Rapport du jury

> Cette leçon est particulièrement vaste et il convient de faire des choix, qui devront pouvoir être justifiés. La notion d'ordre (d'un groupe, d'un élément et d'un sous-groupe) est très importante dans cette leçon ; le théorème de Lagrange est incontournable. Le théorème de structure des groupes abéliens finis doit figurer dans cette leçon. Sa démonstration est techniquement exigeante, mais il faut que l'énoncé soit bien compris, en particulier le sens précis de la clause d'unicité, et être capable de l'appliquer dans des cas particuliers. Il est souhaitable de présenter des exemples de groupes finis particulièrement utiles comme les groupes Z/nZ et Sn, en en maîtrisant les propriétés élémentaires (générateurs, classes de conjugaison, etc.) Il est important de connaître les groupes d'ordre premier ainsi que les groupes d'ordre inférieur à 8. Des exemples de groupes finis issus de domaines autres que la théorie des groupes doivent figurer en bonne place dans cette leçon. L'étude des groupes d'isométries laissant fixe un polygone (ou un polyèdre) régulier peut être opportunément exploitée sous cet intitulé. Afin d'illustrer leur présentation, les candidates et candidats peuvent aussi s'intéresser à des groupes d'automorphismes ou étudier les groupes de symétries A4, S4, A5 et relier sur ces exemples géométrie et algèbre. Pour aller plus loin, les candidates et candidats peuvent s'attarder sur la dualité dans les groupes abéliens finis. Comme application, la cyclicité du groupe multiplicatif d'un corps fini est tout à fait adaptée. Il est possible d'explorer des représentations de groupes, de donner des exemples de caractères, additifs ou multiplicatifs dans le cadre des corps finis. Il est aussi possible de s'intéresser aux sommes de Gauss. Les candidates et candidats peuvent ensuite introduire la transformée de Fourier discrète, qui pourra être vue comme son analogue analytique, avec ses formules d'inversion, sa formule de Plancherel. Ainsi, la leçon peut mener à introduire la transformée de Fourier rapide sur un groupe abélien dont l'ordre est une puissance de 2 ainsi que des applications à la multiplication d'entiers, de polynômes et éventuellement au décodage de codes via la transformée de Hadamard.

Références

- Cours d'Algèbre - Daniel Perrin

- Mathématiques pour l'Agrégation (Algèbre) - J.E. Rombaldi
- P. Caldero - Carnet de voyage en Analystan
- P. Caldero - Carnet de voyage en Algébrie

Développements

- Probas sur GL2(Fq)
- Automorphismes de Sn

Méta-plan

1. Arithmétique dans les groupes finis
    1. Ordre d'un élément
    2. Combinatoire des groupes finis
2. Etude de certains groupes finis
    1. Groupes $\mathbb{Z}/n\mathbb{Z}$
    2. Groupe symétrique et groupe alterné
3. Final : p-groupes

Plan détaillé

I - Arithmétique dans les groupes finis

On fixe G un groupe fini de cardinal n.

1 - Ordre d'un élément [Perrin]

1. Définition : ordre comme $|\langle g \rangle|$.
2. Remarque : de façon équivalente, l'ordre de g est le plus petit entier non nul tel que $g^k = 1$.
3. Remarque : un groupe peut avoir tous ses éléments d'ordre fini sans être fini (($\mathbb{Z}/n\mathbb{Z})^{\mathbb{N}}$).
4. Exemples :
    1. Dans $\mathfrak{S}_k$, un produit de cycles à support disjoints $c_1 \circ \ldots \circ c_l$ a pour ordre le ppcm des longueurs de ces cycles.
    2. Si $L/\mathbb{F}_q$ est une extension finie de corps, le morphisme $x \mapsto x^q$ est d'ordre $[L : \mathbb{F}_q]$ dans $Aut(L/\mathbb{F}_q)$

5. Définition : quotient. Classe à gauche. Classe à droite. Indice
6. Proposition : $|G| = |H|[G : H]$.
7. Théorème : Lagrange
8. Application : tout groupe d'ordre premier est isomorphe à $\mathbb{Z}/p\mathbb{Z}$.
9. Application : soit q une puissance d'un nombre premier. On considère une extension de corps $K/\mathbb{F}_q$. Alors $\mathbb{F}_q$ est exactement l'ensemble des éléments de K qui sont racines de $X^q - X$.

