Chapitre 2

Groupes

Introduction : lois de composition

Une loi de composition interne sur un ensemble G est une application $G \times G \to G$. L'image du couple (x, y) est notée avec un symbole : suivant le contexte $x+y$, $x \times y$, $x \star y$ ...

Définition 2.0.1. a) La loi de composition $\star$ est commutative sur G si et seulement si :

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

b) La loi de composition $\star$ est associative sur G si et seulement si :

$$\forall x \in G,\ \forall y \in G,\ \forall z \in G,\ ((x \star y) \star z) = (x \star (y \star z))\ .$$

c) e est élément neutre pour $\star$ dans G si et seulement si :

$$\forall x \in G,\ x \star e = e \star x = x\ .$$

d) x' est symétrique de x pour la loi de composition $\star$ de neutre e, si et seulement si :

$$x \star x' = x' \star x = e$$

Remarque 2.0.2. Il y a unicité du neutre et du symétrique.

2.1 Structure de groupe

Définition 2.1.1. a) Une loi de composition $\star$ sur G définit une structure de groupe si et seulement si elle associative, admet un élément neutre, et si tout élément de G admet un élément symétrique.

Le groupe $(G, \star)$ est commutatif (ou abélien) si et seulement si la loi de composition $\star$ est commutative.

En notation additive, l'élément symétrique est appelé opposé et noté $-x$; en notation multiplicative l'élément symétrique est appelé inverse et noté x^{-1}.

Exemples 2.1.2. $(\mathbb{Z}, +)$ est un groupe.
Le groupe multiplicatif des racines complexes n-ièmes de 1 : $(U_n, \times)$.
Le groupe des bijections de X noté $(\mathcal{B}(X), \circ)$.
Le groupe symétrique $\mathcal{S}_n = \mathcal{B}(\{1, \ldots, n\})$.

2.2 Sous-groupe

Définition 2.2.1. Une partie H d'un groupe $(G, *)$ est une groupe si et seulement si elle est non vide et stable pour l'opération $*$ et la symétrisation.

On peut reformuler la définition :

a) Le neutre e est dans H ;
b) pour tous x et y dans H, $x * y$ est dans H ;
c) pour tout x dans H, le symétrique x' est dans H.

2.3 Ordre d'un élément

Définition 2.3.1. Soit x un élément d'un groupe G. Le sous-groupe engendré par x, noté $< x >$ est le plus petit sous-groupe qui contient x ; on dit alors que x est un générateur u sous-groupe $< x >$.

Justification de l'existence du sous-groupe engendré par x, et plus généralement du sous-groupe engendré par une partie A d'un groupe G : l'intersection de plusieurs sous-groupe est un sous-groupe ; l'intersection de tous les sous-groupes qui contiennent x (resp. A) est le plus petit sous-groupe qui contient x (resp. A).

Définition 2.3.2. Un élément x d'un groupe G est d'ordre fini si et seulement si le sous-groupe $< x >$ est fini. Dans ce cas l'ordre de x est le nombre d'éléments du sous-groupe $< x >$.

Proposition 2.3.3. *Un élément x d'un groupe G est fini si et seulement s'il existe un entier $n > 0$ tel qu'en composant n exemplaires de x on retrouve le neutre, et l'ordre de x est le plus petit parmi ces entiers n.*

En notation additive, la composition de n fois x s'écrit nx, et pour $n = -m < 0$, nx est l'élément symétrique de mx (l'opposé).

En notation multiplicative, la composition de n fois x s'écrit x^n, et pour $n = -m < 0$, x^n est l'élément symétrique de x^m.

Lemme 2.3.4. *Soit G un groupe noté multiplicativement. Le sous-groupe engendré par x est l'ensemble des x^n, $n \in \mathbb{Z}$.*

Exemple 2.3.5. Dans le groupe $(\mathbb{C}^*, \times)$, $e^{\frac{i\pi}{3}}$ est d'ordre 6.

