Leçon 104 - Groupes finis. Exemples et applications.

Extrait du rapport de 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 $\mathbb{Z}/n\mathbb{Z}$ et $\mathfrak{S}_n$, 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 candidats peuvent aussi s'intéresser à des groupes d'automorphismes ou à des représentations de groupes, ou étudier les groupes de symétries $\mathfrak{A}_4$, $\mathfrak{S}_4$ et $\mathfrak{A}_5$ et relier sur ces exemples géométrie et algèbre.
Pour aller plus loin, les 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, des 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.

Présentation de la leçon

Je vais vous présenter la leçon 104 intitulée "Groupes finis. Exemples et applications". Les premières manifestations de groupes apparaissent dans les travaux de Lagrange sur la résolubilité d'équations polynomiales, et la notion est réellement identifiée et exploitée par Galois qui en développe largement la théorie sur le cas du groupe symétrique. La théorie des groupes se structure avec Jordan et von Dyck, avant de connaître un incroyable essor au XXème siècle avec par exemple les nombreux travaux aboutissant à la classification des groupes simples finis en 1982. Dans cette leçon, on s'intéressera à l'étude ainsi qu'à la construction de groupes de "petits cardinaux".
On s'intéresse dans une première partie aux généralités concernant les groupes finis avec tout d'abord les premières propriétés. Pour cela, on donne la définition d'un groupe ainsi que d'un élément d'ordre fini puis l'on énonce ensuite le théorème de Lagrange qui est un outil très utile notamment pour déterminer la structure de groupes finis de "petite taille". Cependant ce théorème n'admet pas toujours de réciproque et on s'efforcera à chercher des cas où la réciproque est vraie. On termine en donnant quelques résultats sur les ordres d'éléments. Dans un deuxième point, on étudie les groupes finis du point de vue des actions de groupes. Ces actions de groupes nous permettent d'aboutir par exemple au théorème de Cayley ainsi qu'à l'équation aux classes dont l'intérêt est justifié par un premier résultat sur la structure interne des p-groupes avec la proposition 11. Dans un dernier point, on s'intéresse aux théorèmes de Sylow avec l'étude des p-groupes. Le théorème de Sylow est fondamental car il permet de donner des informations sur un groupe à partir de son cardinal uniquement. La puissance de ce théorème s'explique par le fait qu'il permet par exemple de montrer qu'un groupe est simple ou cyclique mais également qu'il apporte une réciproque partielle au théorème de Lagrange pour les sous-groupes d'ordre premier !
Dans une deuxième partie, on s'intéresse à l'étude des groupes abéliens finis tout particulièrement. On parle tout d'abord des groupes cycliques (dont l'intérêt sera donné dans la sous-partie II.3) en commençant par donner la définition d'un groupe monogène et d'un groupe cyclique puis on commence à classifier ces groupes avec le théorème 24, le corollaire 25 et la proposition 26. On montre ensuite que la réciproque du théorème de Lagrange est vraie pour les groupes cycliques et que les groupes simples abéliens finis sont exactement les $\mathbb{Z}/p\mathbb{Z}$ avec p un nombre premier et on conclut cette sous-partie en donnant des générateurs du groupe cyclique $\mathbb{Z}/n\mathbb{Z}$ ainsi que le théorème 31. Dans un deuxième point, on s'attarde sur la notion d'exposant d'un groupe en commençant par donner la définition d'un groupe d'exposant fini ainsi qu'un premier résultat. On donne ensuite deux résultats dans le cas particulier des groupes abéliens. Dans un dernier point, on s'intéresse à la structure des groupes abéliens finis avec tout d'abord le théorème de structure des groupes abéliens finis qui justifie que l'on s'intéresse tant aux groupes cycliques $\mathbb{Z}/n\mathbb{Z}$ et qui possède énormément d'applications. En particulier, on tire de cette partie que tous les groupes abéliens finis vérifient la réciproque du théorème de Lagrange. De plus, le théorème de structure des groupes abéliens finis ainsi que l'étude des groupes cycliques $\mathbb{Z}/n\mathbb{Z}$ justifient que l'on connaît très bien n'importe quel

