathbb{Z}, +)$ et ses sous-groupes. Pour $n \in \mathbb{Z}$, notons $n\mathbb{Z} := \langle n\rangle$ le sous-groupe engendré par n. Alors on a :

Proposition 2.10 — (1) $n\mathbb{Z} = \{kn \mid k \in \mathbb{Z}\}$.

(2) Tout sous-groupe de $(\mathbb{Z}, +)$ est de la forme $n\mathbb{Z}$ pour un certain $n \in \mathbb{Z}$.

(3) Si a et b sont deux entiers avec $b \neq 0$, on a $b|a$ si et seulement si $a\mathbb{Z} \subset b\mathbb{Z}$.

(4) Pour $a, b \in \mathbb{Z}$, soient $d \in \mathbb{N}$ le PGCD de a et de b et $m \in \mathbb{N}$ le PPCM de a et de b. Alors on a

$$\langle a, b\rangle = d\mathbb{Z} \text{ et } a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}.$$

Démonstration. (1) Par Prop. 2.8 on a :

$$n\mathbb{Z} = \{an + b(-n) \mid a, b \in \mathbb{N}\} = \{(a - b)n \mid a, b \in \mathbb{N}\} = \{kn \mid k \in \mathbb{Z}\}$$

la dernière afirmation venant du fait que tout entier $k \in \mathbb{Z}$ est de la forme $a - b$ pour certains $a, b \in \mathbb{N}$.

(2) Soit H un sous-groupe de $(\mathbb{Z}, +)$. Si $H = \{0\}$, alors il est de la forme $0\mathbb{Z}$. Sinon, alors il existe $0 \neq k \in H$. On a que soit k, soit $-k \in H$ est un nombre positif, donc $H \cap \mathbb{N} \neq \{0\}$. Soit donc $n \in H$ le plus petit entier positif de H. On va montrer que $H = n\mathbb{Z}$. Comme n est un sous-groupe et que $n \in H$, on sait déjà que $n\mathbb{Z} \subset H$, reste donc a montrer l'autre inclusion.

Soit donc $m \in H$. La division euclidienne permet d'écrire $m = qn + r$ avec $q \in \mathbb{Z}$ et $r \in \mathbb{N}$, $0 \leq r < n$. Comme $qn, m \in H$, on a que $r = m - qn \in H$. Comme n est le plus petit élément posif de H, on obtient donc que $r = 0$, et donc $m|n$, i.e. $m \in n\mathbb{Z}$. On a donc montré que $H = n\mathbb{Z}$.

(3) Si $b|a$ alors il existe $l \in \mathbb{Z}$ avec $a = bl$, donc $a \in b\mathbb{Z}$. Comme de plus $b\mathbb{Z}$ est un sous-groupe, on a aussi que $a\mathbb{Z} = \langle a\rangle \subset b\mathbb{Z}$. Réciproquement, si $a\mathbb{Z} \subset b\mathbb{Z}$, alors $a \in b\mathbb{Z}$, donc il existe $l \in \mathbb{Z}$ tel que $a = bl$, donc on a bien $b|a$.

(4) On sait déjà que $\langle a, b\rangle$ et $\langle a\rangle \cap \langle b\rangle$ forment des sous-groupes de $\mathbb{Z}$, donc par (2), il existe d' et m' tel que

$$\langle a, b\rangle = d'\mathbb{Z}, \quad \langle a\rangle \cap \langle b\rangle = m'\mathbb{Z}.$$

Montrons que $d' = d$ et que $m' = m$.

D'une part on a :

$$a\mathbb{Z} \subset d'\mathbb{Z} = \langle a, b\rangle \text{ et } b\mathbb{Z} \subset d'\mathbb{Z} = \langle a, b\rangle \overset{(3)}{\Rightarrow} d'|a \text{ et } d'|b$$

donc d' est bien un diviseur commun de a et de b. D'autre part, si $k \in \mathbb{Z}$ est un diviseur commun de a et de b alors, par (3), on a que $a\mathbb{Z} \subset k\mathbb{Z}$ et $b\mathbb{Z} \subset k\mathbb{Z}$, d'où $a, b \in k\mathbb{Z}$, et donc $d'\mathbb{Z} = \langle a, b\rangle \subset k\mathbb{Z}$ ou encore, par (3), $k|d'$. Donc $d' = d$ est bien le plus petit diviseur de a et de b.

De façon similaire, puisque $m' \in a\mathbb{Z}$ et $m' \in b\mathbb{Z}$ on obtient par (3) que $a|m'$ et $b|m'$. De plus, si $q \in \mathbb{Z}$ est un multiple quelconque de a et de b, alors (3) implique que $q \in a\mathbb{Z}$ et $q \in b\mathbb{Z}$, donc $q \in a\mathbb{Z} \cap b\mathbb{Z} = m'\mathbb{Z}$, où encore $m'|q$. On en déduit que $m' = m$.

□

Corollaire 2.11 — (Bézout) Soient a et b deux entiers et soit d leur PGCD. Il existe des entiers u et v tels que $au + bv = d$.

Démonstration. C'est une reformulation de l'égalité $\langle a, b\rangle = d\mathbb{Z}$. □

2.4. **L'ordre d'un élément.**

Définition 2.12 — Soit $(G, \cdot)$ un groupe et $x \in G$. **L'ordre de** x est le cardinal du sous-groupe de G engendré par x :

$$\operatorname{ord} x := |\langle x\rangle|.$$

On dit que x est *ordre fini* si $\operatorname{ord} x \in \mathbb{Z}$, autrement on dit que x est d'ordre infini.

En pratique, on utilise le résultat suivant pour calculer l'ordre d'un élément :

Proposition 2.13 — Soit $(G, \cdot)$ un groupe et $x \in G$. Alors

$$\operatorname{ord} x = \inf\{d > 0 \mid x^d = e\}.$$

De plus, si $m \in \mathbb{Z}$ satisfait $x^m = e$ alors $\operatorname{ord} x|m$.

Démonstration. On se rappelle que $\langle x\rangle = \{x^d \mid d \in \mathbb{Z}\}$.

Cas 1 : $\operatorname{ord} x = \infty$. Comme $\langle x\rangle$ est infini, on va montrer que $x^d \neq e\ \forall d \in \mathbb{Z} - \{0\}$. En effet, supposons par contradiction qu'il existe $d \neq 0$ avec $x^d = e$, qu'on peut supposer positif. Pour tout $n \in \mathbb{Z}$, on fait la division euclidienne $n = qd + r$ avec $0 \leq r < d$ et on obtient

$$x^n = (x^d)^q \cdot x^r = x^r$$

donc $\langle x\rangle = \{e, x, \dots x^{d-1}\}$ est fini, contradiction. On obtient donc que $\inf\{d > 0 \mid x^d = e\} = \infty$.

Cas 2 : $\operatorname{ord} x = d \in \mathbb{N}$. Comme $\langle x\rangle$ est fini, il s'ensuit qu'il existe $1 \leq a < b$ tel que $x^a = x^b$. En multipliant avec $(x^{-1})^a$, on a qu'il existe $f = b - a > 0$ avec $x^f = e$. Soit donc $l > 0$ minimal avec la propriété $x^l = e$. On veut montrer que $\langle x\rangle = \{e, x, \dots, x^{l-1}\}$. En effet, on a d'une part $\{e, x, \dots, x^{l-1}\} \subset \langle x\rangle$. Réciproquement, soit $x^n \in \langle x\rangle$ avec $n \in \mathbb{Z}$. On raisonne comme avant : la division euclidienne $n = ql + r$ avec $0 \leq r < l$ donne $x^n = (x^l)^q \cdot x^r = x^r \in \{e, x, \dots, x^{l-1}\}$, donc on a bien l'égalité des deux ensembles. Cela implique $l = d$. En effet, sinon alors certaines puissances dans $\{e, x, \dots, x^{l-1}\}$ se répètent, i.e. $\exists 0 \leq a < b \leq l - 1$ avec $x^a = x^b$, ou encore $x^{b-a} = e$. Mais cela est impossible car $0 < b - a < l$ et l était minimal.

Finalement, supposons qu'il existe $m \in \mathbb{Z}$ avec $x^m = e$. Si $m = 0$, il n'y a rien à montrer, sinon on peut supposer que $m > 0$. Cela implique aussi que $d = \operatorname{ord} x$ est fini. Par ce qu'on a déjà montré, on a de plus $d \leq m$. La division euclidienne $m = dq + r$, $0 \leq r < d$ implique comme avant que $e = x^m = x^r$. Comme $d = \min\{l > 0 \mid x^l = e\}$ et $r < d$, on obtient que $r = 0$, i.e. $d = \operatorname{ord} x|m$.

□

Remarque 2.14. *Si G est un groupe fini, alors pour tout $x \in G$ on obtient $|\langle x \rangle| \leq G$, donc* $\mathrm{ord}(x)$ *est toujours fini.*

Exemple 2.2 — (1) $\operatorname{ord} x = 1 \Leftrightarrow x = e$.

(2) $\operatorname{ord} \bar{1} = 4$ et $\operatorname{ord} \bar{2} = 2$ dans $(\mathbb{Z}/4\mathbb{Z}, +)$.

(3) $\operatorname{ord} 2 = \infty$ dans $(\mathbb{Z}, +)$.

3. Morphismes de groupes

Comme en algèbre linéaire, il est temps de voir quelles sont les bonnes applications à considérér entre deux groupes : il faut qu'une telle application preserve les structures algébrique qu'on considère. C'est ce qu'on appelle un morphisme :

Définition 3.1 — Soit $(G, \star)$ et $(H, \cdot)$ deux groupes d'éléments neutres e_G et e_H respectivement.

1. Une application $\varphi\colon G \to H$ est dite un *morphisme* (ou un *homomorphisme*) *de groupes* si
$$\forall x, y \in G, \quad \varphi(x \star y) = \varphi(x) \cdot \varphi(y).$$
2. Un morphisme d'un même groupe $\varphi\colon G \to G$ est aussi dit *endomorphisme* du gorupe G.
3. Un morphisme bijectif de groupes est dit *isomorphisme*. Si de plus $G = H$, on utilise aussi le nom *automorphisme*.
4. Les groupes G et H sont dits *isomorphes* si il existe un isomorphisme $\varphi\colon G \to H$.

On a les propriétés importantes suivantes :

Proposition 3.2 — Soit $\varphi\colon G \to H$ un morphism de groupes. Alors on a :

a) $\varphi(e_G) = (e_H)$

b) $\forall g \in G$, $\varphi(g^{-1}) = \varphi(g)^{-1}$.

Proposition 3.3 — Si $\varphi\colon G \to H$ est un isomorphisme de groupes, alors l'application réciproque $\varphi^{-1}\colon H \to G$ est aussi un morphisme de groupe, et donc un isomorphisme.

Proposition 3.4 — La composition de deux morphismes de groupes est un morphisme de groupes. En particulier, pour un groupe G,
$$\mathrm{Aut}(G) = \{\varphi\colon G \to G \mid \varphi \text{ isomorphisme } \} \subset S(G)$$
forme un sous-groupe de $(S(G), \circ)$).

Deux groupes qui sont isomorphes ont les mêmes propriétés, de sorte qu'on va parfois jusqu'à les identifier. Par exemple, on a :

Proposition 3.5 — Soit $\varphi\colon G \to H$ un isomorphisme de groupes. Alors :

a) $|G| = |H|$

b) $\forall g \in G$, $\operatorname{ord} g = \operatorname{ord} \varphi(g)$.

c) G est cyclique ssi H est cyclique.

d) G est commutatif ssi H est commutatif.

A chaque morphisme de groupes $\varphi\colon G \to H$, on associe :

(1) *Le noyau* de φ : $\ker \varphi = \{x \in G \mid \varphi(x) = e_H\} = \varphi^{-1}(e_H) \subset G$;

(2) *L'image* de φ : $\operatorname{im} \varphi = \varphi(G) = \{\varphi(x) \mid x \in G\} \subset H$.

