Chapitre 2

Groupes

Introduction :lois de composition

Une loi de composition interne sur un ensemble E est une application $E \times E \to E$. L'image du couple (x, y) est noté avec un symbole : suivant le contexte $x + y$, $x \times y$, $x \star y$ ...
Associativité, commutativité.
Neutre, unicité ; élément symétrique, unicité.

2.1 Structure de groupe

Définition.
Exemples :$(\mathbb{Z}, +)$ est un groupe ;
groupe des bijections de X noté $(\mathcal{B}(X), \circ)$, cas du 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 que x 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 2.3.2. *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 2.3.3. *Soit G un groupe noté multiplicativement. Le sous-groupe engendré par x est l'ensemble des x^n, $n \in \mathbb{Z}$.*

Exemple 2.3.4. Ordre des éléments dans le groupe symétrique $\mathcal{S}_3$.

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 :

$$x \equiv y \pmod{n}$$

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 :

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

et une classe à gauche :

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

Définition 2.5.6. Le sous-groupe H est distingué (ou normal) si et seulement si pour tout x dans G, on a : $Hx = xH$.

Remarque 2.5.7. La définition est équivalente à :

$$\forall x \in G \ , \ \forall h \in H \ , xhx^{-1} \in H \ .$$

Si H est un sous-groupe distingué, on note G/H l'ensemble des classes, et on définit une opération sur les classes en composant les représentants :

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

Proposition 2.5.8. *Si H est un sous-groupe distingué, alors l'opération sur les classes est bien définie et G/H est 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 $\mathbb{Z}/p\mathbb{Z}$.

2.7 Groupe des permutations

On note $\mathcal{S}_n$ le groupe des permutations de $\{1, 2, \ldots, n\}$

Définition 2.7.1. La transposition (ij) est la permutation qui échange i et j et ne change pas les autres éléments.

Définition 2.7.2. Le cycle d'ordre 3 : (ijk) est la permutation σ définie par :

$$\sigma(i) = j \ , \ \sigma(j) = k \ \sigma(k) = i \ , \ \forall x \notin \{i, j, k\} \ , \ \sigma(x) = x \ .$$

Définition 2.7.3. Le cycle d'ordre p : $(i_1, \ldots, i_p)$ est la permutation σ définie par :

$$\sigma(i_1) = i_2 \ , \ \sigma(i_2) = i_3 \ , \ldots, \sigma(i_p) = i_1, \ \forall x \notin \{i_1, \ldots, i_p\} \ , \ \sigma(x) = x \ .$$

L'ensemble $\{i_1, \ldots, i_p\}$ s'appelle le support du cycle.

Théorème 2.7.4. *Toute permutation se décompose en cycles à supports disjoints. Cette décomposition commute et est unique à l'ordre près.*

Remarque 2.7.5. On peut déduire l'ordre de la permutation.

Théorème 2.7.6. *Toute permutation peut s'écrire comme composée de transpositions.*

Définition 2.7.7. Soit $\sigma \in \mathcal{S}_n$. On appelle inversion pour la permutation σ tout couple (i, j) tel que : $1 \leq i < j \leq n$ et $\sigma(i) > \sigma(j)$.

On note I_σ l'ensemble des inversions pour σ, et on pose :

$$\epsilon_\sigma = (-1)^{\mathrm{card}(I_\sigma)} \ .$$

Proposition 2.7.8.

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

Théorème 2.7.9. *L'application qui à σ associe ϵ_σ est l'unique morphisme de groupe de $\mathcal{S}_n$ vers $\{\pm 1\}$ qui vaut -1 sur les transpositions.*

2.8 Compléments

2.8.1 Groupes de matrices

On note $GL(n, \mathbb{K})$ ou $GL_n(\mathbb{K})$ les matrices carrées d'ordre n à coefficients dans $\mathbb{K}$ qui sont inversibles. Avec la multiplication ces matrices forment un groupe.

Dans le cas où $\mathbb{K}$ est un corps : $\mathbb{R}$, $\mathbb{C}$ ou $\mathbb{Q}$, ce sont les matrices de déterminant non nul.

Dans le cas $\mathbb{K} = \mathbb{Z}$, il s'agit des matrices de déterminant ± 1.

Fin du cours du 13/02

2.8.2 Le produit direct

Soit $(G_1, \square)$ et $(G_2, \diamond)$ deux groupes, on définit sur le produit cartésien $G_1 \times G_2$ une loi de composition $*$:

$$(x_1, x_2) * (y_1, y_2) = (x_1 \square y_1, x_2 \diamond y_2)$$

Proposition 2.8.1. *$(G_1 \times G_2, *)$ est un groupe appelé le produit direct de G_1 et G_2, noté simplement $G_1 \times G_2$.*

Exemple.
$\mathbb{Z}/6 \simeq \mathbb{Z}/2 \times \mathbb{Z}/3$.

2.8.3 Théorème de Cauchy

Théorème 2.8.2. *Soit G un groupe fini de cardinal n, et p un nombre premier qui divise n, alors G contient au moins un élément d'ordre p.*

2.8.4 Ordre des permutations

Théorème 2.8.3. *Soit σ une permutation décomposée en cycles à supports disjoints, alors l'ordre de σ est le PPCM des longueurs des cycles de la décomposition.*