groupe abélien fini en termes de structure interne.
Enfin dans une dernière partie, on s'intéresse aux groupes finis non abéliens où les choses ne sont plus si simples malheureusement... Dans un premier point on s'intéresse au groupe symétrique dont l'intérêt de l'étude est appuyé par le théorème de Cayley. On commence par rappeler quelques générateurs avant d'en venir à la définition du groupe alterné. Le résultat fondamental du groupe alterné est le théorème 51 qui montre que les groupes alternés forment une deuxième famille de groupes finis simples après les $\mathbb{Z}/p\mathbb{Z}$. Ce résultat nous permet d'en déduire le centre de $\mathfrak{S}_n$ ainsi que ses sous-groupes distingués. Dans un deuxième point, on s'intéresse au groupe diédral en en donnant une présentation ainsi qu'une interprétation géométrique. On donne également son centre ainsi que son groupe dérivé en fonction de la parité de n. On termine enfin ce point en classifiant les groupes d'ordre $2p$. Dans un troisième point on s'intéresse au groupe des quaternions pour deux raisons : tout d'abord car il s'agit du premier groupe "spécial" à apparaître dans la classification des petits groupes (au sens où il est moins naturel que ses prédécesseurs) mais également car il possède la propriété remarquable d'avoir tous ses sous-groupes distingués sans être commutatif ! On termine enfin avec un dernier point qui traite du groupe linéaire. On énonce tout d'abord le théorème de Burnside qui donne une autre réciproque au lemme 33 avant de se placer dans le cas d'un corps fini où l'on dénombre les éléments de $\mathrm{GL}_n(\mathbb{F}_q)$ et $\mathrm{SL}_n(\mathbb{F}_q)$ ainsi que de leurs centres respectifs et leur groupes dérivés. On conclut ce point avec quelques isomorphismes exceptionnels puis le lemme de Fitting ainsi que la décomposition de Fitting qui permettent de dénombrer les endomorphismes nilpotents sur un corps fini.
On trouvera également en annexe la classification des groupes finis d'ordre inférieur ou égal à 15 à l'isomorphisme près (annexe 1) ainsi qu'une interprétation géométrique de D_{10} sur le pentagone régulier (annexe 2).

Plan général

Cours détaillé

Dans toute cette leçon, on considère un groupe $(G, *)$ (noté simplement G par la suite) et de neutre noté "e_G".

I Généralités

I.1 Premières propriétés

Dans toute cette sous-partie, on suppose que G est de cardinal fini noté n.

Définition 1 : Ordre d'un groupe et d'un élément [Berhuy, p.128 + 149] :
On considère $x \in G$.
$*$ On appelle **ordre du groupe** G le cardinal de G.
$*$ On appelle **ordre de** x le cardinal de $< x >$ et on le note $o(x)$.

Théorème 2 : Théorème de Lagrange [Berhuy, p.148] :
Soit H un sous-groupe de G.
On a $\text{Card}(G) = \text{Card}(G/H)\,\text{Card}(H)$.
En particulier, l'ordre de tout sous-groupe de G divise le cardinal de G et il en est de même pour l'ordre de tout élément de G.

Remarque 3 : [Berhuy, p.148]
La réciproque du théorème de Lagrange est fausse en général ($\mathfrak{A}_5$ est d'ordre 60 mais ne possède pas de sous-groupe d'ordre 30 par exemple (cf. III.1)).

Exemple 4 :
$*$ $\overline{2}$ est d'ordre 3 dans $\mathbb{Z}/3\mathbb{Z}$. $*$ (1 2 3) est d'ordre 3 dans $\mathfrak{S}_3$.
$*$ $< (\overline{1}, \overline{1}) >$ est d'ordre 2 dans $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Corollaire 5 : [Berhuy, p.151]
Soit $x \in G$.
$*$ On a $x^n = e_G$.
$*$ Pour tout $d \in \mathbb{N}^*$, l'élément x^d est d'ordre fini et on a $o\left(x^d\right) = \frac{o(x)}{\text{PGCD}(d, o(x))}$.
En particulier :
- Si d divise $o(x)$, alors $o\left(x^d\right) = \frac{o(x)}{d}$.
- Si d et $o(x)$ sont premiers entre eux, alors $o\left(x^d\right) = o(x)$.

I.2 Actions de groupes

Dans toute cette sous-partie, on considère E un ensemble quelconque non vide, on suppose que G agit sur E via une action de groupe notée "$\cdot$" et on note $\text{Stab}_G(x)$ et $\text{Orb}(x)$ respectivement le stabilisateur et l'orbite de $x \in E$ sous l'action de G.

Remarque 6 : [Berhuy, p.170]
La donnée d'une action de G sur E est équivalente à la donnée d'un morphisme de groupes de G dans $\mathfrak{S}_E$. En effet, G agit sur E via $\cdot$ si, et seulement si, l'application

$$\Psi : \left| \begin{array}{ccc} G & \longrightarrow & \mathfrak{S}_E \\ g & \longmapsto & \sigma_g : \left| \begin{array}{ccc} E & \longrightarrow & E \\ x & \longmapsto & g \cdot x \end{array} \right. \end{array} \right.$$

est un morphisme de groupes.

Théorème 7 : Théorème de Cayley [Berhuy, p.177] :
Si G est d'ordre n, alors G est isomorphe à un sous-groupe de $\mathfrak{S}_n$.

Lemme 8 : Équation aux classes [Berhuy, p.173] :
Si E est un ensemble fini et que Ω est un système de représentants de E, on a alors $\text{Card}(E) = \sum_{\omega \in \Omega} \text{Card}(\text{Orb}(\omega))$.