Ceci sont des sous-groupes dans les groupes respectifs. On a plus :

Proposition 3.6 — Si $\varphi\colon G \to H$ est un morphisme de groupes et $G' < G$, $H' < H$ sont des sous-groupes, alors $\varphi(G') < G$ et $\varphi^{-1}(H') < G$ sont aussi des sous-groupes. En particulier, $\ker\varphi$ et $\operatorname{im}\varphi$ sont des sous-groupes. De plus, $\ker\varphi$ est un sous-groupe distingué.

En pratique, l'enoncé ci-haut donne une façon rapide et facile de montrer que différents ensembles sont des sous-groupes, ou même des groupes.

Et comme pour les espaces vectoriels, on a :

Proposition 3.7 — Un morphisme de groupes $\varphi\colon G \to H$ est injectif ssi $\ker\varphi = \{e_G\}$.

Voici quelques exemples de morphismes et d'isomorphismes :

(1) Soit $(G, \star)$ un groupe et $g \in G$. L'application $\varphi_g\colon \mathbb{Z} \to G$, $n \to g^n$ est un morphisme des groupes. Elle est surjective précisément si $G = \langle g \rangle$, et elle est injective précisément si g est d'ordre infini.

(2) $\varphi\colon (\mathbb{Z}, +) \to (\mathbb{Z}, +)$, $x \mapsto 2x$ est un morphisme injectif.

(3) $\varphi\colon (\mathbb{R}, +) \to (\mathbb{R}_{>0}, \cdot)$ $x \mapsto \exp(x)$ est un isomorphisme.

(4) Pour chaque $n \in \mathbb{N}$, $n > 0$, $\pi\colon (\mathbb{Z}, +) \to (\mathbb{Z}/n\mathbb{Z}, +)$ est un morphisme surjectif de groupes.

(5) Si $(G, \cdot)$ est un groupe et $g \in G$, $C_g\colon G \to G$, $x \mapsto g^{-1} \cdot x \cdot g$ est un isomorphisme de G, appelé le morphisme de conjugaison par g - détails en TD.

(6) Si G et H sont deux groupes, alors les projections naturelles $G \times H \to G$ et $G \times H \to H$ sont des morphismes de groupes surjectifs.

4. Les groupes symétriques

Les groupes finis les plus importants sont les groupes symétriques. Cela vient du fait que tout groupe fini peut être réalisé comme sous-groupe d'un groupe symétrique. On pourraît donc dire que si on connaissait tous les sous-groupes des groupes symétriques, on connaîtrait tous les groupes finis (à isomorphisme près). Bien sûr, connaître tous les sous-groupes d'un groupe donné n'est absolument pas une tâche facile, mais cela motive notre étude qui suit.

On rappelle les définitions suivantes :

Définition 4.1 — Soit $n \in \mathbb{N}$. Le **groupe symétrique** S_n est l'ensemble de toutes les bijections de $\{1, \ldots, n\}$ avec la composition comme operation de groupe. Les éléments de S_n s'appellent **permutations**. On note la permutation σ par un tableau :

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

L'identité du groupe S_n est noté avec 1.

Remarque 4.2. *Tout groupe symétrique S_n s'injecte dans un groupe symétrique plus grand S_m, $m \geq n$, via le morphisme de groupes*

$$\varphi\colon S_n \to S_m, \quad \varphi(\sigma)(k) = \begin{cases} \sigma(k) & k \leq n \\ k & k > n \end{cases}.$$

4.1. k-Cycles.

Définition 4.3 — Soient $a_1, \ldots, a_k$ k éléments distincts de $\{1, \ldots, n\}$. Le **k-cycle** $(a_1, \ldots, a_k)$ est la permutation

$$(a_1, \ldots, a_k)\colon j \mapsto \begin{cases} a_{i+1} & j = a_i \text{ pour} 1 \leq i < k \\ a_1 & j = a_k \\ j & \text{sinon} \end{cases}.$$

On appelle k sa **longueur**.

Une **transposition** est un 2-cycle, i.e. une permutation qui échange exactement 2 éléments.

Remarque 4.4. *Dans la notation d'un k-cycle $(a_1, \dots, a_k)$, on peut échanger les éléments $a_1, \dots, a_k$ de façon cyclique, sans que la permutation elle-même change, i.e.*

$$(a_1, \dots, a_k) = (a_2, \dots, a_k, a_1) = (a_k, a_1, \dots, a_{k-1}) \text{ etc.}$$

De plus, on a :

$$(a_1, \dots, a_k)^{-1} = (a_k, \dots, a_1)$$

et

$$(a_1 \dots, a_k) = (a_1, a_2)(a_2, a_3) \dots (a_{k-1}, a_k). \tag{1}$$

En particulier, un k-cycle est un produit de $(k-1)$ transpositions.

On remarque que $(i,j)^2 = 1$, i.e. $(i,j)^{-1} = (i,j)$. Plus généralement, l'ordre d'un k-cycle est k.

Exemple 4.1 — Le groupes S_2 et S_3 contiennent seulement des cycles :

$$S_2 = \{1, (1,2)\}, \quad S_3 = \{1, (1,2), (1,3), (2,3), (1,2,3), (1,3,2)\}.$$

Dans S_4,

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

n'est pas un cycle, mais peut s'écrire comme produit des cycles : $\sigma = (1,4)(2,3)$.

Le support d'une permutation σ est donné par

$$\operatorname{supp}(\sigma) := \{i \mid \sigma(i) \neq i\}.$$

On a :

Lemme 4.5 — Si $\sigma, \tau \in S_n$ ont des supports disjoints, alors $\sigma\tau = \tau\sigma$. En particulier, tous deux cycles disjoints commutent.

Remarque 4.6. *La réciproque du lemme ci-haut est loin d'´être vrai : $\sigma = (1,2) = \tau$ ne sont pas à supports disjoints, cependent on a $\sigma\tau = \tau\sigma$.*

Définition 4.7 — On dit que deux permutations $\tau_1, \tau_2 \in S_n$ sont **conjuguées** s'il existe $\sigma \in S_n$ tel que $\tau_1 = \sigma\tau_2\sigma^{-1}$.

Lemme 4.8 — Soit $(a_1, \dots, a_k) \in S_n$ un k-cycle. Pour tout $\sigma \in S_n$ on a

$$\sigma \circ (a_1, \dots, a_k) \circ \sigma^{-1} = (\sigma(a_1), \dots, \sigma(a_k)).$$

Donc toute permutation conjuguée à un k-cycle est aussi un k-cycle.

Corollaire 4.9 — Pour tout k-cycle $\tau \in S_n$, il existe $\sigma \in S_n$ tel que $\sigma\tau\sigma^{-1} = (1, \dots, k)$. De plus, σ peut être choisi avec $\operatorname{supp}(\sigma) \subset \operatorname{supp}(\tau) \cup \{1, \dots, k\}$.

Démonstration. Pour un k-cycle $(a_1, \dots, a_k) \in S_n$, on choisit $\sigma \in S_n$ avec

$$\sigma(a_1) = 1, \dots, \sigma(a_k) = k$$

et on applique le lemme d'avant. □

Théorème 4.10. *Considérons le groupe S_n, $n \in \mathbb{N}$.*

(1) Toute permutation $\sigma \in S_n$ peut s'écrire comme un produit des cycles à supports disjoints, et cela de façon unique à l'ordre près. Les longueurs de ces cycles $k_1 \leq \dots \leq k_r$ forment une partition de n, dans le sens que $n = \sum_{i=1}^{r} k_i$, et on appelle $(k_1, \dots, k_r)$ le type de σ.

(2) Deux permutations de S_n sont conjuguées précisément quand elles ont le même type.

Démonstration. Soit $\sigma \in S_n$ et $a_0 \in \{1, \dots, n\}$. Considérons la suite :

$$a_0, \quad a_1 := \sigma(a_0), \dots, a_k = \sigma(a_{k-1}) = \sigma^k(a_0), \dots$$

Comme il s'agit d'une suite dans $\{1, \dots, n\}$, elle est forcément finie, il existe donc $k \geq 1$ minimal tel que $a_k = a_i \in \{a_0, \dots, a_k\}$ pour un certain $i \in \{0, \dots, k\}$. Si $i > 0$, alors on obtient

$$\sigma^k(a_0) = \sigma^i(a_0) \overset{\circ\sigma^{-i}}{\Longrightarrow} a_{k-i} = a_0$$

ce qui contredit la minimalité de k. On obtient donc que $a_k = a_0$ et que σ agit sur l'ensemble $\{a_0, \dots, a_{k-1}\}$ comme le k-cycle $(a_0, \dots, a_{k-1})$.

On raisonne maintenant par récurrence sur le cardinal $l \geq 0$ du support de σ . Pour $\sigma \in S_n$ avec $|\mathrm{supp}(\sigma)| = 0$ on a que $\sigma = 1$, donc il n'y a rien à montrer. Soit $l \in \mathbb{N}$ avec $1 \leq l < n$ fixé, et supposons que la propriété (1) soit verifiée pour toutes les permutations $\sigma \in S_n$ avec $|\mathrm{supp}(\sigma)| \leq l$. Montrons que cela est aussi le cas pour les permutations $\sigma \in S_n$ avec $|\mathrm{supp}(\sigma)| = l + 1$.

Soit donc $\sigma \in S_n$ avec $|\mathrm{supp}(\sigma)| = l + 1$, $a_0 \in \mathrm{supp}(\sigma)$ et $\tau = (a_0, \dots, a_{k-1})$ le k-cycle construit à partir de σ comme avant. En particulier, $\tau^{-1}\sigma(a_i) = a_i \ \forall i \in \{0, \dots, k-1\}$, donc $|\mathrm{supp}(\tau^{-1}\sigma)| < |\mathrm{supp}(\sigma)| = l+1$ et on peut appliquer l'hypothèse de récurrence à $\tau^{-1}\sigma$ pour obtenir une décomposition en cycles disjoints $\tau^{-1}\sigma = \tau_1 \cdots \tau_r$. On a montré donc que σ est un produit de cycles disjoints $\sigma = \tau\tau_1 \cdots \tau_r$.

Si $\sigma = \tau_1 \cdots \tau_r$ est une décomposition en cycles disjoints de longeurs $k_1, \dots, k_r$, alors chaque élément $l \in \{1, \dots, n\}$ se trouve dans le support d'exactement un des cycles $\tau_1, \dots, \tau_r$, déterminé de façon unique comme $(l = a_0, \sigma(l), \sigma^2(l) \dots)$. On a donc bien l'unicité des cycles, ainsi que $\sum_i k_i = n$.

Pour la partie (2), Lemme 4.8 montre que la conjugaison respecte le type d'une permutation. Réciproquement, il faut appliquer le Lemme 4.8 et son Corollaire 4.9 avec attention à chaque cycle de la décomposition d'une permutation, pour montrer que toute permutation de type $(k_1, \dots, k_r)$ est conjuguée à

$$(1, \dots, k_1)(k_1 + 1, k_1 + 2, \dots, k_1 + k_2) \cdots (\sum_{i=1}^{r-1} k_i + 1, \dots, n).$$

Ecrivons la preuve en détail pour un produit des deux cycles $\sigma = \tau_1\tau_2$ de type (k, l). Cor. 4.9 nous dis qu'il existe $\psi_1 \in S_n$ avec $\mathrm{supp}(\psi_1) \subset \mathrm{supp}(\tau_1) \cup \{1, \dots k\}$ t.q.

$$\psi_1\tau_1\psi_1^{-1} = (1, \dots, k) =: \tau_1'.$$

Soit aussi $\tau_2' := \psi_1\tau_2\psi_1^{-1}$. Comme τ_1, τ_2 sont à supports disjoints, Lemme 4.8 implique que leurs conjugués τ_1', τ_2' par ψ_1 le sont aussi, et donc $\mathrm{supp}(\tau_2') = \{k + 1, \dots, n\}$. On applique à nouveau Cor. 4.9 pour trouver $\psi_2 \in S_n$ avec $\mathrm{supp}(\psi_2) \subset \mathrm{supp}(\tau_2') \cup \{k + 1, \dots, n\} = \{k + 1, \dots, n\}$ et $\psi_2\tau_2'\psi_2^{-1} = (k + 1, \dots, n)$.

