Chapitre 1
Groupes

Le professeur de mathématiques de Niels **Abel** détecte ses aptitudes exceptionnelles et récolte des fonds pour permettre à son élève de suivre des cours à l'université d'Oslo. Le jeune prodige obtient alors une bourse d'études qu'il utilise pour rencontrer les plus grands mathématiciens de l'époque en Allemagne et en France. Atteint de tuberculose, il rentre en Norvège sans le sou. C'est au surlendemain de sa mort, à 27 ans, qu'arrive la lettre annonçant sa nomination à l'université de Berlin. Abel démontre que l'équation du cinquième degré ne peut se résoudre par radicaux, c'est-à-dire qu'il n'existe pas de formule, comme pour le degré 2, donnant les solutions à l'aide des coefficients. Ce résultat sera affiné par Évariste **Galois**. Il introduit une classe importante de fonctions appelées intégrales elliptiques. C'est en son honneur que les groupes commutatifs sont aussi appelés abéliens.

Niels Abel
1802-1829

■■ Objectifs

■ Les incontournables

▷ Connaître les propriétés des groupes

▷ Savoir prouver qu'une partie d'un groupe en est un sous-groupe

▷ Savoir calculer modulo un entier fixé

▷ Savoir reconnaître et classifier les groupes monogènes

▷ Savoir déterminer l'ordre d'un élément d'un groupe.

■ Et plus si affinités…

▷ S'intéresser aux groupes classiques

▷ Utiliser des notions de théorie des groupes pour prouver des résultats en algèbre, en géométrie, etc.

Résumé de cours

Structure de groupe

Définition : *Un **groupe** est un ensemble G muni d'une loi de composition interne notée $*$ vérifiant les propriétés suivantes :*

– La loi $*$ est associative, c'est-à-dire que : pour tous $a, b, c \in G$, on a : $a * (b * c) = (a * b) * c$.

– Elle est munie d'un élément neutre $e \in G$, c'est-à-dire qu'il existe un élément e qui vérifie : $a * e = e * a$ pour tout $a \in G$.

– Tout élément $x \in G$ possède un symétrique, c'est-à-dire qu'il existe $x' \in G$ tel que :

$$x * x' = x' * x = e.$$

Théorème 1.1.— Groupe produit —. Étant donnés deux groupes $(G_1, *)$ et (G_2, Δ), on définit sur le produit cartésien $G = G_1 \times G_2$ l'opération : $(x_1, x_2)\Upsilon(y_1, y_2) = (x_1 * y_1, x_2 \Delta y_2)$.
L'opération Υ définit sur G une structure de groupe.
Par récurrence, on définit, plus généralement, le groupe produit d'une famille finie de groupes.

Définition : *Une partie H du groupe $(G, *)$ est un **sous-groupe** de G lorsqu'elle vérifie les assertions suivantes :*

i) H n'est pas vide ;

ii) H est stable pour $*$, c'est-à-dire : $\forall (x, y) \in H^2$, $x * y$ appartient à H ;

iii) le symétrique de tout élément de H est un élément de H.

Proposition 1.2.— H est un sous-groupe de G si, et seulement si, H contient l'élément neutre e et pour tout $(a, b) \in H \times H$, $a * b^{-1}$ appartient à H.

Remarque : Si H est un sous-groupe de G, alors la loi induite par $*$ sur H est une loi de composition interne, et H, muni de cette loi, est un groupe.

Lemme 1.3.— Toute intersection de sous-groupes de G est un sous-groupe de G.

Théorème-Définition 1.4.— Soit A une partie du groupe G. L'intersection de tous les sous-groupes de G contenant A est un sous-groupe. C'est le plus petit sous-groupe de G contenant A. Ce groupe s'appelle le ***sous-groupe engendré*** par A.

Définition : *Une partie X du groupe G est une partie génératrice lorsque le sous-groupe engendré par X est égal à G.*

Exemple : Soit E un espace euclidien. L'ensemble des réflexions est une partie génératrice du groupe orthogonal $O(E)$.

Théorème 1.5.— Sous-groupes de $\mathbb{Z}$ —. Les sous-groupes de $(\mathbb{Z}, +)$ sont les ensembles $n\mathbb{Z}$ pour $n \in \mathbb{Z}$.