Proposition 9 : [Berhuy, p.174]
Pour tout $x \in E$, l'application suivante est une bijection :

$$f_x : \left| \begin{array}{ccc} G/\text{Stab}_G(x) & \longrightarrow & \text{Orb}(x) \\ \overline{g} & \longmapsto & g \cdot x \end{array} \right.$$

En particulier, si G est fini, alors pour tout $x \in E$, l'ensemble $\text{Orb}(x)$ est fini, son cardinal divise l'ordre de G et $\text{Card}(\text{Orb}(x)) = \frac{\text{Card}(G)}{\text{Card}(\text{Stab}_G(x))}$.

Définition 10 : p-groupe [Berhuy, p.180] :
On considère p un nombre premier.
On appelle **p-groupe** tout groupe fini d'ordre une puissance de p.

Proposition 11 : [Berhuy, p.181]
Si G est un p-groupe non trivial, alors $Z(G)$ est non trivial.

Proposition 12 : Formule de Burnside [Berhuy, p.176] :
Si G et E sont finis, que l'on note $\text{Fix}(g) = \{x \in E \text{ tq } g \cdot x = x\}$ et Ω l'ensemble des orbites de E sous l'action de G, alors on a l'égalité :

$$\text{Card}(\Omega) = \frac{1}{\text{Card}(G)} \sum_{g \in G} \text{Card}(\text{Fix}(g))$$

Corollaire 13 : [Caldero, p.305]
Si G est un groupe non abélien d'ordre n possédant k classes de conjugaison, alors la probabilité p que deux éléments commutent est égale à $\frac{k}{n}$.

I.3 Les théorèmes de Sylow

Dans toute cette sous-partie, on suppose que G est de cardinal fini noté n et p un nombre premier.

Définition 14 : p-sous-groupe de G [Berhuy, p.311] :
On appelle **p-sous-groupe de** G tout sous-groupe de G de cardinal une puissance de p.

Désormais, on écrit $\text{Card}(G) = n = p^m q$ où $p \nmid q$ et $m \in \mathbb{N}^*$.

Définition 15 : p-sous-groupe de Sylow de G [Berhuy, p.311] :
On appelle **p-sous-groupe de Sylow de** G (ou plus simplement p-Sylow) tout sous-groupe de G d'ordre p^m.

Exemple 16 :
$*$ $\mathbb{Z}/6\mathbb{Z}$ contient un 2-Sylow et un 3-Sylow (respectivement $\mathbb{Z}/2\mathbb{Z}$ et $\mathbb{Z}/3\mathbb{Z}$).
$*$ $\mathbb{Z}/56\mathbb{Z}$ contient un 2-Sylow et un 7-Sylow (respectivement $\mathbb{Z}/8\mathbb{Z}$ et $\mathbb{Z}/7\mathbb{Z}$).

Théorème 17 : Théorème de Sylow [Berhuy, p.313] :
$*$ Il existe des p-sous-groupes de Sylow de G et tout p-sous-groupe de G est contenu dans un p-Sylow.
$*$ Le conjugué d'un p-Sylow est un p-Sylow et tous les p-Sylow de G sont conjugués entre eux. En particulier, si S est un p-Sylow de G, alors S est distingué dans G si, et seulement si, S est l'unique p-Sylow de G.
$*$ Si n_p désigne le nombre de p-Sylow de G, alors $n_p \equiv 1\ [p]$ et $n_p | q$.

Exemple 18 : [Berhuy, p.315 + 328]
Tout groupe d'ordre 63 ou 255 n'est pas simple.

Corollaire 19 :
Tout groupe d'ordre pq avec $p < q$ qui sont deux nombres premiers n'est pas simple.

Corollaire 20 : [Berhuy, p.315]
Tout groupe d'ordre 33 cyclique.

Théorème 21 : Théorème de Cauchy [Berhuy, p.179] :
G possède au moins un élément d'ordre p.

II Les groupes abéliens finis

II.1 Les groupes cycliques

Définition 22 : Groupe monogène/cyclique [Berhuy, p.154] :
On dit que le groupe G est :
$*$ **monogène** lorsqu'il est engendré par un unique élément.
$*$ **cyclique** lorsqu'il est monogène et fini.

Exemple 23 : [Berhuy, p.154]
$*$ Le groupe $\mathbb{Z}$ est monogène mais non cyclique.
$*$ Pour tout entier naturel $n \geq 1$, le groupe $\mathbb{Z}/n\mathbb{Z}$ est cyclique d'ordre n.

Théorème 24 : [Berhuy, p.154]
$*$ Tout groupe monogène infini est isomorphe à $\mathbb{Z}$.
$*$ Tout groupe cyclique d'ordre n est isomorphe à $\mathbb{Z}/n\mathbb{Z}$. En particulier, deux groupes cycliques sont isomorphes si, et seulement si, ils ont le même ordre.

Corollaire 25 : [Berhuy, p.155]
Soit p un nombre premier.
Si G est d'ordre p, alors G est cyclique et $G \cong \mathbb{Z}/p\mathbb{Z}$.