Posant $\psi := \psi_2\psi_1$ et utilisant que ψ_2 et $(1, \dots, k)$ sont à supports disjoints et donc commutent, on obtient

$$\begin{aligned}\psi\sigma\psi^{-1} &= \psi_2\psi_1\tau_1\psi_1^{-1}\psi_1\tau_2\psi_1^{-1}\psi_2^{-1} = \psi_2(1, \dots, k)\tau_2'\psi_2^{-1} \\ &= (1, \dots, k)\psi_2\tau_2'\psi_2^{-1} = (1, \dots, k)(k + 1, \dots, n).\end{aligned}$$

□

La formule (1), avec un peu plus de calculs (voir TD), nous donne :

Théorème 4.11. *Toute permutation de S_n est produit de transpositions. On a même plus : l'ensemble des transpositions $\{(i,i+1)|1\leq i<n\}$ forment un système de générateurs pour S_n.*

4.2. **La signature d'une permutation.**

Définition 4.12 — Soit $\sigma\in S_n$. **La signature** de σ est :

$$\operatorname{sign}(\sigma)=\prod_{1\leq i<j\leq n}\frac{\sigma(j)-\sigma(i)}{j-i}\in\mathbb{Q}.$$

Par exemple on calcule, dans S_n :

$$\begin{aligned}\operatorname{sign}(1,2)&=\frac{\sigma(1)-\sigma(2)}{1-2}\cdot\prod_{i=1,j>2}\frac{\sigma(1)-\sigma(j)}{1-j}\cdot\prod_{i=2,j>2}\frac{\sigma(2)-\sigma(j)}{2-j}\cdot\prod_{2<i<j\leq n}\frac{\sigma(i)-\sigma(j)}{i-j}\\&=\frac{2-1}{1-2}\cdot\prod_{j>2}\frac{2-j}{1-j}\cdot\prod_{j>2}\frac{1-j}{2-j}\cdot 1=-1.\end{aligned}$$

En général on a :

Théorème 4.13. *L'application signature définit un morphisme de groupes*

$$\operatorname{sign}:S_n\to\{\pm1\},\quad \sigma\mapsto\operatorname{sign}(\sigma).$$

Si $\tau=(a,b)\in S_n$ est une transposition, alors $\operatorname{sign}(\tau)=-1$. *Si τ est un k-cycle, alors* $\operatorname{sign}(\tau)=(-1)^{k-1}$.

Démonstration. Montrons tout d'abord que $|\operatorname{sign}(\sigma)|=1$ et donc que $\operatorname{sign}(\sigma)\in\{-1,1\}$. On a

$$|\operatorname{sign}(\sigma)|=\prod_{1\leq i<j\leq n}\frac{|\sigma(i)-\sigma(j)|}{|i-j|}=\frac{\prod_{1\leq i<j\leq n}|\sigma(i)-\sigma(j)|}{\prod_{1\leq i<j\leq n}|i-j|}.$$

D'autre part :

$$\{|\sigma(i)-\sigma(j)|,1\leq i<j\leq n\}=\{|i-j|,1\leq i<j\leq n\}$$

et ainsi $|\operatorname{sign}(\sigma)|=1$, ou encore $\operatorname{sign}(\sigma)\in\{\pm1\}$.

Montrons que sign est un morphisme de groupes. Soit $\sigma,\tau\in S_n$. On a

$$\operatorname{sign}(\sigma\circ\tau)=\prod_{1\leq i<j\leq n}\frac{\sigma\circ\tau(i)-\sigma\circ\tau(j)}{i-j}=\left(\prod_{1\leq i<j\leq n}\frac{\sigma(\tau(i))-\sigma(\tau(j))}{\tau(i)-\tau(j)}\right)\cdot\left(\prod_{1\leq i<j\leq n}\frac{\tau(i)-\tau(j)}{i-j}\right).$$

L'application $\{i,j\}\to\{\tau(i),\tau(j)\}$ étant une bijection de l'ensemble de paires $\{\{i,j\}\mid 1\leq i<j\leq n\}$, on obtient :

$$\operatorname{sign}(\sigma\circ\tau)=\left(\prod_{1\leq i<j\leq n}\frac{\sigma(i)-\sigma(j)}{i-j}\right)\cdot\left(\prod_{1\leq i<j\leq n}\frac{\tau(i)-\tau(j)}{i-j}\right)=\operatorname{sign}(\sigma)\operatorname{sign}(\tau).$$

Si $\tau=(1,2)$, on a déjà vu dans un calcul précédent que $\operatorname{sign}(1,2)=-1$. Sinon, par le Lemme 4.8, toute transposition $\tau=(a,b)$, $a<b$, est conjuguée à la transposition $(1,2)$. En effet, si $2<a<b$, on conjugue avec $\sigma=(2,b)(1,a)$ et on obtient

$$(2,b)(1,a)(1,2)(1,a)(2,b)=(a,b).$$

Si $a=1<2<b$, on prend plutôt $\sigma=(2,b)$, et si $a=2<b$ on prend $\sigma=(1,b)$. Comme sign est morphisme, on obtient dans tous les cas :

$$\operatorname{sign}(\tau)=\operatorname{sign}(\sigma)\operatorname{sign}(1,2)\operatorname{sign}(\sigma)^{-1}=\operatorname{sign}(1,2)=-1.$$

Finalement on déduit le résultat pour un k-cycle via la formule (1). □

On déduit immédiatement :

Corollaire 4.14 — Pour $\sigma \in S_n$ sont équivalents :

(1) σ est un produit pair de transpositions

(2) $\text{sign}(\sigma) = 1$.

4.3. **Le groupe alterné.**

Définition 4.15 — On dit qu'une permutation $\sigma \in S_n$ est **paire** si $\text{sign}(\sigma) = 1$, et **impaire** si $\text{sign}(\sigma) = -1$. **Le groupe alterné** est :

$$A_n := \{\sigma \in S_n \mid \sigma \text{ pair}\} = \ker(\text{sign}).$$

On remarque que A_n est un sous-groupe distingué de S_n.

Corollaire 4.16 — Si $\sigma \in S_n$ est de type $(k_1, \ldots, k_r)$, alors

$$\text{sign}(\sigma) = \prod_{i=1}^{r} (-1)^{k_i - 1}.$$

Donc σ est paire précisément quand elle a un nobre paire de cycles de longueurs paires dans sa décomposition en cycles disjoints.

Finalement, on a :

Proposition 4.17 — Une permutation $\sigma \in S_n$ est paire exactement si elle peut s'écrire comme produit de 3-cycles.

Démonstration. On doit montrer que tout élément $\sigma \in A_n$ est un produit de 3-cycles. D'après Théorème 4.11, il suffit de considérer les permutations de la forme $\sigma = (a\ b)(c\ d)$.

Cas $\{a, b\} = \{c, d\}$: On a $\sigma = 1$, donc un produit vide des 3-cycles.

Cas$\{a, b\} \cap \{c, d\} = \{b = c\}$: On peut écrire

$$(a\ b)(b\ d) = \begin{pmatrix} a & b & d \\ b & d & a \end{pmatrix} = (a\ b\ d).$$

Cas $\{a, b\} \cap \{c, d\} = \emptyset$: D'après le deuxième cas, on peut écrire

$$(a\ b)(c\ d) = (a\ b)(b\ c)(b\ c)(c\ d) = (a\ b\ c)(b\ c\ d).$$

Ceci montre l'assertion. □

Rappelons une utilisation importante du morphisme de signature :

Définition 4.18 — Le déterminant d'une matrice $A = (a_{ij}) \in M_n$ est

$$\det(A) = \sum_{\sigma \in S_n} \text{sign}(\sigma) \prod_{i=1}^{n} a_{\sigma(i),i}.$$

5. Morphismes et quotients

5.1. **Rappel : Les relations d'équivalence.** On commence par un rappel approfondi sur les relations d'équivalences et leur rapport aux partitions. Dans cette section, on fixe E un ensemble non-vide.

Définition 5.1 — On appelle **relation** sur E la donnée d'un sous-ensemble $R \subset E \times E$. On écrit xRy, et on dit que x est en relation avec y, si $(x, y) \in R$.

Une relation R sur E est dite **relation d'équivalence** si elle satisfait les trois propriétés suivantes :

(1) *réflexivité* : $\forall x \in E$, xRx ;

(2) *symétrie* : $\forall x, y \in E$, $xRy \iff yRx$;

(3) *transitivité* : $\forall x, y, z \in E$ si xRy et yRz, alors xRz.

On note souvent les relations d'équivalence avec le symbole $\sim$ (au lieu de R).

Exemple 5.1 — La relation d'égalité est une relation d'équivalence.

Pour $E = \mathbb{Z}$, $\leq$ définit est une relation

$$R = \{(x, y) \in \mathbb{Z}^2 \mid x \leq y\},$$

qui n'est pas une relation de s'équivalence : elle n'est pas symétrique. Par contre, pour tout $n \in \mathbb{N}$, $n \leq 1$,

$$R_n = \{(a, b) \in \mathbb{Z}^2 \,|\, n|a - b\}$$

définit une relation d'équivalence, qu'on appelle la relation de congruence modulo n. Pour cette relation, on utilise la notation :

$$a \equiv b \mod n \Leftrightarrow aR_n b, \quad a, b \in \mathbb{Z}$$

et on remarque que deux entiers sont équivalents modulo n précisément quand ils donnent les mêmes restes par division à n.

Définition 5.2 — Soit $\sim$ une relation d'équivalence.

(1) Pour $x \in E$, on appelle **classe d'équivalence** de x, et on note $\bar{x}$ ou $[x]$, l'ensemble des $y \in E$ qui sont en relation avec x, c'est-à-dire défini par

$$\bar{x} := \{y \in E, \,|\, x \sim y\} \subset E.$$

(2) On appelle **représentant** de $\bar{x}$ tout élément de l'ensemble $\bar{x} \subset E$.

(3) L'ensemble des classes d'équivalences E

$$/\sim := \{\bar{x} \mid x \in E\}$$

et est appelé **ensemble quotient** ou E **modulo** $\sim$. C'est un sous-ensemble de $\mathcal{P}(E)$, l'ensemble de tous les sous-ensembles de E. Une classe d'équivalence est donc à la fois un sous-ensemble de E, et un élément de $E/\sim$.

(4) L'application naturelle $\pi : E \to E/\sim$ définie par $\pi(x) := \bar{x} = \{y \in E \,|\, x \sim y\}$ est appelée la **projection canonique** de E dans $E/\sim$.

Exemple 5.2 — Pour tout $x \in E$, x est toujours un représentant de $\bar{x}$, par la propriété de réfléxivité.

Pour la relation d'égalité, on a $\bar{x} = \{x\}$ et la projection canonique est une bijection entre E et $E/=$.

Dans la relation de congruence modulo n, on a

$$\bar{k} = \{ln + k \mid l \in \mathbb{Z}\}$$

et donc il existe précisément n classes d'équivalences, ayant comme représentants distingués $0, 1, \ldots, n-1$. On note avec $\mathbb{Z}/n\mathbb{Z}$ l'espace quotient : il contient donc n éléments :

$$\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \ldots, \bar{n}\}.$$

En particulier, pour $n = 2$ on a seulement deux classes d'équivalence : $\bar{0}$ = entiers pairs et $\bar{1}$ = entiers impairs.

Rappelons aussi :

Définition 5.3 — Soit E un ensemble. Une **partition** de E consiste en une famille $(E_i)_{i\in I}$ de sous-ensembles disjoints et non-vides de E, où I est un ensemble d'indices, dont l'union donne E :

$$\forall i \neq j \in I, \quad E_i \cap E_j = \emptyset \quad \text{et} \quad \bigcup_{i\in I} E_i = E.$$

Comme il s'agit d'une union disjointe, on utilise aussi la notation $E = \sqcup_{i\in I} E_i$.

La proposition suivante montre que la donnée d'une relation d'équivalence sur un ensemble E est la même chose que la donnée d'une partition de E.

Proposition 5.4 — 1) Soit E un ensemble et $\sim$ une relation d'équivalence sur E. Soit $x, y \in E$. Il y a équivalence entre les propositions suivantes :

(i) $\bar{x} = \bar{y}$,

(ii) $x \sim y$,

(iii) $x \in \bar{y}$.