■ Morphismes de groupes

Définition : *Soit $(G,*)$ et (G',Δ) deux groupes. On appelle* ***morphisme de groupes*** *de $(G,*)$ dans (G',Δ) une application f de G dans G' qui vérifie :*

$$\forall (a,b)\in G^2,\ f(a*b)=f(a)\Delta f(b).$$

Proposition 1.6.— Soit f un morphisme de groupes de $(G,*)$ dans (G',Δ).
a) Si H est un sous-groupe de G, $f(H)$ est un sous-groupe de G'. Si H' est un sous-groupe de G', $f^{-1}(H')=\{x\in G\ /\ f(x)\in H'\}$ est un sous-groupe de G.
b) $f(G)$ est un sous-groupe de G, appelé image de f et noté $\mathrm{Im}\, f$.
$f^{-1}(\{e'\})=\{x\in G\ /\ f(x)=e'\}$ est un sous-groupe de G, appelé ***noyau*** de f et noté $\mathsf{Ker}\, f$.
c) f est surjectif si, et seulement si, $\mathsf{Im}\, f=G'$. f est injectif si, et seulement si, $\mathsf{Ker}\, f=\{e\}$.

Définition : *On appelle* ***isomorphisme de groupes*** *de $(G_1,*_1)$ sur $(G_2,*_2)$ un morphisme de groupes bijectif.*

Proposition 1.7.— Si f est un isomorphisme de groupes de $(G_1,*_1)$ sur $(G_2,*_2)$, sa bijection réciproque f^{-1} est un isomorphisme de groupes de $(G_2,*_2)$ sur $(G_1,*_1)$.

■ Groupe $\mathbb{Z}/n\mathbb{Z}$

Définition : Congruence modulo n —. *Fixons un entier $n\in\mathbb{N}$; les entiers $a\in\mathbb{Z}$ et $b\in\mathbb{Z}$ sont dits congrus modulo n lorsque $b-a\in n\mathbb{Z}$. On note alors $a\mathcal{R}_n b$.*

Proposition 1.8.— La relation $\mathcal{R}_n$ de congruence modulo n est une relation d'équivalence sur $\mathbb{Z}$.

Notation : *Dans la suite, $\bar{k}$ désigne la classe d'équivalence de $k\in\mathbb{Z}$.*
On a donc : $\bar{0}=n\mathbb{Z}$, $\bar{1}=\{\ldots,1-2n,1-n,1,n+1,2n+1\ldots\}$, *etc.*
L'ensemble dont les éléments sont les classes d'équivalence selon $\mathcal{R}_n$ se note $\mathbb{Z}/n\mathbb{Z}$.

Proposition 1.9.— Pour $n\in\mathbb{N}^*$ fixé, $\mathbb{Z}/n\mathbb{Z}$ est un ensemble fini de cardinal n :

$$\boxed{\mathbb{Z}/n\mathbb{Z}=\{\overline{0},\overline{1},\ldots,\overline{n-1}\}\ .}$$

Lemme 1.10.— Soit $(a,a',b,b')\in\mathbb{Z}^4$ avec $a\ \mathcal{R}_n\ a'$ et $b\ \mathcal{R}_n\ b'$, alors $a+b\ \mathcal{R}_n\ a'+b'$. On dit que la relation $\mathcal{R}_n$ est *compatible* avec l'addition. On peut donc définir sur $\mathbb{Z}/n\mathbb{Z}$ l'opération :

$$u+v=\overline{a+b},\ \text{où } u=\bar{a} \text{ et } v=\bar{b}\ .$$

L'élément de $\mathbb{Z}/n\mathbb{Z}$ ainsi défini ne dépend pas des représentants choisis.

Théorème 1.11.— Muni de l'addition ainsi définie, l'ensemble $\mathbb{Z}/n\mathbb{Z}$ est un groupe commutatif. L'application $\mathbb{Z}\to\mathbb{Z}/n\mathbb{Z}, z\mapsto\bar{z}$ est un morphisme de groupes surjectif. On l'appelle le morphisme canonique, ou la surjection canonique, de $\mathbb{Z}$ vers $\mathbb{Z}/n\mathbb{Z}$.

■ Groupe engendré par un élément

Notation : *En général, la loi du groupe G est noté multiplicativement et sans symbole : $ab = a * b$; l'élément neutre se note e ou 1_G, le symétrique d'un élément x est noté x^{-1}.*

Lemme 1.12.— Soit $(G, .)$ un groupe et $a \in G$. Le sous-groupe engendré par a est :
$$G_a = \{a^k,\ k \in \mathbb{Z}\}.$$

Définition : *Un groupe G est dit **monogène** lorsqu'il est engendré par un seul élément. Tout élément qui l'engendre s'appelle un générateur.*

Définition : *Un groupe **cyclique** est un groupe monogène fini, c'est-à-dire fini et engendré par un seul élément. Tout élément qui l'engendre s'appelle un générateur.*

Exemple : Le groupe $\mathbb{Z}/n\mathbb{Z}$ est cyclique engendré par $\bar{1}$ car $\bar{k} = k\ 1 = 1 + 1 + \ldots + 1$ (k fois). Plus généralement :

Théorème 1.13.— Les générateurs de $\mathbb{Z}/n\mathbb{Z}$ sont les $\bar{k}$ avec $k \wedge n = 1$.