2.4 Morphisme de groupe

Définition 2.4.1. Soient $(G, *)$ et $(G', \top)$ deux groupes. Une application $f : G \to G'$ est un morphisme de groupe si et seulement si :

$$\forall x \in G \ , \ \forall y \in G \ , \ , f(x * y) = f(x) \top f(y) \ .$$

Exemple 2.4.2. L'application logarithme est un morphisme du groupe $(]0, +\infty[, \times)$ vers le groupe $(\mathbb{R}, +)$.

Exemple 2.4.3. Soit x un élément dans un groupe G noté multicativement. L'application $g_x : \mathbb{Z} \to G$ qui à n associe x^n est un morphisme de groupe.

Définition 2.4.4. Le noyau d'un morphisme de groupe $f : G \to G'$ est l'ensemble des éléments dont l'image est le neutre e' de G'.

Proposition 2.4.5. *Soit $f : G \to G'$ un morphisme de groupe.*
a) Le noyau de f est un sous-groupe de G.
b) f est injective si et seulement si son noyau ne contient que le neutre e de G.

Définition 2.4.6. L'image d'un morphisme de groupe $f : G \to G'$ est l'ensemble :

$$\mathrm{Im}(f) = f(G) = \{f(x), \ x \in G\} \ .$$

Proposition 2.4.7. *Soit $f : G \to G'$ un morphisme de groupe.*
a) L'image de f est un sous-groupe de G'.
b) f est surjective si et seulement si son image est égale à G'.

2.5 Groupe quotient

2.5.1 Cas de $\mathbb{Z}$

Définition 2.5.1. Soit n un entier. On dit que deux entiers x et y sont congrus modulo n, et on écrit :

$$x \equiv y \ (\mod n)$$

si et seulement si $x - y$ est multiple de n.

La relation de congruence modulo n est une relation d'équivalence. Pour $x \in \mathbb{Z}$, la classe d'équivalence de x est : $x + n\mathbb{Z}$.

Définition 2.5.2. On appelle ensemble quotient de $\mathbb{Z}$ par le sous-groupe $n\mathbb{Z}$ l'ensemble des classes d'équivalence ; on note ce quotient $\mathbb{Z}/n\mathbb{Z}$.

Remarque 2.5.3. La classe de x, qui est un sous-ensemble de $\mathbb{Z}$ et un élément de $\mathbb{Z}/n\mathbb{Z}$ est habituellement noté $\overline{x}$.

On définit une addition des classes en additionnant les représentants :

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

Proposition 2.5.4. *L'addition des classes est bien définie et $(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe. Ce groupe est engendré par la classe $\overline{1}$ qui est d'ordre n.*

2.5.2 Cas abélien

Soit $(G, +)$ un groupe commutatif et H un sous-groupe. Les classes modulo H sont les $x + H = \{x + h,\ h \in H\}$; la classe de x est habituellement notée $\overline{x}$. On note G/H l'ensemble des classes, et on définit une addition des classes en additionnant les représentants :

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

Proposition 2.5.5. *L'addition des classes est bien définie et $(G/H, +)$ est un groupe.*

2.5.3 Cas général

Soit G un groupe dont la loi de groupe est notée comme un produit, et H un sous-groupe. Pour $x \in G$, on a une classe à droite modulo H :

$$xH = \{xh,\ h \in G\} \ ,$$

et une classe à gauche modulo H :

$$Hx = \{hx,\ h \in G\} \ .$$

En général les classes à droite ne sont pas les mêmes que les classes à gauche, et ne forment pas un groupe.

2.6 Le théorème de Lagrange

Soit H un sous-groupe d'un groupe fini G.

Théorème 2.6.1. *Le cardinal du sous-groupe H divise le cardinal de G. En particulier, l'ordre de tout élément de G divise le cardinal de G.*

La preuve repose sur le fait que toutes les classes à droite ont le même nombre d'éléments.

Définition 2.6.2. On appelle indice de H dans G, et on note $[G : H]$ le nombre de classes à droite modulo H, aussi égal au quotient du cardinal de G par le cardinal de H.

Exercice 2.6.3. Démontrer que tout groupe G dont le cardinal est un nombre premier p est isomorphe à $\mathbb{Z}/p\mathbb{Z}$.