2) L'ensemble des classes d'équivalences de E forme une partition de E.
3) Soit $(E_i)_{i\in I}$ une partition d'un ensemble E et soit R la relation définie par

$$R = \{(x, y) \in E^2 \,|\, \exists i \in I,\, x \in E_i \text{ et } y \in E_i\} \subset E^2,$$

c'est-à-dire : xRy si et seulement si il existe un indice $i \in I$ tel que $x \in E_i$ et $y \in E_i$. Alors R est une relation d'équivalence dont les classes sont les ensembles E_i.

Démonstration. 1. Montrons (ii)⇒(i). On a $\bar{x} = \{z, | \, x \sim z\}$. Supposons $x \sim y$ et montrons que $\bar{x} = \bar{y}$. Soit $z \in \bar{x}$, alors $x \sim z$ et comme $y \sim x$, on a donc $z \sim y$ ce qui implique $z \in \bar{y}$ d'où $\bar{x} \subset \bar{y}$. On a l'inclusion réciproque en procédant de même avec la relation $y \sim x$ qui est vraie car $\sim$ est symétrique. Ainsi $\bar{x} = \bar{y}$.
Montrons (i)⇒(iii)⇒(ii). Supposons maintenant que $\bar{x} = \bar{y}$, alors comme $x \in \bar{x}$ (la relation est symétrique) et que $\bar{x} = \bar{y}$, on a $x \in \bar{y}$, c'est à dire $x \sim y$. On a donc montré $\bar{x} = \bar{y} \Rightarrow x \in \bar{y} \Rightarrow x \sim y$, d'où les équivalences.
2. Soient $x, y \in E$ tels que $\bar{x} \neq \bar{y}$. Montrons que $\bar{x} \cap \bar{y} = \emptyset$. S'il existe $z \in \bar{x} \cap \bar{y}$, alors $x \sim z$ et $y \sim z$ donc $y \sim x$ et $\bar{x} = \bar{y}$, donc deux sous ensembles distincts sont disjoints. Par ailleurs chaque élément x est dans sa propre classe $\bar{x}$, la réunion des classes d'équivalences est donc E. L'ensemble des classes d'équivalences forme donc une partition.
3. Soit $x \in E$. Comme $(E_i)_{i\in I}$ est une partition de E, il existe $i \in I$ unique tel que $x \in E_i$. On a alors $x \in E_i$, d'où xRx : la relation R est réflexive.
Soient $x, y \in E$. On a xRy ssi ($\exists i \in I$, $x \in E_i$ et $y \in E_i$) ssi yRx. La relation est donc symétrique.
Soient $x, y, z \in E$. Supposons xRy et yRz. Il existe des indices $i, j \in I$ tels que $x \in E_i, y \in E_i$, $y \in E_j$, $z \in E_j$. Alors $E_i \cap E_j$ contient y, donc par propriété des partitions, $E_i = E_j$ (et $i = j$), d'où $x \in E_i, z \in E_i$ et donc xRz. On a donc montré que R est bien une relation d'équivalence. □

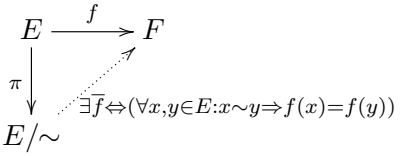
Définition 5.5 — Etant donnée une relation d'équivalence, on appelle **système de représentants** de E modulo $\sim$ un sous-ensemble $F \subset E$ tel que $\forall \alpha \in E/\sim$, $\exists! x \in F$ avec

$\alpha = [x]$. En d'autre termes, la projection canonique restreinte à F est une bijection, ou encore, de façon équivalente, $([x])_{x\in F}$ forme une partition de E.

Exemple 5.3 — Pour la relation de congruence modulo 2, $\{2,3\}$ est un système de représentant et $\{0,1\}$ aussi.

Un dernier fait important nous dit quand est-ce que une application est *bien* définie sur des espaces quotients :

Proposition 5.6 — Soit E un ensemble, $\sim$ une relation d'équivalence sur E et $\pi\colon E \to E/\!\sim$ la projection canonique. Soit $f : E \to F$ une application. Il existe alors une application $\bar{f} : E/\!\sim \to F$ avec $\bar{f}\circ\pi = f$ ssi pour tout $x, y \in E$, $x \sim y \Rightarrow f(x) = f(y)$. On exprime cela par le diagramme



et on dit dans ce cas-ci que f se factorise par π.

Démonstration. Supposons d'abord qu'une telle application $\bar{f}$ existe. Soient $x, y \in E$ avec $x \sim y$. On a alors que $\pi(x) = \pi(y)$, et donc

$$f(x) = \bar{f}(\pi(x)) = \bar{f}(\pi(y)) = f(y).$$

Réciproquement, supposons que $\forall x, y \in E$, $x \sim y \Rightarrow f(x) = f(y)$. Définissons l'application $\bar{f} : E/\!\sim \to F$ par $\bar{f}(\alpha) := f(x)$, ou $x \in \alpha$, $\alpha \in E/\!\sim$. Puisque on a fait le choix du représentant x de la classe α dans la définition de $\bar{f}$, il faut voir que cela ne depend cependant pas de ce choix, i.e. que $\bar{f}$ est bien définie. En effet, si $y \in \alpha$ est un autre représentant de α, alors on a que $x \sim y$, et donc par hypothèse $f(x) = f(y)$, donc la définition de $\bar{f}$ ne depend pas du choix. De plus, on a que pour tout $x \in E$, $f(x) = \bar{f}([x]) = \bar{f}(\pi(x))$, i.e. $f = \bar{f}\circ\pi$. □

Exemple 5.4 — $f : \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}$, $[n] \to n$ n'est pas bien définie : on a $[0] = [2]$, donc on devrait avoir $0 = f([0]) = f([2]) = 2$, ce qui est absurde. En d'autres mots, l'application $\mathbb{Z} \to \mathbb{Z}$, $n \mapsto n$ ne factorise pas la projection canonique $\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$.

Par contre, l'application $\bar{f}\colon \mathbb{Z}/4\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$, $[n](\mod 4) \mapsto [n](\mod 2)$ est bien définie, notamment elle est donnée par la factorisation de $f : \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$, $n \mapsto [n](\mod 2)$.

5.2. **Classes modulo un sous-groupe.** Nous allons appliquer la notion d'équivalence dans le contexte de groupes : on va associer à tout sous-groupe H d'un groupe G deux relations d'équivalence sur G, et donc deux partitions de G.

Pour $x \in G$, notons $xH = \{xh \,|\, h \in H\} \subset G$ et $Hx = \{hx \mid h \in H\}$.

Proposition 5.7 — Soit G un groupe et H un sous-groupe. La relation

$$x \sim_H y \Leftrightarrow x^{-1}y \in H \Leftrightarrow y \in xH$$

est une relation d'équivalence, dont les classes d'équivalences sont données par xH. On la nomme la relation d'équivalence modulo H *à gauche*, et on note l'espace quotient correspondant par G/H.

Démonstration. Soient $x, y, z \in G$. On a $x \sim_H x$ car H est un sous-groupe et $x^{-1}x = e \in H$, donc la relation est réflexive. Si $x \sim_H y$, alors $x^{-1}y \in H$, et donc aussi $(x^{-1}y)^{-1} = y^{-1}x \in H$, ce qui implique $y \sim_H x$, ainsi la relation est symétrique. Finalement, si $x \sim_H y$ et $y \sim_H z$ alors $x^{-1}y \in H$ et $y^{-1}z \in H$ donc $x^{-1}z = x^{-1}yy^{-1}z \in H$ d'où $x \sim_H z$ et la relation est transitive. □

Tout à fait de la même manière on définit sur G une relation d'équivalence à droite

$$x \;{}_H\!\sim y \Leftrightarrow yx^{-1} \in H \Leftrightarrow y \in Hx$$

dont les classes seront données par Hx et l'espace quotient sera noté $H\backslash G$. Si G est abelien, les deux constructions coincïdent.

Exemple 5.5 — Considérons $G = \mathbb{Z}$ le groupe additif et $H = n\mathbb{Z} \subset \mathbb{Z}$ un sous-groupe, $n \geq 1$. Pour tout $x \in \mathbb{Z}$ on a :

$$x + H = \{x + h \,|\, h \in n\mathbb{Z}\} = \{x + nk \,|\, k \in \mathbb{Z}\}$$

donc la relation d'équivalence modulo H coincïde avec la congruence modulo n.

5.3. **Théorème de nombre de classes et Théorème de Lagrange.**

Proposition 5.8 — Soit $(G, \cdot)$ un groupe et H un sous-groupe. Alors les deux espaces quotients G/H et $H\backslash G$ sont en bijection. En particulier, si G/H est fini, alors $H\backslash G$ est aussi fini et on appelle le nombre de classes de G modulo H

$$[G : H] := |G/H| = |H\backslash G|$$

l'indice de H dans G.

Démonstration. Soit $\pi : G \to G/H$ la projection canonique, et soit $\tilde{\varphi}\colon G \to G\backslash H$ l'application $g \mapsto Hg^{-1}$. Supposons que $g, h \in G$ satisfont $g \sim_H h$. Alors

$$g^{-1}h \in H \Rightarrow (g^{-1}h)^{-1} = h^{-1}g \in H \Rightarrow Hg^{-1} = Hh^{-1}$$

donc $\tilde{\varphi}(g) = \tilde{\varphi}(h)$. Cela implique que φ factorise par π et induit une application $\varphi\colon G/H \to H\backslash G$, $gH \mapsto Hg^{-1}$.

On montre de la même façon que l'application $\tilde{\psi}\colon G \to G/H$, $g \mapsto g^{-1}H$ induit une application bien définie $\psi\colon G\backslash H \to G/H$, $Hg \mapsto g^{-1}H$. Clairement ψ est la réciproque de φ, donc φ est une bijection. Cela implique que G/H et $G\backslash H$ ont le même cardinal. □

Théorème 5.9 (Nombre de classes)**.** *Soit $(G, \cdot)$ un groupe fini et $H < G$ un sous-groupe. Alors on a la formule suivante :*

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

Démonstration. Comme G est fini et la projection naturelle $\pi\colon G \to G/H$ est surjective, $[G : H] = |G/H|$ est un nombre (fini), qu'on denotera par n. Soit $(x_1, \ldots, x_n)$ un système de représentants de G/H, de sorte que $G/H = \{x_1H, \ldots, x_nH\}$. On a alors la partition de G

$$G = \bigcup_{i=1}^{n} x_iH, \quad x_iH \cap x_jH = \emptyset \text{ pour } i \neq j.$$

On déduit que $|G| = \sum_{i=1}^{n} |x_iH|$. En même temps, pour tout $x \in G$, l'application $H \to xH$, $h \mapsto xh$ est une bijection, ayant comme réciproque $xH \to H$, $u \mapsto x^{-1}u$. On a donc $|H| = |xH|$, et on conclut :

$$|G| = \sum_{i=1}^{n} |x_iH| = \sum_{i=1}^{n} |H| = n|H| = [G : H] \cdot |H|. \qquad \square$$

Comme corollaire imédiat, on a le théorème important :

Corollaire 5.10 (Théorème de Lagrange) — Soit $(G, \cdot)$ un groupe fini d'ordre n et $H < G$ un sous-groupe. Alors l'ordre de H divise l'ordre de G. En particulier, si $x \in G$, alors $\mathrm{ord}(x)|n$ et $x^n = e$.

Démonstration. L'enoncé pour H suit de la formule du nombre de classes. Si $x \in G$, alors $H := \langle x \rangle$ est un sous-groupe de G, donc $\mathrm{ord}(x) = |H||n$. Cela implique que $x^n = e$. □

Remarque 5.11. *Le théorème de Lagrange n'a pas de réciproque : si n divise l'ordre de G, il n'existe pas nécessairement de sous-groupe H d'ordre n. Par exemple S_5, qui est de cardinal*

120, *n'admet pas de sous-groupes d'ordre* 30. *Cependant, il y a des réciproques partielles. Par exemple le théorème de Cauchy garantit que si p est un nombre premier qui divise l'ordre de G, alors G contient un sous-groupe d'ordre p.*

Corollaire 5.12 — Soit G un groupe fini et soient H et K deux sous-groupes de G avec $K \subset H$. Alors on a $[G : K] = [G : H][H : K]$.