Développement 1 : (A) [cf. BERHUY]

Proposition 26 : [Berhuy, p.194]
Soit p un nombre premier.
Si G est d'ordre p^2, alors $G \cong \mathbb{Z}/p^2\mathbb{Z}$ ou $G \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

Théorème 27 : [Berhuy, p.155]
Si G est un groupe cyclique d'ordre n, alors pour tout diviseur positif d de n, il existe un unique sous-groupe H_d d'ordre d de G et ce sous-groupe est cyclique.
De plus, si x_0 est un générateur de G, on a alors les égalités :

$$H_d = \left\langle x_0^{\frac{n}{d}} \right\rangle = \left\{ x \in G \text{ tq } x^d = e_G \right\}$$

Remarque 28 :
On a ici un cas où la réciproque du théorème de Lagrange est vraie !

Théorème 29 : [Berhuy, p.161]
Les groupes abéliens simples sont exactement les $\mathbb{Z}/p\mathbb{Z}$ avec p un nombre premier.

Proposition 30 : [Rombaldi, p.283]
Soient a un entier relatif et n un entier naturel non nul.
$\overline{a}$ est un générateur du groupe cyclique $\mathbb{Z}/n\mathbb{Z}$ si, et seulement si, l'entier relatif a est premier avec n (ou encore si, et seulement si, $\overline{a}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$).

Théorème 31 : [Rombaldi, p.292]
Si p est un nombre premier impair et r un entier naturel non nul, alors le groupe $(\mathbb{Z}/p^r\mathbb{Z})^\times$ est cyclique.

II.2 Exposant d'un groupe

Définition 32 : Groupe d'exposant fini [Berhuy, p.344] :
On dit que G est **d'exposant fini** lorsqu'il existe un entier $n \in \mathbb{N}^*$ tel que pour tout $x \in G,\ x^n = e_G$.
Dans ce cas, on appelle **exposant de** G le plus petit entier $n \in \mathbb{N}^*$ vérifiant cette propriété et on le note $\exp(G)$.

Lemme 33 : [Berhuy, p.344]
Si G est un groupe d'exposant fini, alors $\exp(G) = \text{PPCM}(\{o(x),\ x \in G\})$.
De plus, si G est fini, on a $\exp(G)$ qui divise $\text{Card}(G)$.

Exemple 34 : [Berhuy, p.345]
$*$ Si G est cyclique d'ordre n, alors $\exp(G) = n$.
$*$ On a $\exp(D_4) = 4$ et $\exp(\mathfrak{S}_3) = 6$.

Proposition 35 : [Berhuy, p.345]
Si G est un groupe abélien d'exposant fini, alors il existe un élément $x \in G$ d'ordre $\exp(G)$.

Corollaire 36 : [Berhuy, p.345]
Si G est un groupe abélien fini, alors on a l'équivalence :

$$(\exp(G) = \text{Card}(G)) \iff (G \text{ cyclique})$$

Remarque 37 : [Berhuy, p.346]
L'ensemble $\mathfrak{S}_3$ montre que les deux résultats précédents sont faux si G n'est pas supposé abélien.

Théorème 38 : [Berhuy, p.346]
Soit $\mathbb{K}$ un corps commutatif quelconque.
Tout sous-groupe fini de $\mathbb{K}^\times$ est cyclique.

Remarque 39 : [Berhuy, p.346]
$*$ En particulier, on en déduit que tout sous-groupe de $\mathbb{F}_q^\times$ est cyclique (avec $q = p^n$ où p est un nombre premier et n un entier naturel non nul).
$*$ Si p est un nombre premier, on a alors que $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique et on retrouve le résultat du théorème 30 dans le cas où $r = 1$.

II.3 Structure des groupes abéliens finis

Dans toute cette sous-partie, on suppose que G est d'ordre fini et abélien.

Théorème 40 : Théorème de structure [ADMIS] [Berhuy, p.358] :
Il existe des entiers $d_1, ..., d_s \geq 2$ vérifiant $d_1|d_2|...|d_s$ et tels que $G \cong \prod_{i=1}^s \mathbb{Z}/d_i\mathbb{Z}$.
De plus, la suite d'entiers $(d_1, ..., d_s)$ est unique, et ne dépend que de la classe d'isomorphisme de G.

Définition 41 : Facteurs invariants [Berhuy, p.361] :
Les entiers $d_1, ..., d_s$ fournis par le théorème précédent sont appelés les **facteurs invariants de** G.

Corollaire 42 : [Berhuy, p.362]
Deux groupes abéliens finis sont isomorphes si, et seulement si, ils ont les mêmes facteurs invariants.

Exemple 43 : [Berhuy, p.363]
$*$ Si $G = \mathbb{Z}/4\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})^2 \times \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$, alors $G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/180\mathbb{Z}$.
$*$ Il y a exactement 3 groupes abéliens d'ordre 120 (à l'isomorphisme près).