2 - Combinatoire des groupes finis [Algébrie et Analystan]

> On suppose connues les généralités sur les actions de groupe

1. Proposition : on a une bijection $G/Stab_G(x) \cong Orb_G(x)$.
2. Théorème (équation aux classes) : $|X| = |G| \sum \frac{1}{|Stab_G(x)|}$
3. Application : le centre d'un groupe d'ordre p^α est non trivial.
4. Théorème (formule de Burnside) : $|Orb_G(X)| = \frac{1}{|G|} \sum_{g \in G} |Fix(g)|$.
5. Application : La probabilité que deux matrices tirées au hasard, indépendamment et avec probabilité uniforme, dans $GL_2(\mathbb{F}_q)$, commutent est $\frac{1}{(p^2-p)}$.(DVT 1)

II - Etude de certains groupes finis

1 - Groupes cycliques [Rombaldi]

1. Définition : groupe cyclique
2. Exemples :
    1. Le groupe additif de l'anneau Z/nZ
    2. l'ensemble des racines n-ièmes de l'unité.
3. Théorème : tous les sous-groupes cycliques d'ordre n sont isomorphes.
4. Corollaire : Si G est un groupe cyclique d'ordre n, pour tout $d \mid n$, G admet un unique sous-groupe d'ordre d. De plus, tout sous-groupe de G est cyclique.
5. Proposition : on a un isomorphisme de groupes

$$\begin{aligned} Aut(\mathbb{Z}/n\mathbb{Z}) &\to (\mathbb{Z}/n\mathbb{Z})^\times \\ \sigma &\mapsto \sigma(1) \end{aligned}$$

6. Lemme (chinois) : on a un isomorphisme de $\mathbb{Z}$-algèbres $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \cong /nm\mathbb{Z}$ ssi n et m sont premiers entre eux.

7. Application (nombres de Carmichael) : soit $n \geq 2$ un entier composé. Les assertions suivantes sont équivalentes :
    1. n met en défaut le test de primalité de Fermat, c'est-à-dire que pour tout a premier avec n, $a^{n-1} \equiv 1[n]$.
    2. pour tout facteur premier p de n, la valuation p-adique de n est 1 et $p-1 \mid n-1$.
8. Théorème : si G est un sous-groupe fini de $K^\times$, avec K un corps, G est cyclique.
9. Application : si $\mathbb{F}_q$ est un corps fini et L un extension finie de $\mathbb{F}_q$, il existe $\alpha \in L$ tel que $L = \mathbb{F}_q(\alpha)$.

2 - Groupe symétrique [Perrin]

1. Théorème (Cayley)
2. Théorème (décomposition en produit de cycles)
3. Théorème (générateurs de $\mathfrak{S}_n$) : $\mathfrak{S}_n$ est engendré par :
    1. les cycles
    2. les transpositions
    3. la transposition $(1\ 2)$ et le n-cycle $(1\ 2\ \dots\ n)$.
4. Exemple
5. Théorème : pour $n \geq 5$, $\mathfrak{A}_n$ est un groupe simple.
6. Corollaire : pour $n \geq 5$, les seuls sous-groupes distingués de $\mathfrak{S}_n$ sont $1, \mathfrak{S}_n$ et $\mathfrak{A}_n$.
7. Contre-exemple : dans $\mathfrak{S}_4$, le groupe composé des double-transpositions et de l'identité est distingué.
8. Définition : automorphisme intérieur
9. Théorème : les automorphismes de $\mathfrak{S}_n$ sont intérieurs, sauf peut-être pour $n = 6$ (DVT 2)

III - Final : p-groupes [Perrin + mémoire]

> Cette partie va utiliser tous les outils précédemment développés.