Démonstration. On applique le théorème du nombre de classes au couples $K < H$, $H < G$ et $K < G$ pour obtenir :

$$|G| = |K| \cdot [G : K] = |H| \cdot [G : H] = (|K| \cdot [H : K]) \cdot [G : H].$$

En simplifiant par $|K|$ dans l'expression, on obtient la formule à prouver. □

5.4. **Sous-groupes distinguées et le groupe quotient.** Maintenant qu'on a construit des espaces quotients des groupes G/H et $H\backslash G$, une question naturelle est : sont ces espaces quotients des groupes aussi (d'une façon naturelle) ? Comme on va le voir, la réponse depend des propriétés du sous-groupe H choisit.

Définition 5.13 — Un sous-groupe $H < G$ s'appelle *distingué* ou *normal*, noté $H \lhd G$, si

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

Remarque 5.14. *C'est équivalent à demander* $\forall g \in G, \forall h \in H, \quad g^{-1}hg \in H$.

Proposition 5.15 — Un sous-groupe $H < G$ est distingué si et seulement si pour tout $g \in G$ on a $gH = Hg$. En particulier, les deux espaces quotients G/H et $H\backslash G$ coïncident.

Démonstration. Déjà si pour tout $g \in G$ on a $gH = Hg$, on a $gHg^{-1} = H$ et pour tout $h \in H$, $ghg^{-1} \in H$. Réciproquement, soit $g \in G$. Alors pour tout $h \in H$ on a $ghg^{-1} \in H$ donc $gh \in Hg$, donc $gH \subseteq Hg$. Aussi, $g^{-1}hg \in H$ donc $hg \in gH$, donc $Hg \subseteq gH$. □

Remarque 5.16. *Dans un groupe abelien, tout sous-groupe est normal. On a donc :* $d\mathbb{Z} < \mathbb{Z}$ *est normal, mais* $\langle \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \rangle < S_3$ *n'est pas normal.*

Théorème 5.17. *Soit* $(G, \cdot)$ *un groupe et* $H < G$ *un sous-groupe. Alors les conditions suivantes sont équivalentes :*

(1) H *est normal.*

(2) Il existe un morphisme de groupes $\varphi : G \to G'$ *tel que* $H = \ker \varphi$.

(3) Il existe une structure de groupe $\star$ *sur le quotient* G/H *telle que la projection naturelle* $\pi : G \to G/H$ *soit un morphisme de groupes.*

Démonstration. (3) ⇒ (2) : Posons $G' := G/H$, qui est un groupe par hypothèse, et $\varphi = \pi : G \to G'$, qui est un morphisme de groupes. Alors clairement on a $\ker \varphi = H$.

(2) ⇒ (1) : Soit $\varphi : G \to G'$ comme dans l'hypothèse, $h \in H = \ker \varphi$ et $g \in G$. Alors on a :

$$\varphi(g^{-1}hg) = \varphi(g)^{-1}\varphi(h)\varphi(g) = \varphi(g)^{-1}\varphi(g) = e_{G'}$$

donc $g^{-1}hg \in \ker \varphi = H$ et H est normal.

(1) ⇒ (3). Soit $\tau_1, \tau_2 \in G/H$ deux classes et $g_1 \in \tau_1$, $g_2 \in \tau_2$ deux représentants. On définit l'operation $\star$ par

$$\tau_1 \star \tau_2 := g_1 g_2 H.$$

Il faut d'abord vérifier que $\star$ est bien définie, i.e. ne dépend pas des représentants choisis. Si $g_1' \in \tau_1$ et $g_2' \in \tau_2$ sont d'autres représentants, alors $g_i' = g_i \cdot h_i$ pour $h_i \in H$, $i = 1, 2$. En utilisant que $hH = H$ pour tout $h \in H$ et que H est normal, donc que $gH = Hg$ pour tout $g \in G$, on obtient alors

$$g_1'g_2'H = g_1h_1g_2h_2H = g_1h_1g_2H = g_1h_1Hg_2 = g_1Hg_2 = g_1g_2H$$

donc $\star$ est bien définie.

L'élément neutre de $\star$ est $H = eH$:

$$gH \star H = gH = H \star gH, \quad \forall g \in G$$

l'élémént inverse de $gH \in H/G$ pour $\star$ est $g^{-1}H$:

$$gH \star g^{-1}H = gg^{-1}H = H = g^{-1}gH = g^{-1}H \star gH$$

et finalement $\star$ est associative, puisque l'operation $\cdot$ sur G est associative :

$$(g_1H \star g_2H) \star g_3H = (g_1g_2H) \star g_3H = (g_1g_2)g_3H = g_1(g_2g_3)H = g_1H \star g_2g_3H = g_1H \star (g_2H \star g_3H).$$

La projection π est bien un morphisme, car

$$\pi(g_1g_2) = g_1g_2H = g_1H \star g_2H = \pi(g_1) \star \pi(g_2), \quad \forall g_1, g_2 \in G.$$

□

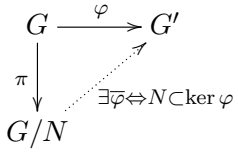
Remarque 5.18. *Si $H \lhd G$ est distingué, alors la structure de groupe sur G/H avec les propriétés demandées est unique. En effet, comme on veut que π soit un morphisme, on est obligé de définir $\star$ par*

$$g_1H \star g_2H = \pi(g_1) \star \pi(g_2) = \pi(g_1g_2) = g_1g_2H.$$

On appelle $(G/H, \star)$ ainsi défini le groupe quotient.

Exemple 5.6 — Comme on l'a déjà remarqué, $n\mathbb{Z} \subset \mathbb{Z}$ est distingué, pour tout $n \in \mathbb{N}$. La structure de groupe qu'on obtient par le théorème d'en haut sur l'espace quotient $\mathbb{Z}/n\mathbb{Z}$ est justement la structure déjà connue de groupe de $\mathbb{Z}/n\mathbb{Z}$.

Théorème 5.19 (Propriété universelle du groupe quotient)**.** *Soit $(G, \cdot)$ un groupe, $N \lhd G$ un sous-groupe distingué et $\pi : G \to G/N$ la projection canonique. Soit de plus $\varphi : G \to G'$ un morphisme de groupes. Alors il existe un morphisme de groupes $\overline{\varphi} : G/N \to G'$ tel que $\overline{\varphi} \circ \pi = \varphi$ si et seulement si $N \subset \ker \varphi$. En diagramme :*



Si c'est le cas, on a de plus $\ker \overline{\varphi} = \pi(\ker \varphi)$ et $\operatorname{im} \overline{\varphi} = \operatorname{im} \varphi$.

Démonstration. Supposons d'abord qu'il existe un tel morphisme $\overline{\varphi}$ avec $\overline{\varphi} \circ \pi = \varphi$. Comme $N = \ker \pi$, on obtient alors

$$\varphi(N) = \overline{\varphi}(\pi(N)) = \overline{\varphi}(e) = e$$

donc on a bien $N \subset \ker \varphi$.

Réciproquement, supposons que $N \subset \ker \varphi$. Définissons $\overline{\varphi}$ par $\overline{\varphi}(gN) := \varphi(g)$, $g \in G$ et vérifions que $\overline{\varphi}$ est bien définie : en effet, si $g' \in gN$ alors $g' = gn$ pour un $n \in N$ et en utilisant $N \subset \ker \varphi$ on obtient

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

i.e. la définition de $\overline{\varphi}$ ne dépend pas du choix du représentant $g \in gN$. Par définition on a que

$$\overline{\varphi} \circ \pi(g) = \overline{\varphi}(gN) = \varphi(g), \quad \forall g \in G$$

et $\overline{\varphi}$ est bien un morphisme :

$$\overline{\varphi}(g_1N \star g_2N) = \overline{\varphi}(g_1g_2N) = \varphi(g_1g_2) = \varphi(g_1)\varphi(g_2) = \overline{\varphi}(g_1N)\overline{\varphi}(g_2N).$$

Finalement, pour un tel morphisme $\overline{\varphi}$, comme $\varphi = \overline{\varphi} \circ \pi$ et que π est surjectif, on obtient $\operatorname{im} \varphi = \overline{\varphi}(\operatorname{im} \pi) = \operatorname{im} \overline{\varphi}$. Pour montrer $\ker \overline{\varphi} = \pi(\ker \varphi)$: si $x \in \ker \overline{\varphi}$ alors il existe $y \in G$

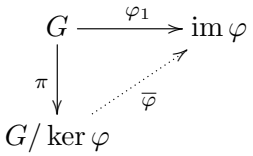
avec $\pi(y) = x$ et alors $\varphi(y) = \overline{\varphi}(\pi(y)) = \overline{\varphi}(x) = e$ donc $x = \pi(y) \in \pi(\ker\varphi)$. Si $x \in \pi(\ker\varphi)$, alors $\exists y \in \ker\varphi$ avec $x = \pi(y)$. Mais alors $\overline{\varphi}(x) = \overline{\varphi}(\pi(y)) = \varphi(y) = e$, donc $x \in \ker\varphi$. □

Remarque 5.20. *Dans le cadre du théorème, si le morphisme $\overline{\varphi}$ existe alors il est unique et on dit dans ce cas là que φ factorise au dessus de G/N.*

Corollaire 5.21 (Théorème d'isomorphisme) — Tout morphisme de groupes $\varphi : G \to G'$ induit un isomorphisme de groupes naturel

$$\overline{\varphi} : G/\ker\varphi \xrightarrow{\cong} \operatorname{im}\varphi.$$

Démonstration. On sait que $\operatorname{im}\varphi < G'$ est un sous-groupe, en particulier il hérite une structure naturelle de groupe de G'. De plus, par définition, φ induit un morphisme surjectif $\varphi_1 : G \to \operatorname{im}\varphi$, $x \mapsto \varphi(x)$. En appliquant le théorème ci-dessus au sous-groupe normal $N = \ker\varphi_1 = \ker\varphi$ et au diagramme :



on obtient un morphisme naturel $\overline{\varphi} : G/\ker\varphi \to \operatorname{im}\varphi$ avec $\ker\overline{\varphi} = \pi(\ker\varphi_1) = [e_G]$ et $\operatorname{im}\overline{\varphi} = \operatorname{im}\varphi_1 = \operatorname{im}\varphi$, donc un isomorphisme. □

Voici quelques applications :

Proposition 5.22 — Soit $(G, \cdot)$ un groupe monogène. Alors $(G, \cdot)$ est isomorphe à $(\mathbb{Z}, +)$ ou à $(\mathbb{Z}/n\mathbb{Z}, +)$ pour un $n \in \mathbb{N}^*$. En particulier, si $(G, \cdot)$ est un groupe fini de cardinal un nombre premier p, alors $(G, \cdot) \cong (\mathbb{Z}/p\mathbb{Z}, +)$.

Démonstration. Si $G = \langle x \rangle$, $x \in G$, on considère le morphisme de groupes $\varphi : \mathbb{Z} \to G$, $n \mapsto x^n$, et on lui applique le théorème d'isomorphisme.

Si $p = |G|$ est un nompre premier et $x \in G$ n'est pas l'élément neutre, le théorème de Lagrange nous dit que $1 < \operatorname{ord} x$ divise p, donc $\operatorname{ord} x = p$ et x est un générateur de G. On déduit que G est cyclique, donc isomorphe à $(\mathbb{Z}/p\mathbb{Z}, +)$. □

Proposition 5.23 — Soient $n, m \in \mathbb{N} \setminus \{0\}$. Alors les groupes $(\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}, +)$ et $(\mathbb{Z}/nm\mathbb{Z}, +)$ sont isomorphes si et seulement si m et n sont premiers entre eux.