Théorème 1.14.— Un groupe monogène infini est isomorphe à $\mathbb{Z}$.
Un groupe cyclique de cardinal n est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

Corollaire 1.15.— Le groupe $\mathbb{U}_n = \{e^{2ik\pi/n},\ 0 \leqslant k < n\}$ des racines n-ièmes de l'unité est engendré par $e^{2i\pi/n}$ puisque $e^{2ik\pi/n} = (e^{2i\pi/n})^k$. Il est donc isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

■ Ordre d'un élément d'un groupe

Définition : *Soit $(G, .)$ un groupe. On dit que l'élément x de G est **d'ordre fini** lorsque le cardinal du sous-groupe de G engendré par x est fini ; celui-ci est alors appelé l'ordre de l'élément x.*

Théorème 1.16.— Si x est d'ordre fini d et si e désigne le neutre de G, alors, pour n dans $\mathbb{Z}$, on a :
$$x^n = e \Longleftrightarrow d|n.$$

Théorème 1.17.— Si G est un groupe fini, alors tout élément de G est d'ordre fini, et son ordre divise Card (G).

■ Groupe symétrique

Définition : Groupe symétrique —. *Le groupe symétrique $\mathcal{S}_n$ est l'ensemble des bijections de l'ensemble $\{1, 2, \ldots, n\}$ dans lui-même (appelées **permutations** de $\{1, \ldots, n\}$), muni de la composition des applications. Le groupe symétrique $\mathcal{S}_n$ possède $n!$ éléments.*

Remarque : $\mathcal{S}_1 = \{\mathrm{id}\}$, aussi, dans la suite de ce paragraphe, on suppose que $n \geqslant 2$.

Proposition 1.18.— L'application $\epsilon : \mathcal{S}_n \to \{-1, 1\}$, $\sigma \mapsto \prod_{1 \leqslant i < j \leqslant n} \frac{\sigma(i) - \sigma(j)}{i - j}$ est un morphisme de groupes, appelé la ***signature***.
Son noyau $\mathsf{Ker}\,(\epsilon)$ est un sous-groupe de cardinal $n!/2$, on le note $\mathcal{A}_n$ et on l'appelle le *groupe alterné* d'indice n.

Vocabulaire : *Une transposition intervertit deux éléments et laisse fixe tous les autres.*
Plus généralement, on nomme k-cycle, ou cycle de longueur k, une bijection qui opère une permutation circulaire sur k éléments $a_1, a_2, \ldots a_k$ et laisse fixe les autres. On le note $(a_1, a_2, \ldots a_k)$.
Par exemple une transposition est un 2-cycle.

Proposition 1.19.— Un k-cycle est d'ordre k et a pour signature $(-1)^{k-1}$.

Théorème 1.20.— Les transpositions engendrent $\mathcal{S}_n$.

Remarque : Chaque élément de $\mathcal{S}_n \setminus \{\mathrm{id}\}$ s'écrit, de manière unique à l'ordre près des facteurs, comme composée (on dit « produit ») de cycles disjoints.

Méthodes

Comment montrer qu'un ensemble muni d'une loi de composition interne est un groupe

❑ **Méthode 1.1.—** Pour montrer que $(G, .)$ est un groupe, on peut :
- Utiliser la définition d'un groupe.
- Montrer que c'est un sous-groupe d'un groupe connu.

Mise en œuvre : exercice 1.1, **exercice 1.3**, **exercice 1.9**, **exercice 1.10**.

Remarques : ▶ Avant d'utiliser la définition d'un groupe, regardez si l'ensemble étudié n'est pas inclus dans un groupe déjà connu. Ceci évite de démontrer l'associativité et de chercher un élément neutre.
▶ Parfois, l'ensemble étudié est composé de fonctions. Il est utile de se rappeler que l'ensemble des fonctions d'un ensemble quelconque dans un groupe $(G, *)$ est lui-même un groupe pour l'opération, encore notée $*$, définie par : $f * g : x \mapsto f(x) * g(x)$.
▶ Les axiomes de groupe s'appliquent à une loi de composition interne. Ceci implique que, pour montrer que $(G, *)$ est un groupe, il faut d'abord vérifier la stabilité de la loi, c'est-à-dire que le produit de deux éléments de G est bien un élément de G.

Comment montrer qu'un sous-ensemble H d'un groupe G est un groupe

❑ **Méthode 1.2.—** Soit $(G, .)$ un groupe. Soit H une partie de G. Pour montrer que H est un sous-groupe de G, on peut :
- Utiliser la caractérisation des sous-groupes.
- Montrer que H est l'intersection d'une famille de sous-groupes.
- Montrer que H est l'image d'un groupe par un morphisme.
- Montrer que H est le noyau d'un morphisme de groupes (ou, plus généralement, l'image réciproque d'un sous-groupe par un morphisme).