Corollaire 44 :
Pour tout diviseur d de l'ordre de G, il existe un sous-groupe de G d'ordre d.

Théorème 45 : [ADMIS] [Berhuy, p.364]
Si G est un groupe abélien de type fini, alors il existe des entiers naturels r, s et des entiers $d_1, ..., d_s \geq 2$ vérifiant $d_1|d_2|...|d_s$ tels que $G \cong \mathbb{Z}^r \times \prod_{i=1}^s \mathbb{Z}/d_i\mathbb{Z}$.
De plus, l'entier r et la suite d'entiers $(d_1, ..., d_s)$ sont uniques.

III Exemples de groupes finis non abéliens

III.1 Le groupe symétrique

Dans toute cette sous-partie, on considère un entier naturel $n \geq 2$. On notera $\mathfrak{S}_n$ le groupe symétrique sur $[\![1;n]\!]$ (de cardinal $n!$).

Théorème 46 : [Berhuy, p.204]
Toute permutation de $\mathfrak{S}_n$ se décompose en produit de cycles à supports disjoints et cette décomposition est unique à l'ordre des facteurs près.

Théorème 47 : [Berhuy, p.208]
L'ordre d'une permutation est le PPCM des longueurs des cycles à supports disjoints qui la composent.

Proposition 48 : [Berhuy, p.212 + 213]
Le groupe $\mathfrak{S}_n$ est engendré par chacune des familles suivantes :
$*$ Les cycles. $*$ Les transpositions. $*$ Les transpositions $(1\ i)$ pour $i \in [\![2;n]\!]$.
$*$ Les transpositions $(i\ i+1)$ pour $i \in [\![1;n-1]\!]$. $*$ $(1\ 2)$ et $(1\ 2\ \ldots\ n)$.

Définition 49 : Signature [Berhuy, p.213] :
Il existe un unique morphisme de groupes $\varepsilon : \mathfrak{S}_n \longrightarrow \mathbb{C}^\times$ non trivial appelé **signature** tel que pour toute transposition σ, $\varepsilon(\sigma) = -1$ et pour toute permutation ρ qui s'écrit comme produit de s transpositions, on a $\varepsilon(\rho) = (-1)^s$.

On note $\mathfrak{A}_n$ le noyau de ε, aussi appelé groupe alterné sur $[\![1;n]\!]$ (de cardinal $\frac{n!}{2}$).

Remarque 50 : [Berhuy, p.301 + 302]
On a $\mathfrak{S}_n = \mathfrak{A}_n \rtimes \mathbb{Z}/2\mathbb{Z}$.
Autrement dit, on a la suite exacte scindée :

$$\{\mathrm{Id}_{[\![1;n]\!]}\} \longrightarrow \mathfrak{A}_n \xrightarrow{\iota} \mathfrak{S}_n \underset{s}{\overset{\varepsilon}{\rightleftarrows}} \mathbb{Z}/2\mathbb{Z} \longrightarrow \{\mathrm{Id}_{[\![1;n]\!]}\}$$

Développement 2 : [cf. ROMBALDI]

Théorème 51 : [Rombaldi, p.50] :
Pour $n = 3$ ou $n \geq 5$, le groupe $\mathfrak{A}_n$ est simple.

Remarque 52 : [Berhuy, p.219 + Perrin, p.28 + 37]
$*$ En réalité, $\mathfrak{A}_5$ est le plus petit groupe simple non abélien (et tout groupe simple d'ordre 60 est isomorphe à $\mathfrak{A}_5$).
$*$ Ce résultat est cohérent avec le théorème de Feit-Thompson (tout groupe simple fini et non abélien est d'ordre pair).
$*$ Ce résultat a une importance historique majeure car il permet de montrer que pour $n \geq 5$, $\mathfrak{A}_n$ n'est pas résoluble et donc que les solutions des équations polynomiales de degré supérieur ou égal à 5 ne peuvent s'écrire à l'aide des quatre opérations élémentaires et de la racine carré.

Remarque 53 : [Perrin, p.30]
$*$ Si $n = 4$, alors $\mathfrak{A}_n$ n'est pas simple car contient comme sous-groupe distingué $H = \{\mathrm{Id}_{[\![1;4]\!]}, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$.
$*$ De plus, $\mathfrak{A}_4$ est le plus petit groupe (à l'isomorphisme près) qui ne vérifie pas la réciproque du théorème de Lagrange.

Proposition 54 : [Berhuy, p.219]
Si $n \geq 3$, alors le centre de $\mathfrak{S}_n$ est trivial.

Corollaire 55 : [Berhuy, p.220 + Delcourt p.139]
$*$ Si $n \geq 5$, les sous-groupes distingués de $\mathfrak{S}_n$ sont exactement $\mathrm{Id}_{[\![1;n]\!]}, \mathfrak{A}_n$ et $\mathfrak{S}_n$ et on a $D(\mathfrak{A}_n) = \mathfrak{A}_n$.
$*$ De plus, on a $D(\mathfrak{S}_n) = \mathfrak{A}_n$.

