4 Leçon 104 : Groupes finis. Exemples et applications.

I. Généralités sur les groupes finis

1. Notion d'ordre [BER] [ROM]

Ordre d'un groupe et d'un élément, classes à gauche, th de Lagrange, sous-groupe distingué

2. Actions de groupe [ULM] [BER]

Action de groupe, morphisme dans $\mathcal{S}_n$, théorème de Cayley, stabilisateur, orbite, point fixe, formule des classes, équation des classes, DEV 1 : formule de Burnside + application, p-groupe

II. Un groupe fini abélien : $\mathbb{Z}/n\mathbb{Z}$

1. Le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$ et cyclicité [BER] [ROM]

Définition de $\mathbb{Z}/n\mathbb{Z}$, groupe monogène, groupe cyclique, sous-groupes de $\mathbb{Z}/n\mathbb{Z}$

DEV 2 : classification des groupes d'ordre p^2

2. Théorème de structure [BER]

Théorème chinois, théorème de structure, annexe sur les groupes abéliens de petit ordre

3. Le groupe des inversibles $(\mathbb{Z}/n\mathbb{Z})^\times$ [ROM]

Dèf de $(\mathbb{Z}/n\mathbb{Z})^\times$, inversibles de $\mathbb{Z}/n\mathbb{Z}$, cardinal de $(\mathbb{Z}/n\mathbb{Z})^\times$, sous-groupe fini du groupe multiplicatif d'un corps

III. Un groupe fini non abélien : $\mathcal{S}_n$ [BER]

Dèf de $\mathcal{S}_n$, produit de cycles, ordre d'une permutation, générateurs de $\mathcal{S}_n$, signature, groupe alterné, générateurs de $\mathcal{A}_n$, sous-groupes distingués de $\mathcal{S}_n$, $\mathcal{A}_n$ est simple, centre de $\mathcal{S}_n$

Annexe :

Classification des groupes abéliens de petit ordre [BER]

Présentation :

- La notion de groupes est omniprésente en mathématiques : géométrie, étude des racines des polynômes… Elle possède aussi des applications dans de nombreux domaines, par exemple en chimie pour observer la structure de certaines molécules.

  C'est une des premières structures algébriques enseignées qui apporte une richesse mathématique.

- Le théorème de Lagrange est fondamental car permet d'obtenir des informations sur le groupe à partir de son cardinal. Le corollaire qui dit que l'ordre de tout élément divise l'ordre du groupe est utilisé à de nombreuses reprises lorsque l'on travaille dans des groupes.

- L'étude de $\mathbb{Z}/n\mathbb{Z}$ est motivée par le fait que tout groupe cyclique est isomorphe à un $\mathbb{Z}/n\mathbb{Z}$, et donc qu'il suffit d'étudier ce groupe en particulier. De plus, les groupes $\mathbb{Z}/n\mathbb{Z}$ apparaissent dans le théorème de structure des groupes abéliens finis.

- L'étude de $\mathcal{S}_n$ est motivée par le théorème de Cayley, car tout groupe fini d'odre n est isomorphe à un sous-groupe de $\mathcal{S}_n$.

- Le fait que $\mathcal{A}_n$ soit simple pour $n \geqslant 5$ a une importance historique car il permet de montrer que les solutions des équations polynomiales de degré supérieur ou égal à 5 ne peuvent s'écrire à l'aide des quatres opérations élémentaires et de la racine carrée.

Développements :

- Formule de Burnside + application

  - Algèbre : le grand combat, Berhuy, p172

  - Carnet de voyage en Algébrie, Caldero-Peronnier, p163

- Classification des groupes d'ordre p^2

  - L'oral à l'agrégation de mathématiques - Une sélection de développements , Isenmann-Pecatte, p106

Références :

- [BER] Algèbre : le grand combat, Berhuy
- [ROM] Mathématiques pour l'agrégation : Algèbre et géométrie, Rombaldi
- [ULM] Théorie des Groupes, Ulmer

Leçon 104 : Groupes finis. Exemples et applications

Dans cette leçon on considère un groupe $(G, *)$, noté G, d'élément neutre 1.

I Généralités sur les groupes finis

1) Notion d'ordre [BER] [ROM]

Déf 1 : Si G est un groupe fini, son nombre d'éléments $|G|$ est appelé l'ordre de G.