Mise en œuvre : exercice 1.1, **exercice 1.2**, **exercice 1.9**.

Remarques : ▶ Pour montrer que H est un sous-groupe de G en utilisant la caractérisation des sous-groupes, il faut montrer que :
1 - H n'est pas vide. En général, on justifie qu'il contient l'élément neutre de G.
2 - H est stable par la loi du groupe : c'est fondamental, ceci revient à montrer que la loi est une loi de composition interne pour H.
3 - Le symétrique de tout élément a de H est encore dans H. Souvent, on connaît déjà la forme de ce symétrique. Il suffit alors seulement de montrer qu'il est dans H.
▶ On peut condenser les deux assertions 2 et 3 en une seule propriété :

$$\forall (a, b) \in H^2,\ a * b^{-1} \in H.$$

Ceci peut faire gagner du temps. Il ne faut l'utiliser que si la forme du symétrique dans G est connue. Dans les autres cas, il est préférable de séparer la stabilité et l'existence du symétrique.

Exemple : *Soit E un espace vectoriel de dimension n. Montrer que*
$$\mathrm{SL}(E) = \{f \in \mathcal{L}(E) \ / \ \mathsf{Det}\,(f) = 1\}$$
est un sous-groupe de $(GL(E), \circ)$.
On considère $\varphi : f \mapsto \mathsf{Det}\,(f)$. C'est un morphisme du groupe $\mathrm{GL}(E)$ dans $(\mathbb{K}^*, \times)$ car, pour tous $f, g \in \mathrm{GL}(E)$, $\mathsf{Det}\,(f \circ g) = \mathsf{Det}\,(f) \times \mathsf{Det}\,(g)$. L'élément neutre de $(\mathbb{K}^*, \times)$ étant 1, $\mathrm{SL}(E)$ est le noyau de φ, c'est donc un sous-groupe de $(\mathrm{GL}(E), \circ)$.

Exemple : L'ensemble des fonctions continues, bornées de $\mathbb{R}$ dans lui-même est un groupe pour l'addition des fonctions, car c'est l'intersection de l'ensemble des fonctions continues et de celui des fonctions bornées qui sont, d'après le cours, des groupes.

■ Comment rechercher l'ordre d'un élément d'un groupe

❑ **Méthode 1.3.—** Soit G un groupe, noté mutiplicativement, et soit $a \in G$. Pour déterminer l'ordre de l'élément a, on peut :

- Calculer les puissances successives de l'élément a jusqu'à l'obtention de l'élément neutre.
- Trouver une propriété qui montre qu'aucune puissance de a ne peut être le neutre.

Remarque : Si le groupe est fini, tout élément a un ordre fini qui divise l'ordre, c'est-à-dire le cardinal, du groupe.

Mise en œuvre : exercice 1.9, **exercice 1.12**, **exercice 1.14**.

Exemple : *Chercher l'ordre de chacun des éléments $M = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$, $N = \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix}$ et $P = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ dans le groupe $GL_2(\mathbb{C})$ des matrices inversibles (2,2) à coefficients complexes.*
Le calcul de $M^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ montre que $M^3 \neq I_2$ et $M^4 = I_2$ donc l'ordre de M est 4.
Comme $\mathsf{Det}\,(N) = -2$, on a : $\forall n \in \mathbb{N}^*$, $\mathsf{Det}\,(N^n) = (-2)^n \neq 1$, donc N est d'ordre infini.
On obtient $P^2 = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$, et on montre par une récurrence facile que : $\forall n \in \mathbb{N}$, $P^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$.
Ainsi, pour tout $n > 0$, $P^n \neq I_2$, ce qui montre que P est d'ordre infini.

Exemple : *Soit $z = re^{2i\pi\theta} \in \mathbb{C}$ avec $r > 0$ et $\theta \in \mathbb{R}$. Chercher l'ordre de z dans le groupe $(\mathbb{C}^*, \times)$ des nombres complexes non nuls.*
– Si $r \neq 1$, alors, pour $n \geqslant 1$, $|z^n| = r^n \neq 1$ donc $z^n \neq 1$. Ainsi, l'ordre de z est infini.
– Si $r = 1$ alors $z^n = 1$ si, et seulement si, $n\theta \in \mathbb{Z}$. Si θ est irrationnel, ceci est impossible pour $n \neq 0$, donc z est d'ordre infini. Si θ est rationnel, $\theta = p/q$ avec $p \wedge q = 1$ et $q > 0$, alors q est le plus petit entier strictement positif tel que $q\theta \in \mathbb{Z}$. On en déduit que l'ordre de z est égal à q.