Remarque 56 : [Berhuy, p.220]
Si $n = 4$, alors il faut rajouter à la liste précédente le sous-groupe H de $\mathfrak{S}_4$ (cf. remarque 53).

Théorème 57 : [Combes, p.175]
On a $\mathrm{Isom}^+(\mathcal{C}) \cong \mathfrak{S}_4$ et $\mathrm{Isom}(\mathcal{C}) \cong \mathfrak{S}_4 \times \mathbb{Z}/2\mathbb{Z}$.

III.2 Le groupe diédral

Définition 58 : Groupe diédral [Berhuy, p.274] :
On appelle **groupe diédral d'ordre** $2n$ le groupe :

$$D_{2n} \cong \langle a, b \mid a^n = 1,\ b^2 = 1,\ bab^{-1} = a^{-1} \rangle$$

Proposition 59 : [Delcourt, p.98]
Le groupe diédral d'ordre $2n$ est un groupe non abélien de cardinal $2n$.

Remarque 60 : [Perrin, p.23]
Le groupe diédral d'ordre $2n$ possède une interprétation géométrique : il s'agit du groupe des isométries du plan euclidien conservant un polygone régulier à n côtés. Il est engendré par la rotation τ de mesure d'angle $\frac{2\pi}{n}$ et la symétrie orthogonale σ par rapport à l'axe (Ox) (cf. annexe 2).

Remarque 61 : [Perrin, p.23]
Le sous-groupe des rotations est distingué et isomorphe à $\mathbb{Z}/n\mathbb{Z}$. De plus, comme $\text{Card}(D_{2n}) = 2n$, on a donc une suite exacte :

$$\{\text{Id}\} \longrightarrow \mathbb{Z}/n\mathbb{Z} \longrightarrow D_{2n} \xrightarrow{p} \mathbb{Z}/2\mathbb{Z} \longrightarrow \{\text{Id}\}$$

et un isomorphisme $D_{2n} \cong \mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$ car n'importe quelle réflexion fournit une section de p.

Proposition 62 : [Delcourt, p.139]
* Si n est impair, alors centre de D_{2n} est réduit au sous-groupe trivial.
* Si n est pair, alors le centre de D_{2n} est égal à $\left\{\text{Id}, \tau^{\frac{n}{2}}\right\}$.

Proposition 63 : [Delcourt, p.136]
* Si n est impair, alors le groupe dérivé de D_{2n} est égal à $<\tau> \cong \mathbb{Z}/n\mathbb{Z}$.
* Si $n = 2m$ est pair, alors le groupe dérivé de D_{2n} est égal à $\langle\tau^2\rangle \cong \mathbb{Z}/m\mathbb{Z}$.

Développement 3 : (B) [cf. BERHUY]

Proposition 64 : [Berhuy, p. 310]
Soit p un nombre premier supérieur ou égal à 3.
Si G est d'ordre $2p$, alors G est isomorphe à $\mathbb{Z}/2p\mathbb{Z}$ ou à D_{2p}.

III.3 Le groupe des quaternions

Définition 65 : Groupe des quaternions [Delcourt, p.40] :
On appelle **groupe des quaternions** le groupe :

$$\mathbb{H}_8 \cong \langle a, b \mid a^4 = 1,\ b^4 = 1,\ ba = a^3b\rangle$$

Proposition 66 : [Delcourt, p.43 + 136]
Le groupe $\mathbb{H}_8$ (non commutatif !) possède 6 sous-groupes stricts et chacun est commutatif et distingué dans $\mathbb{H}_8$.
En particulier, $Z(\mathbb{H}_8) = \{-1; 1\}$ et $D(\mathbb{H}_8) = \{-1; 1\}$.

III.4 Autour du groupe linéaire

Dans toute cette sous-partie, on considère un corps $\mathbb{K}$ commutatif fini à $q = p^r$ éléments (avec p un nombre premier et $r \in \mathbb{N}^*$) et E un $\mathbb{K}$-espace vectoriel de dimension finie $n \geq 1$. On utilisera l'identification de $\text{GL}(E)$ avec $\text{GL}_n(\mathbb{K})$.

Théorème 67 : Théorème de Burnside [Francinou, p.353] :
Soit H un sous-groupe de $\text{GL}_n(\mathbb{C})$.
Si H est d'exposant fini, alors il est fini.

Proposition 68 : [Rombaldi, p.156]

$$\text{Card}(\text{GL}_n(\mathbb{F}_q)) = \prod_{k=0}^{n-1}\left(q^n - q^k\right) \text{ et } \text{Card}(\text{SL}_n(\mathbb{F}_q)) = \frac{1}{q-1}\prod_{k=0}^{n-1}\left(q^n - q^k\right)$$

Proposition 69 : [Perrin, p.105]
Le centre de $\text{GL}_n(\mathbb{F}_q)$ est de cardinal égal à $q-1$ et celui de $\text{SL}_n(\mathbb{F}_q)$ est de cardinal égal à $\text{PGCD}(n, q-1)$.