Exemple 2 : $\mathfrak{S}_n$ est d'ordre $n!$ et $\mathbb{Z}/n\mathbb{Z}$ est d'ordre n.

Déf 3 : On appelle ordre de $g \in G$ l'ordre de $\langle g \rangle$. On le note $\mathrm{ord}(g)$.

Prop 4 : Soit $g \in G$. Alors g est d'ordre fini ssi il existe $n > 0$ tel que $g^n = 1$. Alors $\mathrm{ord}(g)$ est le plus petit entier $n > 0$ tel que $g^n = 1$. On a : $\langle g \rangle = \{1, g, \dots, g^{n-1}\}$

Pour $n \in \mathbb{Z}$, on a : $g^n = 1 \iff \mathrm{ord}(g) \mid n$.

Corollaire 5 : Soit $g \in G$ d'ordre fini. Alors pour tout $d \geq 1$, g^d est d'ordre fini et $\mathrm{ord}(g^d) = \dfrac{\mathrm{ord}(g)}{\mathrm{pgcd}(d, \mathrm{ord}(g))}$

Prop 6 : Soit H un sous-groupe de G. La relation définie par $g_1 \sim g_2 \iff g_1^{-1} g_2 \in H$ est une relation d'équivalence

Notation 7 : On note $\bar{g} = gH$ la classe d'équivalence de $g \in G$. L'ensemble de ces classes est noté G/H, appelé ensemble des classes à gauche modulo H

On peut définir de manière analogue $H \backslash G = \{Hg ; g \in G\}$ l'ensemble des classes à droite modulo H.

Déf 8 : Soit H sous-groupe de G. Le cardinal de G/H est noté $[G : H]$ et est appelé indice de H dans G.

Théorème 9 (de Lagrange) : Soit G un groupe fini et H sous groupe de G. Alors $|G| = [G : H] \times |H|$, donc l'ordre de H divise celui de G.

Corollaire 10 : L'ordre de tout élément divise l'ordre du groupe.

Déf 11 : On dit qu'un sous-groupe H de G est distingué si on a $gH = Hg$ pour tout $g \in G$. On note $H \trianglelefteq G$.

Exemple 12 : $\{1\}$ et G sont toujours distingués dans G.

Si G est commutatif, tout sous-groupe est distingué.

Le noyau d'un morphisme est distingué.

Prop 13 : Soit $H \trianglelefteq G$. L'ensemble quotient G/H muni de $gH \cdot g'H = gg'H$ est un groupe.

Déf 14 : On dit que G est simple si ses seuls sous-groupes distingués sont $\{1\}$ et G.

2) Actions de groupe [ULM] [BER]

Soit G un groupe et X un ensemble.

Déf 15 : On appelle action à gauche de G sur X tout application $G \times X \to X$, $(g, x) \mapsto g \cdot x$ telle que : 1) $1 \cdot x = x \quad \forall x \in X$; 2) $g \cdot (h \cdot x) = (gh) \cdot x \quad \forall g, h \in G, \forall x \in X$

Remarque 16 : Il est équivalent de se donner un morphisme de groupes de G dans $\mathfrak{S}(X)$.

Exemple 17 : G agit sur lui-même par translation à gauche

Théorème 18 (de Cayley) : Tout groupe fini d'ordre n est isomorphe à un sous-groupe de $\mathfrak{S}_n$.

Déf 19 : L'ensemble $\mathrm{Stab}(x) = \{g \in G ; g \cdot x = x\} \subset G$ est appelé le stabilisateur de x.

Soit $x \in X$. L'ensemble $\mathcal{O}_x = \{g \cdot x ; g \in G\} \subset X$ est appelé orbite de x sous l'action de G.

On dit que $x \in X$ est un point fixe si $g \cdot x = x \ \forall g \in G$. On note X^G l'ensemble des points fixes.

Prop 20 : Soit $x \in X$. L'application suivante est bijective :

$$f_x : \begin{array}{ccc} G/\mathrm{Stab}(x) & \longrightarrow & \mathcal{O}_x \\ \bar{g} & \longmapsto & g \cdot x \end{array}$$

Corollaire 21 : Si G et X sont finis, alors pour tout $x \in X$, $|G| = |\mathcal{O}_x| \times |\mathrm{Stab}(x)|$.