Démonstration. Supposons d'abord qu'on a un isomorphisme entre $G := \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ et $\mathbb{Z}/nm\mathbb{Z}$. Cela implique que G est cyclique, et donc contient un élément z d'ordre nm. D'autre part, un tel élément est de la forme (x, y) avec $x \in \mathbb{Z}/n\mathbb{Z}$ et $y \in \mathbb{Z}/m\mathbb{Z}$. Puisque $nx = \bar{0}$ dans $\mathbb{Z}/n\mathbb{Z}$ et $my = \bar{0}$ dans $\mathbb{Z}/m\mathbb{Z}$, on obtient que $l =$ppcm(n, m) satisfait $lz = (lx, ly) = (\bar{0}, \bar{0})$, et donc forcément l'ordre de z est un diviseur de l. Or $nm|$ppcm(n, m) est seulement possible si ppcm$(n, m) = mn$, ce qui implique que m et n sont premiers entre eux.

Réciproquement, en supposant que n et m sont premiers entre eux, on va directement construire un isomorphisme entre G et $\mathbb{Z}/nm\mathbb{Z}$. Soit $\varphi : \mathbb{Z} \to G$ le morphisme de groupes donné par $x \mapsto (\bar{x}, [x])$, où l'on note avec $\bar{x}$ la classe de x modulo n et avec $[x]$ sa classe modulo m. Soit aussi $\pi : \mathbb{Z} \to \mathbb{Z}/nm\mathbb{Z}$ la projection canonique. On sait que φ induit un morphisme $\overline{\varphi} : \mathbb{Z}/nm\mathbb{Z} \to G$ avec $\overline{\varphi} \circ \pi = \varphi$ si et seulement si $nm\mathbb{Z} \subset \ker\varphi$. Or on a :

$$x \in \ker\varphi \Leftrightarrow \bar{x} = 0 \text{ et } [x] = 0 \Leftrightarrow n|x \text{ et } m|x \Leftrightarrow \text{ppcm}(n, m) = nm|x$$

d'où on deduit que $\ker\varphi = nm\mathbb{Z}$. Donc le morphisme $\overline{\varphi}$ existe bien et de plus $\ker\overline{\varphi} = \pi(\ker\varphi) = \{e\}$ donc $\overline{\varphi}$ est injectif. Comme $|G| = mn = |\mathbb{Z}/nm\mathbb{Z}|$, on déduit que $\overline{\varphi}$ est bijectif, et donc un isomorphisme de groupes.

□

Proposition 5.24 — Soient $(G,\cdot)$ un groupe et $x,y\in G$ deux éléments avec $xy=yx$ et $a=\operatorname{ord}x$, $b=\operatorname{ord}y\in\mathbb{N}$. Alors $\operatorname{ord}(xy)|\operatorname{ppcm}(a,b)$. Si de plus on a $\langle x\rangle\cap\langle y\rangle=\{e\}$, alors $\operatorname{ord}(xy)=\operatorname{ppcm}(a,b)$.

Démonstration. Si $m=\operatorname{ppcm}(a,b)$, alors on peut écrire $m=au=vb$ avec $a,b\in\mathbb{N}$. Comme $xy=yx$, on a donc que

$$(xy)^m=x^my^m=(x^a)^u(y^b)^v=e$$

et donc $\operatorname{ord}(xy)|m$.

Supposons de plus que $\langle x\rangle\cap\langle y\rangle=\{e\}$ et soit $l=\operatorname{ord}(ab)$. Alors $(xy)^l=e$ implique

$$x^l=(y^{-1})l\in\langle x\rangle\cap\langle y\rangle=\{e\}$$

donc $x^l=y^l=e$ et $a|l$ et $b|l$. D'ici on déduit que $m|l$ et donc $l=m$. □

Remarque 5.25. *Dans la proposition précédente, sans l'hypothèse $\langle x\rangle\cap\langle y\rangle=\{e\}$ on n'a pas en général $\operatorname{ord}(xy)=ppcm(a,b)$. En effet, un contre-exemple est donné en prennant x d'ordre $a>1$ et $y=x^{-1}$. Alors $\operatorname{ord}(xy)=\operatorname{ord}(e)=1\neq a$, mais en effet $\langle x\rangle\cap\langle x^{-1}\rangle=\langle x\rangle\neq\{e\}$.*

Corollaire 5.26 — Soit $n\in\mathbb{N}$, $n\geq 2$ et soient σ et τ deux cycles dans S_n à supports disjoints, de longueurs respectives a et b. Alors $\operatorname{ord}(\sigma\tau)=\operatorname{ppcm}(ab)$.

Démonstration. On a $\operatorname{ord}(\sigma)=a$ et $\operatorname{ord}(\tau)=b$. Comme σ et τ sont à support disjoints, ils commutent, donc on est dans le cadre de la proposition d'avant et il suffit de montrer que $\langle\sigma\rangle\cap\langle\tau\rangle=\{\mathsf{id}\}$. Mais pour tout $l\in\mathbb{N}$ on a $\operatorname{supp}(\sigma^l)\subset\operatorname{supp}(\sigma)$ et $\operatorname{supp}(\tau^l)\subset\operatorname{supp}(\tau)$. Donc si $\psi\in\langle\sigma\rangle\cap\langle\tau\rangle$ alors $\operatorname{supp}(\psi)\subset\operatorname{supp}(\sigma)\cap\operatorname{supp}(\tau)=\emptyset$. On déduit que $\psi=\mathsf{id}$. □

6. Actions des groupes

6.1. Premières définitions et exemples.

Définition 6.1 — Soit X un ensemble et $(G,\cdot)$ un groupe. **Une action de G sur X** est une application

$$\psi\colon G\times X\to X$$

avec les propriétés :

(1) $\psi(1_G,x)=x$, $\forall x\in X$

(2) $\psi(g,\psi(h,x))=\psi(gh,x)$ pour tout $g,h\in G$ et $x\in X$. On dit aussi que G agit ou opère sur X, et on utilise souvent la notation $g.x:=\psi(g,x)$.

Rappelons que l'ensemble $S_X=\{f:X\to X \text{ bijection}\}$ avec la composition forme un groupe. Il s'ensuit de la définition précédente qu'une application $\psi:G\times X\to X$ est une action de groupe ssi l'application induite

$$\chi\colon G\to S_X,\quad g\mapsto(\psi(g,\cdot):X\to X)\in S_X$$

est bien définie et un morphisme de groupes. Notons que en effet, pour une action de groupe, $\psi(g,\cdot)$ est bijective, d'inverse $\psi(g,\cdot)^{-1}=\psi(g^{-1},\cdot)$.

Exemple 6.1 — A) Soit $n\geq 1$. Alors S_n agit de manière naturelle sur $X=\{1,\dots,n\}$ par

$$(\sigma,k)\in S_n\times X\to\sigma(k)\in X=\{1,\dots,n\}.$$

Ici $S_X=S_n$ et χ est l'identité.

B) Il y a trois actions naturelles différentes d'un groupe G sur lui-même :

(1) action par translation à gauche : $\psi_1:G\times G\to G$, $(g,x)\to g\cdot x:=gx$. Pour cette action, χ est injectif. Il s'en suit que tout groupe G est isomorphe à un sous-groupe de S_G.

(2) action par translation à droite : $\psi_2:G\times G\to G$, $(g,x)\to g\cdot x:=xg^{-1}$(noter qu'il faut prendre l'inverse sinon cela ne fonctionne pas : on a pas la relation $(gh).x=g.(h.x)$) ;

(3) action par conjugaison : $\psi_3 : G \times G \to G$, $(g, x) \to g \cdot x := gxg^{-1}$. Dans ce dernier cas, le noyau de χ est le centre de G.

C) Le groupe $\mathrm{GL}(n, \mathbb{C})$ agit sur $\mathbb{C}^n$ par multiplication à gauche :

$$\mathrm{GL}(n, \mathbb{C}) \times \mathbb{C}^n \to \mathbb{C}^n, \quad (A, v) \mapsto Av.$$

D) Le groupe $\mathrm{GL}(n, \mathbb{C})$ agit aussi sur l'espace des matrices $X = \mathrm{Mat}_{n\times n}(\mathbb{C})$ par conjugaison :

$$\mathrm{GL}(n, \mathbb{C}) \times \mathrm{Mat}_{n\times n}(\mathbb{C}) \to \mathrm{Mat}_{n\times n}(\mathbb{C}), \quad , (A, M) \mapsto AMA^{-1}.$$

E) $\mathrm{GL}_n(\mathbb{C}) \times \mathrm{GL}_n(\mathbb{C})$ opère sur $\mathrm{Mat}_n(\mathbb{C})$ par $(P, Q).M = PMQ^{-1}$pour $(P, Q) \in \mathrm{GL}_n(\mathbb{C}) \times \mathrm{GL}_n(\mathbb{C})$ et $M \in \mathrm{Mat}_n(\mathbb{C})$.

F) Soit H un sous-groupe de G. Alors G opère sur l'ensemble G/H des classes à gauche modulo H par : $g \cdot (xH) := (gx)H$.

Définition 6.2 — Soit G un groupe qui opère sur un ensemble X, et soit $x \in X$.

(1) $G_x := \{g \in G | g.x = x\} \subset G$ est appelé le **stabilisateur de** x. On note aussi le stabilisateur par $\mathrm{Stab}_G(x)$.

(2) Le sous-ensemble de X donné par $O_x = \{gx \mid g \in G\} \subset X$ est appelé **l'orbite de** x, noté aussi avec Gx.

Exemple 6.2 — Pour l'exemple 6.1 (A) de l'action de $G = S_n$ sur $X = \{1, \ldots, n\}$, le stabilisateur de $n \in X$ est donné par toutes les permutations qui fixent n, et s'identifie donc avec S_{n-1} vu comme sous-groupe de S_n. Comme pour tout $k \in X$ différent de n la transposition $\sigma := (k, n) \in S_n$ agit comme $\sigma.n = k$, on obtient que $\mathcal{O}_n = X$.

Pour l'exemple (D), l'orbite d'une matrice M est donnée par toutes les matrices semblables à M, et pour l'exemple (E), l'orbite de M est donnée par toutes les matrices équivalentes à M.

Lemme 6.3 — Soit G un groupe qui agit sur X, et soit $x \in X$. Le stabilisateur G_x de x est un sous-groupe de G. De plus, si $g \in G$, alors les stabilisateurs de x et de gx vérifient la relation suivante :

$$G_{gx} = g(G_x)g^{-1}.$$

En particulier, si x et y sont dans la même orbite, alors les stabilisateurs de x et de y sont conjugués.

Démonstration. On vérifie facilement que $G_x < G$. Soit $h \in G$. On a $h \in G_{gx}$ si et seulement si $h.gx = gx$ si et seulement si $hgx = gx$ si et seulement si $g^{-1}hgx = x$ si et seulement si $g^{-1}hg \in G_x$. □

6.2. **L'espace des orbites.**

Proposition 6.4 — Soit $G \times X \to X$ une action de groupe. La relation

$$x \sim x' \iff \exists g \in G \colon g.x = x' \iff x' \in O_x$$

est une relation d'équivalence. La classe déquivalence de $x \in X$ s'identifie avec l'orbite O_x de X. On note avec $X/G := X/\sim$ l'ensemble de toutes les orbites de l'action. En particulier, si X est fini, on a :

$$\#X = \sum_{O \in X/G} \#O. \tag{2}$$

Démonstration. Pour tous $x, y, z \in X$, $g, g' \in G$, on a :

(1) $e.x = x$, donc la relation est réflexive ;

(2) supposons $g.x = y$ alors $g^{-1}.y = x$, donc le relation est symétrique ;

(3) supposons $g.x = y$, $g'y = z$, alors $g'gx = z$: la relation est transitive.

L'ensemble X est donc réunion disjointe de ses classes d'équivalences, qui sont les orbites :

$$X = \bigsqcup_{O \in X/G} O$$

donc si X est fini on retrouve la formule désirée. □

Exemple 6.3 — Dans l'exemple 6.1 (A) il y a une unique orbite, donc X/G est un singleton. Pour l'exemple (E), on sait que deux matrices sont équivalentes ssi elles one le même rang. Il s'en suit que l'espace des orbites X/G est isomorphe à l'ensemble $\{0, \dots, n\}$, l'isomorphisme étant donné par $[A] \in X/G \mapsto \text{rang}(A)$.