Théorème 70 : [Rombaldi, p.154]
Pour $n \geq 2$, on a :
* $D(\text{SL}_n(\mathbb{K})) \subseteq D(\text{GL}_n(\mathbb{K})) \subseteq \text{SL}_n(\mathbb{K})$.
* Pour $n \geq 3$, $D(\text{SL}_n(\mathbb{K})) = D(\text{GL}_n(\mathbb{K})) = \text{SL}_n(\mathbb{K})$.
* Pour $n = 2$, $\mathbb{K} \neq \mathbb{F}_2$ et $\mathbb{K} \neq \mathbb{F}_3$, $D(\text{SL}_n(\mathbb{K})) = D(\text{GL}_n(\mathbb{K})) = \text{SL}_n(\mathbb{K})$.

Remarque 71 : [Rombaldi, p.155]
* Pour $\mathbb{K} = \mathbb{F}_2$, on a $\text{GL}_n(\mathbb{K}) = \text{SL}_n(\mathbb{K})$.
* Pour $n = 2$ et $\mathbb{K} = \mathbb{F}_2$, on a $D(\text{SL}_n(\mathbb{K})) \cong \mathfrak{A}_3$.
* Pour $n = 2$ et $\mathbb{K} = \mathbb{F}_3$, on a $D(\text{SL}_n(\mathbb{K})) \cong \mathbb{H}_8$.

Proposition 72 : [Rombaldi, p.158]
Si G est un groupe fini de cardinal $n \in \mathbb{N}^*$, alors pour tout nombre premier p, G est isomorphe à un sous-groupe de $\text{GL}_n(\mathbb{F}_p)$.

Proposition 73 : [Perrin, p.106]
On a $\text{GL}_2(\mathbb{F}_2) = \text{SL}_2(\mathbb{F}_2) = \text{PSL}_2(\mathbb{F}_2) \cong \mathfrak{S}_3$.

Théorème 74 : [Perrin, p.106]
On a les isomorphismes suivants :
* $\text{PGL}_2(\mathbb{F}_3) \cong \mathfrak{S}_4$ et $\text{PSL}_2(\mathbb{F}_3) \cong \mathfrak{A}_4$.
* $\text{PGL}_2(\mathbb{F}_4) = \text{PSL}_2(\mathbb{F}_4) \cong \mathfrak{A}_5$.
* $\text{PGL}_2(\mathbb{F}_5) \cong \mathfrak{S}_5$ et $\text{PSL}_2(\mathbb{F}_5) \cong \mathfrak{A}_5$.

Dans toute la suite de cette sous-partie, on considère u un endomorphisme de E mais le corps $\mathbb{K}$ de base n'est plus supposé fini.

Lemme 75 : [Caldero, p.74]
Les suites $\left(\mathrm{Ker}\left(u^k\right)\right)_{k\in\mathbb{N}}$ et $\left(\mathrm{Im}\left(u^k\right)\right)_{k\in\mathbb{N}}$ sont respectivement croissante et décroissante au sens de l'inclusion.
De plus, ces deux suites sont stationnaires à partir d'un certain rang $n_0 \in \mathbb{N}$.

Lemme 76 : Lemme de Fitting [Caldero, p.74] :
Avec les notations du lemme précédent, on a $E = \mathrm{Ker}\left(u^{n_0}\right) \oplus \mathrm{Im}\left(u^{n_0}\right)$.
De plus, u induit un endomorphisme nilpotent sur $\mathrm{Ker}\left(u^{n_0}\right)$ et un automorphisme sur $\mathrm{Im}\left(u^{n_0}\right)$.

Définition 77 : Décomposition de Fitting [Caldero, p.74] :
La donnée de $((F,G),v,w)$ où $F = \mathrm{Ker}\left(u^{n_0}\right)$, $G = \mathrm{Im}\left(u^{n_0}\right)$, $v = u|_F$ et $w = u|_G$ avec $E = F \oplus G$, v nilpotent et w un automorphisme est appelée **décomposition de Fitting**.