Théorème 22 (équation des classes) : Si $\{x_1, \dots, x_n\}$ est un système de représentants des orbites, alors :

$$|X| = \sum_{i=1}^{n} |\mathcal{O}_{x_i}| = \sum_{i=1}^{n} \frac{|G|}{|\mathrm{Stab}(x_i)|}$$

BER 179

Déf 23 : Soit $g \in G$. On note $Fix(g) = \{x \in X \ ; \ g \cdot x = x\}$.

Prop 24 (formule de Burnside) : Soit $\mathcal{R}$ l'ensemble des orbites de X sous l'action de G. Alors :

$$|\mathcal{R}| = \frac{1}{|G|} \sum_{g \in G} |Fix(g)|$$

LM 69

Déf 25 : Soit p premier. Un p-groupe est un groupe d'ordre une puissance de p.

Prop 26 : Soit G un p-groupe. Alors : $|x^G| \equiv |x| \ [p]$

Théorème 27 (de Cauchy) : Soit G tel que p premier divise l'ordre de G. Alors il existe un élément d'ordre p dans G.

LM 72

Prop 28 : Soit G un groupe fini et p le + petit nombre premier divisant $|G|$. Alors tout sous-groupe H d'indice p est distingué dans G.

LM 70

Prop 29 : Le centre d'un p-groupe est non-trivial.

Théorème 30 : Tout groupe d'ordre p^2 est abélien.

II Un groupe fini abélien : $\mathbb{Z}/n\mathbb{Z}$

1) Le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$ et cyclicité [BER] [ROM]

BER 31

Lemme 31 : La relation de congruence modulo n est une relation d'équivalence sur $\mathbb{Z}$. On note $\mathbb{Z}/n\mathbb{Z}$ l'ensemble quotient. Si $a \in \mathbb{Z}$, on note $\bar{a}$ sa classe d'équivalence. On peut munir $\mathbb{Z}/n\mathbb{Z}$ d'une structure d'anneau.

BER 32

Lemme 32 : Pour tout $n \geq 1$, l'anneau $\mathbb{Z}/n\mathbb{Z}$ possède n éléments qui sont $\bar{0}, \bar{1}, \dots, \overline{n-1}$.

ROM 13

Déf 33 : On dit que G est monogène s'il existe $g \in G$ tel que $G = \langle g \rangle$. Si de plus G est fini, on dit qu'il est cyclique.

Exemple 34 : $(\mathbb{Z}, +)$ est monogène, engendré par 1.
$(\mathbb{Z}/n\mathbb{Z}, +)$ est cyclique d'ordre n, engendré par $\bar{1}$.

Théorème 35 : Tout groupe monogène infini est isomorphe à $\mathbb{Z}$.

Tout groupe cyclique d'ordre n est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

Exemple 36 : Le groupe U_n des racines n-ièmes de l'unité est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

Corollaire 37 : Tout groupe d'ordre p premier est cyclique et isomorphe à $\mathbb{Z}/p\mathbb{Z}$.

Théorème 38 : Pour $n \geq 2$, tous les sous-groupes de $\mathbb{Z}/n\mathbb{Z}$ sont cycliques d'ordre qui divise n. Réciproquement, pour tout diviseur d de n, il existe un unique sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ d'ordre d qui est $H = \langle \bar{q} \rangle$ où $q = \frac{n}{d}$.

Remarque 39 : On a donc ici la réciproque pour le théorème de Lagrange.

Théorème 40 : Soit G un groupe d'ordre p^2 avec p premier. Alors : $G \simeq \mathbb{Z}/p^2\mathbb{Z}$ ou $G \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ DEV 1

2) Théorème de structure [BER] [ROM]

Théorème 41 (chinois) : Soit $n_1, \dots, n_r \geq 1$ des entiers deux à deux premiers entre eux. Alors le morphisme des projections $\mathbb{Z} \to \mathbb{Z}/n_1\mathbb{Z} \times \dots \times \mathbb{Z}/n_r\mathbb{Z}$ est surjectif de noyau $(n_1 \times \dots \times n_r)$. En particulier, on a un isomorphisme d'anneaux : $\mathbb{Z}/n_1 \dots n_r\mathbb{Z} \simeq \mathbb{Z}/n_1\mathbb{Z} \times \dots \times \mathbb{Z}/n_r\mathbb{Z}$

Théorème 42 (de structure) [ADM1>] : Soit G un groupe abélien fini. Alors il existe des entiers $d_1, \dots, d_s \geq 2$ vérifiant $d_1 | d_2 | \dots | d_s$ tel que :

$$G \simeq \mathbb{Z}/d_1\mathbb{Z} \times \dots \times \mathbb{Z}/d_s\mathbb{Z}$$

De plus, la suite d'entiers $(d_1, \dots, d_s)$ est unique.