On fixe p un nombre premier

1. Définition : p-groupe
2. Proposition : soit G un p-groupe de cardinal p^α. Pour tout $\beta \leqslant \alpha$, G contient un sous-groupe d'ordre p^β. En particlier, G contient un élément d'ordre p.

3. Définition (p-Sylow)
4. Exemple important : l'ensemble des matrices triangulaires supérieures avec des 1 sur la diagonale. C'est un p-Sylow de $GL_n(\mathbb{F}_p)$.
5. Théorème (Sylow)
6. Application 1 : un groupe d'ordre truc muche n'est pas simple.
7. Application 2 : si $p < q$ sont deux nombres premiers, un groupe d'ordre pq est produit semi-direct de Z/pZ avec Z/qZ. Ce produit est direct si et seulement si ce groupe est abélien ssi il est cyclique. En particulier, un tel groupe n'est jamais simple.

Anciennes propositions [Diaz-Toca, Lombardi, Quitté]

> C'était intéressant mais ça empêche de parler des théorèmes de Sylow. En plus, c'est vraiment que des modules. Pour la deuxième, c'est juste trop dangereux, il faut être ultra au taquet sur la théorie des groupes.

III - Structure des groupes abéliens finis.

1 - Présentation d'un groupe abélien

1. Définition (partie libre, base d'une groupe abélien) : une partie finie $S \subset G$ est dite libre si l'application

$$\begin{aligned} \mathbb{Z}^{|S|} &\to G \\ (a_1, \dots a_{|S|}) &\mapsto \sum_{s \in S} a_s s \end{aligned}$$

   est injective. Une base est une partie génératrice libre.
2. Définition (groupe abélien libre)
3. Contre-exemple : $\mathbb{Z}/n\mathbb{Z}$ ne contient aucune famille libre non vide. En particulier, il n'est pas libre.
4. Remarque : un groupe libre de rang r est isomorphe à $\mathbb{Z}^r$.
5. Définition (matrice d'un morphisme de groupes libres)
6. Remarque : on retrouve les propriétés usuelles de composition des matrices connues dans les espaces vectoriels
7. Application : le rang d'un groupe libre non-nul est unique.

8. Définition (présentation de groupe abélien) : soit G un groupe abélien. Une présentation de G est un morphisme de groupes $\phi : \mathbb{Z}^p \to \mathbb{Z}^n$ telle que $G \cong \mathbb{Z}^n / Im(\phi)$.
9. Exemple : le groupe $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ admet pour présentation

$$\begin{aligned} \mathbb{Z}^2 &\to \mathbb{Z}^2 \\ (a, b) &\mapsto (2a, 3b) \end{aligned}$$

2 - Théorème de structure

1. Théorème (Smith)
2. Corollaire : un sous-groupe d'un groupe libre est libre de rang plus petit, et on a une base adaptée.
3. Corollaire : tout groupe abélien fini admet une présentation.
4. Théorème : structure des groupes abéliens finis
5. Exemple

III - Présentation d'un groupe abélien fini

1. Définition (présentation de groupe abélien) soit G un groupe abélien. Une présentation de G est un morphisme de groupes $\phi : \mathbb{Z}^p \to \mathbb{Z}^n$ telle que $G \cong \mathbb{Z}^n / Im(\phi)$.
2. Remarque : une présentation de G est un moyen de définir G par générateurs et relations. Si $\Phi : Z^p \to Z^n$ est une présentation de G, G est engendré par p générateurs satisfaisant des relations déterminées par Φ.
3. Exemple : le groupe $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ admet pour présentation

$$\begin{aligned} \mathbb{Z}^2 &\to \mathbb{Z}^2 \\ (a, b) &\mapsto (2a, 3b) \end{aligned}$$

4. Théorème : tout groupe abélien fini admet une présentation.
5. Corollaire (structure des groupes abéliens finis)
6. Remarque : ce théorème s'étend sans effort aux groupes abéliens de type fini.
7. Exemple : le groupe $\mathbb{Z}^2/\langle (4,0), (2,2) \rangle$ est isomorphe à $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.