Leçon 104 : Groupes finis. Exemples et applications

Références : Berhuy, Rombaldi, Perrin, Delcourt (théorie des groupes)
CAL CVAL (pour le dev.)

DEV 1 : Simplicité de $\mathfrak{A}_n$ pour $n=3$ et $n \geq 5$

DEV 2 : Lemme de Fitting et cône nilpotent

Leçon 104 : Groupes finis. Exemples et applications

Dans cette leçon, on considère $(G,*)$ un groupe (noté G) et de neutre e_G.

I - Généralités

1) Ordre d'un élément [BERH]

DEF 1 : Si G est un groupe fini, son cardinal noté $\#G$ s'appelle l'ordre de G. Étant donné $x \in G$, on note $o(x)$ et on appelle ordre de x le cardinal de $\langle x \rangle$.

THM 2 : (Lagrange) On suppose G fini. Soit H un sous-groupe de G. Alors $\#G = [G:H]\#H$ où $[G:H] = \#G/H$ l'indice de H dans G. En particulier, $\#H \mid \#G$ et l'ordre de tout élément divise le cardinal de G.

REM 3 : La réciproque de ce théorème est fausse en général. Par exemple, $\mathfrak{A}_4$ n'a pas de sous-groupe d'ordre 6.

EX 4 : $\bar{2}$ est d'ordre 3 dans $\mathbb{Z}/3\mathbb{Z}$, $(1\,2\,3)$ est d'ordre 3 dans $\mathfrak{S}_3$ et $\langle(\bar{1},\bar{1})\rangle$ est d'ordre 2 dans $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

COR 5 : Si G est fini d'ordre $n \geq 1$, alors pour tout $x \in G$, $x^n = e_G$.

COR 6 : Soit $x \in G$ d'ordre fini. Alors, pour tout $d \geq 1$, x^d est d'ordre fini et $o(x^d) = \dfrac{o(x)}{d \wedge o(x)}$

2) Actions de groupes [BERH]

Soit E un ensemble non vide. On suppose que G agit sur E par une action notée $\cdot$ et on note $Stab(x)$ et $Orb(x)$ respectivement le stabilisateur et l'orbite d'un élément $x \in G$.

REM 7 : La donnée de l'action $\cdot$ est équivalente à la donnée d'un morphisme de groupes de G dans $\mathfrak{S}_E$

THM 8 (Cayley) : Si G est fini d'ordre n, alors G est isomorphe à un sous-groupe de $\mathfrak{S}_n$.

PROP 9 : Pour tout $x \in E$, l'application $f : G \to Orb(x)$, $g \mapsto g \cdot x$ induit une bijection $\bar{f} : G/Stab(x) \to Orb(x)$, $g\,Stab(x) \mapsto g \cdot x$

PROP 10 (Équation aux classes) : Si G est fini et E est fini, on a $\#E = \sum_{x \in S} \#Orb(x) = \sum_{x \in S} \dfrac{\#G}{\#Stab(x)}$ où S est un système de représentants des orbites.

DEF 11 : Soit p un nombre premier. Un p-groupe est un groupe fini d'ordre une puissance de p.

PROP 12 : Si G est un p-groupe, et E est fini, alors on a $\#E \equiv \#E^G \mod p$ où $E^G = \{g \in G \mid \forall x \in E, g \cdot x = x\}$.

COR 13 : Si G est un p-groupe, alors son centre $Z(G)$ est non réduit à $\{e_G\}$.

PROP 14 : (Formule de Burnside) : On suppose G et E finis. Soit Ω l'ensemble des orbites de E sous l'action de G. Alors :

$$\#\Omega = \frac{1}{\#G} \sum_{g \in G} \#Fix(g).$$

3) Les théorèmes de Sylow [BERH]

On suppose G fini d'ordre n et que p est un nombre premier.

DEF 15 : Écrivons $\#G = p^m q$ avec $p \nmid q$ et $m \geq 0$. On appelle p-sous-groupe de Sylow de G ou p-Sylow tout sous-groupe de G d'ordre p^m.

EX 16 : $\mathbb{Z}/6\mathbb{Z}$ contient un 2-Sylow et un 3-Sylow ($\mathbb{Z}/2\mathbb{Z}$ et $\mathbb{Z}/3\mathbb{Z}$)
$\mathbb{Z}/56\mathbb{Z}$ contient un 2-Sylow et un 7-Sylow ($\mathbb{Z}/2\mathbb{Z}$ et $\mathbb{Z}/7\mathbb{Z}$)

REM 17 : Tout conjugué d'un p-Sylow de G est encore un p-Sylow.

THM 18 : (Sylow)
- Il existe des p-Sylow de G et tout p-sous-groupe de G est contenu dans un p-Sylow.
- Le conjugué d'un p-Sylow de G est encore un p-Sylow de G, et tous les p-Sylow de G sont conjugués. 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 est le nombre de p-Sylow de G, on a $n_p \equiv 1 \mod p$ et $n_p \mid q$.

EX 19 : Un groupe d'ordre 63 n'est pas simple.

EX 20 : Un groupe d'ordre 33 est engendré par un élément.

THM 21 : (Cauchy) G possède au moins un élément d'ordre p.

II - Les groupes abéliens finis

1) Les groupes cycliques [BERH] [ROM]

DEF 22 : On dit que G est monogène lorsqu'il est engendré par un élément : $\exists x \in G$, $G = \langle x \rangle$. On dit que G est cyclique lorsque G est monogène fini.

EX 23 :
- $\mathbb{Z}$ est monogène non cyclique
- Pour tout $n \in \mathbb{N}^*$, $\mathbb{Z}/n\mathbb{Z}$ est cyclique d'ordre n.