Définition 6.5 — Soit $G \times X \to X$ une action de G sur X, avec morphisme associé $\chi : G \to S_X$. On dira que l'action est :
1. **transitive** si $\forall x, y \in X$, $\exists g \in G$ tel que $y = g \cdot x$.
2. **fidèle** si $\forall g \in G \setminus \{e\}$, $\exists x \in X$, $g \cdot x \neq x$,
3. **libre** si $\forall g \in G \setminus \{e\}$, $\forall x \in X$, $g \cdot x \neq x$.

On dit alors que G opère transitivement, fidèlement resp. librement sur X.

Remarque 6.6. *Dire que l'action est fidèle est équivalent à dire que le noyau de χ est trivial. Si χ est libre alors χ est fidèle. Une action est libre précisément quand tous les stabilisateurs sont triviaux.*

Exemple 6.4 —
(1) L'action de G sur lui-même par multiplication à gauche (ou à droite) est fidéle, libre et transitive.

(2) Soit H un sous-groupe G. Alors G opère transitivement sur G/H par l'action $(g, xH) \to gxH$.

Proposition 6.7 — Soit G un groupe qui opère transitivement sur un ensemble X. Pour tout $x \in X$, l'application $f_x : G/G_x \to X$, définie par $f_x(gG_x) := g \cdot x$ est bien définie, et elle est une bijection. En particulier, si G est fini, on obtient

$$\#X = [G : G_x].$$

Démonstration. L'application f_x est bien définie car $gG_x = hG_x$ implique que $h^{-1}g \in G_x$ et donc $h^{-1}gx = x$, d'où $gx = hx$, i.e. la définition de f_x est bien indépendante du choix du représentant g de la classe gG_x. La fonction est injective car $gx = hx$ implique $h^{-1}g \in G_x$ et donc $gG_x = hG_x$. Elle est surjective car par hypothèse G opère transitivement sur X. □

Corollaire 6.8 — Pour tout groupe G qui agit sur un ensemble X et pour tout $x \in X$, on a une bijection $G/G_x \xrightarrow{\cong} \mathcal{O}_x$. En particulier, si G est fini, alors

$$\#O_x = [G : G_x] = |G|/|G_x|.$$

Démonstration. On applique la proposition précédente à l'espace $X' := \mathcal{O}_x \subset X$, sur lequel G agit transitivement. □

Via (2), on obtient :

Théorème 6.9 (La formule des classes)**.** *Soit G un groupe fini qui opère sur un ensemble fini X. Soit $O_1, \dots, O_k \subset X$ les orbites de l'action et pour tout i, $1 \leq i \leq k$, soit x_i un élément de O_i. Alors on a :*

$$\#X = \sum_{i=1}^{i=k} \#O_i = \sum_{i=1}^{i=k} [G : G_{x_i}].$$

Théorème 6.10 (La formule de Burnside)**.** *Soit G un groupe fini qui opère sur un ensemble fini X, et pour tout $g \in G$, soit $Fix(g) := \{x \in X \mid gx = x\}$ l'ensemble des éléments de X fixés par g. Alors on a :*

$$\#X/G = \frac{1}{|G|} \sum_{g \in G} \#Fix(g).$$

Démonstration. On a :

$$\begin{aligned} \textstyle\sum_{g\in G} \#Fix(g) &= \textstyle\sum_{g\in G} \#\{x \in X \mid gx = x\} = \\ &= \#\{(g, x) \in G \times X \mid gx = x\} = \\ &= \textstyle\sum_{x\in X} \#\{g \in G \mid gx = x\} = \\ &= \textstyle\sum_{x\in X} |G_x| = \sum_{x\in X} \frac{|G|}{\#O_x} \end{aligned}$$

oú on a utilisé $\#O_x = [G : G_x] = |G|/|G_x|$.

D'autre part, pour toute orbite $O \in X/G$ et pour tout $x, y \in O$, on a $O = O_x = O_y$. En utilisant que $X = \sqcup_{O\in X/G} O$, on déduit donc :

$$\begin{aligned} \sum_{g\in G} \#Fix(g) &= \sum_{x\in X} \frac{|G|}{\#O_x} \\ &= \sum_{O\in X/G} \sum_{x\in O} \frac{|G|}{\#O_x} \\ &= \sum_{O\in X/G} \left(\#O \cdot \frac{|G|}{\#O} \right) = |G| \cdot \#X/G \end{aligned}$$

ce qui donne la conclusion.

□

7. Classification des groupes abéliens finis

Dans cette section, on va s'occuper de la classification des groupes abéliens finis à isomorphisme près. Plus précisément, on va montrer qu'ils sont tous des produits des groupes cycliques. Cette décomposition en produit n'est pas unique en général, cépendant elle le devient une fois qu'on impose certaines conditions sur les ordres des groupes cycliques qui apparaissent dans la décomposition.

7.1. **Décomposition en p-groupes.** Soit G un groupe abélien d'ordre $n \in \mathbb{N}$. Pour chaque nombre premier p qui divise n, on définit sa **composante p-primaire** comme étant

$$G_p := \{x \in G \mid \exists l \in \mathbb{N} \quad \mathrm{ord}(x) = p^l\}.$$

Si $n = \prod_{i=1}^k p_i^{r_i}$ est la décomposition de n en ses facteurs premiers, on a aussi

$$G_{p_i} = \{x \in G \mid x^{p_i^{r_i}} = e\}.$$

On va comencer par prouver :

Théorème 7.1. *Soit G un groupe abélien d'ordre $n = \prod_{i=1}^k p_i^{r_i}$. Alors pour chaque $i \in \{1, \dots, k\}$, la composante p_i-primaire de G est un groupe à $p_i^{r_i}$ éléments et on a un isomorphisme de groupes :*

$$G \cong G_{p_1} \times \cdots \times G_{p_k}.$$

On divise la preuve en deux lemmes auxiliaires :

Lemme 7.2 — Soit G un groupe abélien à $n = ab$ éléments, avec $\mathrm{pgcd}(a, b) = 1$. Pour $k \in \mathbb{N}$, soit

$$G(k) := \{x \in G, \mid x^k = 1\} = \{x \in G \mid \mathrm{ord}(x) | k\}.$$

Alors $G(k) < G$ et on a un isomorphisme des groupes $G \cong G(a) \times G(b)$.

Démonstration. Comme G est abélien, $\varphi_k \colon G \to G$, $x \mapsto x^k$ est un morphisme de groupes, donc $G(k) = \ker \varphi_k$ est un sous-groupe de G.

Soit

$$\varphi \colon G(a) \times G(b) \to G, \quad (x, y) \mapsto xy.$$

Comme G est abélien, φ est un morphisme. Montrons que φ est bijectif. Puisque $\mathrm{pgcd}(a, b) = 1$, il existe $u, v \in \mathbb{Z}$ tel que $ua + vb = 1$. Pour tout $x \in G$, on a alors :

$$x = x^{ua+vb} = x^{ua} \cdot x^{vb}.$$

De plus $(x^{ua})^b = (x^u)^n = e$, i.e. $x^{ua} \in G(b)$ et pareil $x^{vb} \in G(a)$, donc $x = \varphi(x^{vb}, x^{ua})$ et φ est surjectif.

Si $\varphi(x, y) = e$ alors $y = x^{-1} \in G(a) \cap G(b)$, donc d'une part $\mathrm{ord}(x) | a$ et d'autre part $\mathrm{ord}(x) = \mathrm{ord}(x^{-1}) | b$, ce qui donne $\mathrm{ord}(x) | \mathrm{pgcd}(a, b) = 1$, i.e. $x = y = e$ et φ est injectif. □

Définition 7.3 — Pour un nombre premier p, un groupe fini G de cardinal p^k ($k \in \mathbb{N}$) est appelé **p-groupe**.

Par le théorème de Lagrange, dans un p-groupe, l'ordre de tout élément est une puissance de p. Réciproquement on a :

Lemme 7.4 — Soit H un groupe abélien fini, p un nombre premier tel que pour tout $x \in H$, $\mathrm{ord}(x) = p^l$ pour un certain $l \in \mathbb{N}$. Alors H est un p-groupe.

Démonstration. Comme H est fini, on peut écrire $H = \{x_1, \dots x_k\}$. On définit :

$$\varphi \colon H' = \langle x_1 \rangle \times \cdots \times \langle x_k \rangle \to H, \quad , (y_1, \dots, y_k) \to y_1 \cdots y_k.$$

Comme H est abélien, φ est bien un morphisme. Il est évidemment surjectif. Par le thórème d'isomorphisme, on a donc $H \cong H'/\ker \varphi$. De plus, par hypothèse, $|H'| = \prod_{i=1}^k p^{l_i} = p^s$ où

$s = \sum_{i=1}^{k} l_i$ et p^{l_i} est l'ordre de x_i. Comme le théorème de Lagrange implique que $|H|$ divise $|H'|$, on obtient bien que H est un p-groupe. □

Preuve du Théorème 7.1. Avec la notation du Lemme 7.2, pour $i \in \{1, \dots k\}$, on a $G_{p_i} = G(p_i^{r_i})$. C'est donc bien un sous-groupe de G, qui de plus est un p_i-groupe d'après Lemme 7.4. En applicant inductivement Lemme 7.2, on obtient un isomorphisme $G \cong G_{p_1} \times \cdots \times G_{p_k}$. En comparant les ordres des deux groupes et en utilisant que la décomposition en facteurs premiers est unique dans $\mathbb{N}$, on obtient aussi que G_{p_i} est d'ordre $p_i^{r_i}$. □

Exemple 7.1 — Si G est le groupe additif $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/25\mathbb{Z} \times \mathbb{Z}/7^3\mathbb{Z}$, les composantes p-primaires sont

$$G_2 = \mathbb{Z}/2\mathbb{Z} \times \{0\} \times \{0\} \times \{0\},$$
$$G_5 = \{0\} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/25\mathbb{Z} \times \{0\},$$
$$G_7 = \{0\} \times \{0\} \times \{0\} \times \mathbb{Z}/7^3\mathbb{Z}.$$

Exemple 7.2 — Pour $G = \mathbb{Z}/6\mathbb{Z}$, qui est d'ordre 6, on a

$$G_2 = \{\bar{0}, \bar{3}\}, \quad G_3 = \{\bar{0}, \bar{2}, \bar{4}\}.$$

Les groupes G_2 et G_3 sont d'ordre 2 et 3, ils sont isomorphes à $\mathbb{Z}/2\mathbb{Z}$ et $\mathbb{Z}/3\mathbb{Z}$ respectivement. On a bien $\mathbb{Z}/6\mathbb{Z} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, c'est-à-dire $G \simeq G_2 \times G_3$.

7.2. Décomposition des p-groupes en produit des groupes cycliques. Facteurs invariants.

Théorème 7.5. *Soit p un nombre premier. Tout p-groupe abélien G est isomorphe à un produit de groupes cycliques de la forme $\mathbb{Z}/p^a\mathbb{Z}$, c'est-à-dire qu'il existe des entiers k, $n_k \dots, n_1$ (certains n_j sont possiblement nuls) tels que*

$$G \simeq (\mathbb{Z}/p^k\mathbb{Z})^{n_k} \times (\mathbb{Z}/p^{k-1}\mathbb{Z})^{n_{k-1}} \times \cdots \times (\mathbb{Z}/p\mathbb{Z})^{n_1}.$$

Les nombres k, $n_k \neq 0, \dots, n_1$, sont uniquement déterminés par le groupe G.

Démonstration. On va montrer l'énoncé $P(n)$: "Pour tout groupe abélien G à p^n éléments et tout sous-groupe cyclique $H < G$ d'ordre maximal, il existe un sous-groupe $Q < G$ tel que $Q \cap H = \{e\}$ et $G \cong H \times Q$." par récurrence sur $n \in \mathbb{N} \setminus \{0\}$.