Remarque 43 : On obtient les groupes abéliens de petit ordre, voir l'annexe.

3) Le groupe des inversibles $(\mathbb{Z}/n\mathbb{Z})^\times$ [ROM]

Déf 44 : Pour $n \geq 2$, on note $(\mathbb{Z}/n\mathbb{Z})^\times$ le groupe multiplicatif

des éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$.

Théorème 45 : Soit $a \in \mathbb{Z}$. On a équivalence entre :
1) $\bar{a}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$
2) a est premier avec n
3) $\bar{a}$ est un générateur du groupe cyclique $(\mathbb{Z}/n\mathbb{Z}, +)$

Prop 46 : pour $n \geq 2$: $|(\mathbb{Z}/n\mathbb{Z})^\times| = \ell(n)$ où ℓ est l'indicatrice d'Euler

Théorème 47 : Tout sous-groupe fini du groupe multiplicatif d'un corps est cyclique.

Corollaire 48 : $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique et isomorphe à $\mathbb{Z}/(p-1)\mathbb{Z}$

III Un groupe fini non abélien : S_n [BER]

Soit $n \geq 2$. On note S_n le groupe symétrique sur $[\![1;n]\!]$. Il est de cardinal $n!$.

Théorème 49 : Tout permutation de S_n se décompose en produit de cycles à supports disjoints, et cette décomposition est unique à l'ordre des facteurs près.

Théorème 50 : L'ordre d'une permutation est le PPCM des longueurs des cycles à supports disjoints qui la composent.

Prop 51 : Le groupe S_n est engendré par chacune des familles suivantes :
1) Les cycles 2) Les transpositions 3) Les transpositions $(1\,i)$ pour $i \in [\![2;n]\!]$ 4) Les transpositions $(i\ i+1)$ pour $i \in [\![1;n-1]\!]$ 5) $(1\,2)$ et $(1\,2\,\dots\,n)$

Déf 52 : Il existe un unique morphisme de groupe $\varepsilon : S_n \to \mathbb{C}^\times$ non trivial. Si $\sigma \in S_n$ s'écrit comme produit de s transpositions, alors $\varepsilon(\sigma) = (-1)^s$. Ce morphisme s'appelle la signature.

Déf 53 : On appelle groupe alterné, noté A_n, l'ensemble des permutations de S_n de signature 1.

Prop 54 : A_n est distingué dans S_n et $|A_n| = \frac{n!}{2}$

Prop 55 : Pour $n \geq 3$, le groupe A_n est engendré par les 3-cycles.

Prop 56 : Si $n \geq 5$, les 3-cycles sont conjugués dans A_n

Théorème 57 : Soit $n \geq 3$. Alors A_n est simple ssi $n \neq 4$. DEV 2

Remarque 58 : A_4 n'est pas simple car $H = \{id, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}$ est distingué dans A_4

Prop 59 : Si $n \geq 3$, $Z(S_n) = \{id\}$

Corollaire 60 : Soit $n \geq 2$. Si $n \neq 4$, les seuls sous-groupes distingués de S_n sont : $\{id\}$, A_n, S_n.

Annexe

Classification des groupes abéliens de petit ordre : [BER]

BER
385

Ordre	Groupe abélien (à isomorphisme près)
1	$\{1\}$
2	$\mathbb{Z}/2\mathbb{Z}$
3	$\mathbb{Z}/3\mathbb{Z}$
4	$\mathbb{Z}/4\mathbb{Z}$ ou $(\mathbb{Z}/2\mathbb{Z})^2$
5	$\mathbb{Z}/5\mathbb{Z}$
6	$\mathbb{Z}/6\mathbb{Z} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$
7	$\mathbb{Z}/7\mathbb{Z}$
8	$\mathbb{Z}/8\mathbb{Z}$ ou $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ ou $(\mathbb{Z}/2\mathbb{Z})^3$
9	$\mathbb{Z}/9\mathbb{Z}$ ou $(\mathbb{Z}/3\mathbb{Z})^2$