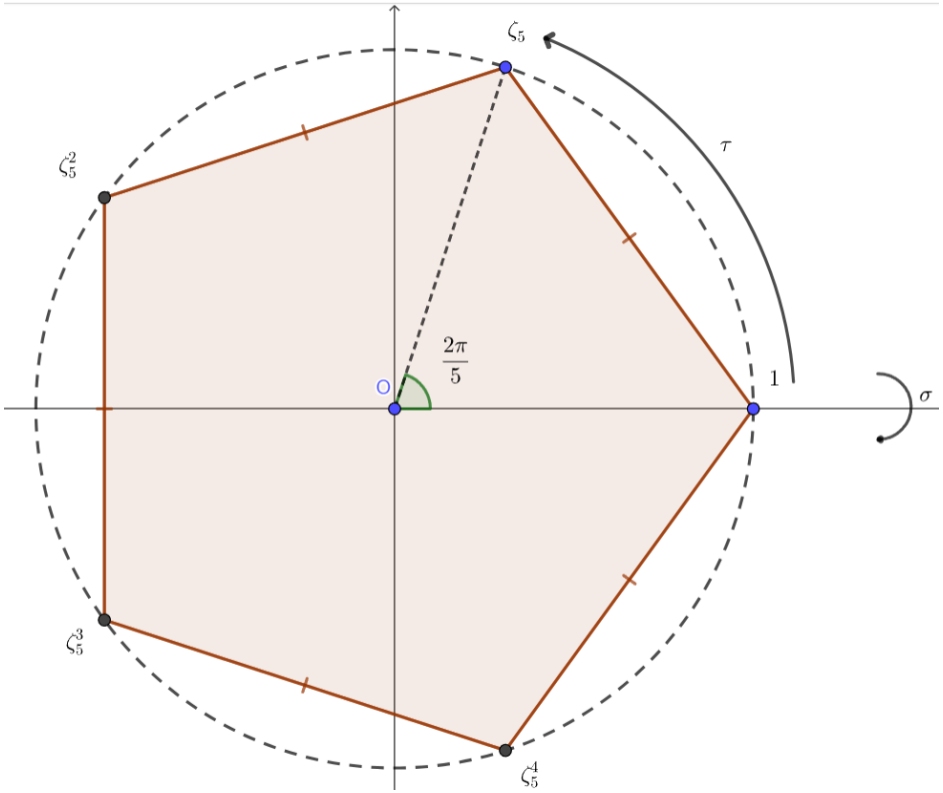
Théorème 78 : [Caldero, p.74]
Si $\mathbb{K}$ est un corps fini commutatif de cardinal q, alors il y a $n_d = q^{d(d-1)}$ matrices nilpotentes de taille $d \times d$ à coefficients dans $\mathbb{K}$.

IV Annexe

IV.1 Liste des groupes finis de cardinal inférieur ou égal à 15 (à isomorphisme près)

Ordre du groupe	Groupes abéliens	Groupes non abéliens
1	$\{e_G\}$	$\emptyset$
2	$\mathbb{Z}/2\mathbb{Z} \cong \mathfrak{S}_2 \cong D_2$	$\emptyset$
3	$\mathbb{Z}/3\mathbb{Z} \cong \mathfrak{A}_3$	$\emptyset$
4	$\mathbb{Z}/4\mathbb{Z}$ ou $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \cong D_4$	$\emptyset$
5	$\mathbb{Z}/5\mathbb{Z}$	$\emptyset$
6	$\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$	$\mathfrak{S}_3 \cong D_6$
7	$\mathbb{Z}/7\mathbb{Z}$	$\emptyset$
8	$\mathbb{Z}/8\mathbb{Z}$ ou $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ ou $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	D_8 ou $\mathbb{H}_8$
9	$\mathbb{Z}/9\mathbb{Z}$ ou $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$	$\emptyset$
10	$\mathbb{Z}/10\mathbb{Z} \cong \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	D_{10}
11	$\mathbb{Z}/11\mathbb{Z}$	$\emptyset$
12	$\mathbb{Z}/12\mathbb{Z} \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ ou $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	$D_{12} \cong D_6 \times \mathbb{Z}/2\mathbb{Z}$ ou $\mathfrak{A}_4$ ou $\mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$
13	$\mathbb{Z}/13\mathbb{Z}$	$\emptyset$
14	$\mathbb{Z}/14\mathbb{Z} \cong \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	D_{14}
15	$\mathbb{Z}/15\mathbb{Z} \cong \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$	$\emptyset$

IV.2 Illustration géométrique de D_{10}



Remarques sur la leçon

— Il est également possible de parler de représentations même si cela n'est plus au programme explicitement (surtout pour le théorème de structure des groupes abéliens de type fini).

— On peut parler des produits directs et semi-directs internes et externes ainsi que donner des caractérisations et faire le lien avec les suites exactes.

Liste des développements possibles

— Classification des groupes d'ordre p^2 et $2p$.

— Exposant d'un groupe.

— Simplicité de $\mathfrak{A}_n$ pour $n = 3$ ou $n \geq 5$.

— Groupe des isométries du cube.

— Théorème de Burnside.

— Dénombrement des endomorphismes nilpotents sur un corps fini.

Bibliographie

— Grégory Berhuy, *Algèbre : le grand combat*.

— Philippe Caldero, *Carnet de voyage en Analystan*.

— Jean-Étienne Rombaldi, *Mathématiques pour l'agrégation, Algèbre et Géométrie*.

— Daniel Perrin, *Cours d'algèbre*.

— Jean Delcourt, *Théorie des groupes*.

— François Combes, *Algèbre et géométrie*.

— Serge Francinou, *Exercices de mathématiques, Oraux X-ENS, Algèbre 2*.

— Philippe Caldero, *Carnet de voyage en Algébrie*.