Pour $n = 1$, $P(1)$ découle de la Proposition 5.22. Soit $n \geq 2$ et supposons l'énoncé $P(n-1)$ vrai. Soit G un groupe abélien à p^n éléments. Si G est cyclique, il n'y a rien à demontrer. Sinon, alors il existe un élément $x \in G$ d'ordre maximal p^m avec $m < n$. On remarque que par Lagrange, tout autre élément $y \in G$ est d'ordre p^l avec $1 \leq l \leq m$ par la maximalité de m. Comme $p^l | p^m$, on a en particulier $y^{p^m} = e$.

Soit $H := \langle x \rangle$. On va d'abord montrer qu'il existe un sous-groupe $K < G$ d'orde p avec $K \cap H = \{e\}$. Pour cela, considérons un élément $z \in G - H$ et sa classe $\bar{z} \neq \bar{e}$ dans G/H. Comme $|G/H| = \frac{|G|}{|H|} = p^{n-m}$, $\bar{z}$ est d'ordre p^r pour un certain $r \in \mathbb{N} \setminus \{0\}$ par Lagrange. Cela implique que $z^{p^r} \in H$, donc il existe $a \in \mathbb{Z}$ tel que $z^{p^r} = x^a$. Par la remarque d'avant appliquée à $y = z$, on a que

$$e = z^{p^m} = (z^{p^r})^{p^{m-r}} = x^{ap^{m-r}}$$

donc $\mathrm{ord}(x) = p^m | ap^{m-r}$. Comme $m - r < m$, cela implique que $p | a$, et donc il existe $b \in \mathbb{Z}$ tel que $a = pb$.

Posons $w := x^{-b} z^{p^{r-1}}$. On a que $\overline{w} = \bar{z}^{p^{r-1}} \neq \bar{e}$ par la définition de r, donc $w \notin H$. De plus, $w^p = x^{-a} z^{p^r} = e$, donc w est d'ordre p. On déduit que $K := \langle w \rangle \subset G$ est bien d'ordre p et n'intersecte pas H : $H \cap K$ peut seulement avoir ordre 1 ou p par Lagrange, mais K n'est pas inclus dans H, donc l'intersection est triviale.

Considérons maintenant le groupe quotient $\overline{G} := G/K$ avec la projection canonique $\pi \colon G \to \overline{G}$ et soit $\overline{H} := \pi(H)$. Comme $\ker \pi \cap H = K \cap H = \{e\}$, on a que π induit

un isomorphisme entre H et $\overline{H}$. En particulier, $\overline{H} < \overline{G}$ est un sous-groupe cyclique d'ordre maximal et $\overline{G}$ est un groupe abélien à p^{n-1} éléments, donc l'hypothès de récurrence implique qu'il existe un sous-groupe $\overline{Q} < \overline{G}$ avec $\overline{Q} \cap \overline{H} = \{\bar{e}\}$ et $\overline{G} \cong \overline{H} \times \overline{Q}$. Soit $Q := \pi^{-1}(\overline{Q}) < G$. On va montrer que $H \cap Q$ est trivial et $G \cong H \times Q$.

Soit $y \in H \cap Q$. Alors $\pi(y) \in \overline{H} \cap (Q) = \{\bar{e}\}$ donc $y \in K$. Mais $K \cap H = \{e\}$, donc $y = e$.

Soit $\varphi\colon H \times Q \to G$, $(h, q) \mapsto h \cdot q$. Comme G est abélien, il est facile de voir que φ est un morphsime de groupes. Montrons que φ est injectif. Si $(h, q) \in H \times Q$ satisfait $\varphi(h, q) = hq = e$, alors on a $h = q^{-1} \in H \cap Q = \{e\}$, donc on a bien $\ker \varphi = \{(e, e)\}$. Pour montrer que φ est un isomorphisme, il suffit de montrer l'égalité des ordres des deux groupes.

On remarque d'abord que $K = \pi^{-1}(\bar{e}) \subset \pi^{-1}(\overline{Q}) = Q$, donc $\ker \pi|_Q = K$ et le théorème d'isomorphisme implique que $\pi|_Q$ induit un isomorphisme entre $\overline{Q}$ et Q/K. En particulier, on a que

$$|\overline{Q}| = \frac{|Q|}{|K|}.$$

En utilisant aussi que $|\overline{H}| = |H|$, on en déduit

$$|G| = |\overline{G}| \cdot |K| = |\overline{H}| \cdot |\overline{Q}| \cdot |K| = |H| \cdot |Q|.$$

Dont φ est bien un isomorphisme de groupes et $P(n)$ a été prouvé.

Finalement pour déduire l'énoncé du théorème, soit G un groupe abélien à p^n éléments et soit $H_1 < G$ un sous-groupe maximal cyclique. On a alors que $H_1 \cong \mathbb{Z}/p^{k_1}\mathbb{Z}$ pour un certain $k_1 \in \{1, \dots n\}$ uniquement détérminé. Si $k_1 = n$, on a l'énoncé. Sinon, alors on applique $P(n)$ pour trouver $Q_1 < G$ qui intersecte trivialement H_1 et tel que $G \cong H_1 \times Q_1$. On prend maintenant $H_2 < Q_1$ un sous-groupe maximal cyclique. On a alors $H_2 \cong \mathbb{Z}/p^{k_2}\mathbb{Z}$ pour un certain $k_2 \in \mathbb{N}$. Puisque $H_2 < G$ et que H_1 était maximal, on aurra que $k_2 \leq k_1$. Si $|Q_1| = p^{k_2}$, on déduit que $G \cong \mathbb{Z}/p^{k_1}\mathbb{Z} \times \mathbb{Z}/p^{k_2}\mathbb{Z}$. Sinon, on applique $P(n - k_1)$ au couple (Q_1, H_2) pour trouver Q_2 et ainsi de suite. Comme la suite de nombres positifs $|Q_i|$ décroît strictement, cet algorithme est fini et nous donne donc l'isomorphisme recherché.

Remarquons que à chaque étape, les k_i sont uniquement détérminés par maximalité à partir des propriétés de G, et donc en particulier les nombres $n_k \neq 0, \dots, n_1$ dans le théorème le seront aussi.

□

On obtient donc le corollaire suivant :

Corollaire 7.6 — Tout groupe abélien fini est isomorphe à un produit de groupes cycliques.

Attention, cette décomposition en produit n'est cependant pas unique , comme on le voit par exemple dans

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \simeq \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z},$$

où on utilise le résultat que $\mathbb{Z}/mn\mathbb{Z} \simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ si et seulement si $n \wedge m = 1$. Le théorème suivant donne une forme d'unicité.

Théorème 7.7. *Soit G un groupe abélien fini. Il existe des entiers $r, n_1, \dots, n_r$ uniquement déterminés par G tels que $n_1|n_2|\dots|n_r$ et tels que*

$$G \cong \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_r\mathbb{Z}.$$

Définition 7.8 — La liste $(n_1, \dots, n_r)$ est appelé **l'invariant du groupe** G. On dit aussi que les entiers $n_1, \dots, n_r$ sont **les facteurs invariants** de G.

Démonstration. Soit $n = \prod_{i=1}^{s} p_i^{a_i}$ la décomposition en facteurs premiers de l'ordre du groupe G. On sait que

$$G \simeq G_1 \times \cdots \times G_s$$

où les G_i sont des p_i-groupes ($1 \leq i \leq s$), qui sont donc chacun isomorphes à

$$G_i \simeq (\mathbb{Z}/p_i^k\mathbb{Z})^{n_{i,k}} \times \cdots \times (\mathbb{Z}/p_i\mathbb{Z})^{n_{i,1}}$$

pour des entiers $k = k(i)$ et $n_{i,j}$, $1 \leq j \leq k$. On part de cette décomposition obtenue en produits de termes de la forme $\mathbb{Z}/p_i^{a_i}\mathbb{Z}$, dont on sait déjà qu'elle est unique. On regroupe alors ces termes de la façon suivante :

Pour chaque $1 \leq i \leq s$, prenons la puissance a_i de p_i la plus élevée (donc ici au départ $a_i = k(i)$). On obtient ainsi un terme :

$$\mathbb{Z}/p_1^{a_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_s^{a_s}\mathbb{Z} \simeq \mathbb{Z}/p_1^{a_1} \ldots p_s^{a_s}\mathbb{Z}$$

car les p_i sont des nombres premiers donc les $p_i^{a_i}$ sont premiers entre-eux. On pose alors $m_1 = p_1^{a_1} \ldots p_s^{a_s}$, et on continue en recommençant avec les termes restants qui n'ont pas été pris. On obtient ainsi m_2 etc, le processus s'arrête au bout d'une certaine r-ième étape, quand il n'y a plus de facteurs restants. Par construction, $m_{i+1}|m_i$. On pose alors $n_1 = m_r$, $n_2 = m_{r-1}$,..., $n_r = m_1$ et on a obtenu le résultat. □

Exemple 7.3 — 1) Considérons le groupe

$$M = (\mathbb{Z}/2\mathbb{Z})^3 \oplus (\mathbb{Z}/3\mathbb{Z})^4 \oplus \mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/5^2\mathbb{Z}.$$

On voit que 4 est le nombre de facteurs maximaux dans la décomposition d'un p-groupe (à cause du facteur $(\mathbb{Z}/3\mathbb{Z})^4$), d'où la liste table à 4 colonnes :

$$\begin{array}{llllll} p=2: & 2^0, & 2^1, & 2^1, & 2^1, \\ p=3: & 3^1, & 3^1, & 3^1 & 3^1, \\ p=5: & 5^0, & 5^0, & 5^1, & 5^2, \end{array}$$

d'où

$$a_1 = 3,\ a_2 = 6,\ a_3 = 30,\ a_4 = 150,$$

On a :

$$M \simeq (\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}3/\mathbb{Z} \times \mathbb{Z}/5^2\mathbb{Z})$$

et donc

$$M \simeq (\mathbb{Z}/3\mathbb{Z}) \oplus (\mathbb{Z}/6\mathbb{Z}) \oplus (\mathbb{Z}/30\mathbb{Z}) \oplus (\mathbb{Z}/150\mathbb{Z}).$$

2) Supposons qu'on ait une décomposition de la forme :

$$G \simeq (\mathbb{Z}/4\mathbb{Z}) \times (\mathbb{Z}/8\mathbb{Z})^2 \times (\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/9\mathbb{Z}) \times (\mathbb{Z}/5\mathbb{Z})^2,$$

ici 3 est le nombre maximal de facteurs dans la décomposition d'un p-groupe (dans le cas du premier $p = 2$). On fait donc une table avec 3 colonnes :

$$\begin{array}{cccc} p=2 & 2^2 & 2^3 & 2^3 \\ p=3 & 1 & 3 & 3^2 \\ p=5 & 1 & 5 & 5 \\ a_i & 4 & 120 & 360 \end{array}$$

Je regroupe alors les termes de la façon suivante :

$$\begin{aligned} G &\simeq \big((\mathbb{Z}/8\mathbb{Z}) \times (\mathbb{Z}/9\mathbb{Z}) \times (\mathbb{Z}/5\mathbb{Z})\big) \times \big((\mathbb{Z}/8\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/5\mathbb{Z})\big) \times (\mathbb{Z}/4\mathbb{Z}) \\ &\simeq (\mathbb{Z}/360\mathbb{Z}) \times (\mathbb{Z}/120\mathbb{Z}) \times (\mathbb{Z}/4\mathbb{Z}) \end{aligned}$$

Le théorème des invariant nous dit que

Corollaire 7.9 — Deux groupes abéliens sont isomorphes si, et seulement si, ils ont les mêmes invariants.

Les résultats sur les facteurs invariants permettent de classer tous les groupes abélien d'ordre fixé. Par exemple tous les groupes d'ordre 24 sont isomorphes à l'un seul des groupes suivants :

$$(\mathbb{Z}/2\mathbb{Z})^2 \times \mathbb{Z}/6\mathbb{Z},\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z},\ \mathbb{Z}/24\mathbb{Z}.$$

En effet $(2,2,6)$, $(2,12)$ et 24 sont les seuls uplets d'entiers $(a_1,\ldots,a_k)$ tels que $a_i|a_{i+1}$ et le produit $\prod a_i$ soit égal à 24.