THM 24 :
- 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 s'ils ont même ordre

COR 25 : Soit p un nombre premier et G un groupe d'ordre p. Alors, G est cyclique et donc $G \simeq \mathbb{Z}/p\mathbb{Z}$.

PROP 26 : Soit p un nombre premier et G d'ordre p^2. Alors $G \simeq \mathbb{Z}/p^2\mathbb{Z}$ ou $G \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

THM 27 : On suppose G cyclique d'ordre n. Pour tout diviseur positif d de n, il existe un unique sous-groupe H_d d'ordre d et ce sous-groupe est cyclique. De plus, si x_0 est un générateur de G, on a : $H_d = \langle x_0^{\frac{n}{d}} \rangle = \{x \in G \,/\, x^d = e_G\}$.

REM 28 : On a donc ici une réciproque du théorème de Lagrange

THM 29 : Les groupes abéliens simples sont exactement les $\mathbb{Z}/p\mathbb{Z}$ avec p premier.

[ROT] **PROP 30 :** Soient $a \in \mathbb{Z}$ et $n \in \mathbb{N}^*$. $\bar{a}$ est un générateur de $\mathbb{Z}/n\mathbb{Z}$ si et seulement si a est premier avec n.

2) Exposant d'un groupe [BERH]

DEF 31 : On dit que G est d'exposant fini lorsqu'il existe $n \in \mathbb{N}^*$ tel que $x^n = e_G$ pour tout $x \in G$. Dans ce cas, on appelle exposant de G et on note $\exp(G)$ le plus petit entier $n \geq 1$ vérifiant cette propriété.

LEMME 32 : On suppose G d'exposant fini. Alors on a :
$\exp(G) = \mathrm{ppcm}(o(x), x \in G)$, et si G est fini, $\exp(G) \mid \#G$.

EX 33 : • Si G est cyclique d'ordre n, alors $\exp(G) = n$.
• On a $\exp(\mathfrak{S}_3) = 6$.

PROP 34 : On suppose G abélien d'exposant fini. Alors, il existe $x \in G$ d'ordre $\exp(G)$.

COR 35 : On suppose G abélien fini. Alors $\exp(G) = \#G$ si et seulement si G est cyclique.

REM 36 : $\mathfrak{S}_3$ ne possède pas d'élément d'ordre son exposant

THM 37 : Soit K un corps. Alors, tout sous-groupe fini de K^* est cyclique.

COR 38 : Soit p un nombre premier. Alors, $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique et de même, tout sous-groupe de $\mathbb{F}_q^*$ est cyclique, où $q = p^m$.

3) Structure des groupes abéliens finis [BERH]

On suppose G fini et abélien.

THM 39 [Admis] : Il existe des entiers $d_1, \dots, d_s \geq 2$ tels que $d_1 | d_2 | \dots | d_s$ tels que $G \simeq \mathbb{Z}/d_1\mathbb{Z} \times \dots \times \mathbb{Z}/d_s\mathbb{Z}$. De plus, la suite $(d_1, \dots, d_s)$ est unique et ne dépend que de la classe d'isomorphisme de G.

DEF 40 : Les entiers $d_1, \dots, d_s$ fournis par le THM 39 sont appelés les invariants de similitude de G.

COR 41 : Deux groupes abéliens finis sont isomorphes si et seulement s'ils ont les mêmes invariants de similitude.

EX 42 : • Si $G = \mathbb{Z}/24\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, alors $G \simeq \mathbb{Z}/2\mathbb{Z} \times (\mathbb{Z}/3\mathbb{Z})^3 \times \mathbb{Z}/8\mathbb{Z}$
• Il y a exactement 3 groupes abéliens d'ordre 120.

COR 43 : Pour tout diviseur d de $\#G$, il existe un sous-groupe de G d'ordre d.

THM 44 : [Admis] Si G est abélien de type fini, alors il existe des entiers $r, s \geq 0$ et des entiers $d_1, \dots, d_s \geq 2$ vérifiant $d_1 | \dots | d_s$ tels que $G \simeq \mathbb{Z}^r \times \mathbb{Z}/d_1\mathbb{Z} \times \dots \times \mathbb{Z}/d_s\mathbb{Z}$. De plus, r et $(d_1, \dots, d_s)$ sont uniques.

III - Exemples de groupes finis non abéliens

1) Le groupe symétrique

Soit $n \geq 2$. On note $\mathfrak{S}_n$ le groupe symétrique sur $[\![1;n]\!]$, de cardinal $n!$

THM 45 : Soit $\sigma \in \mathfrak{S}_n$. Alors σ se décompose en produit de cycles à supports disjoints, et cette décomposition est unique à l'ordre des facteurs près.

PROP 46 : L'ordre de $\sigma \in \mathfrak{S}_n$ est le PPCM des longueurs des cycles qui constituent sa décomposition.

PROP 47 : Le groupe $\mathfrak{S}_n$ est engendré par chacune des familles suivantes :
- les cycles
- les transpositions
- les transpositions $(1\ i)$, $i \in [\![2;n]\!]$
- les transpositions $(i\ i{+}1)$, $i \in [\![1;n-1]\!]$.
- $(1\,2)$ et $(1\,2 \dots n)$

THM 48 : Il existe un unique morphisme de groupes $\varepsilon_n : \mathfrak{S}_n \to \mathbb{C}^*$ non trivial. Si $\sigma \in \mathfrak{S}_n$ s'écrit comme produit de s transpositions, alors on a $\varepsilon_n(\sigma) = (-1)^s$.
Ce morphisme s'appelle la signature

DEF 49 : On note $\mathfrak{A}_n$ et on appelle groupe alterné de $[\![1;n]\!]$ le noyau du morphisme ε.

PROP 50 : On a $\#\mathfrak{A}_n = \frac{n!}{2}$ et $\mathfrak{A}_n$ est distingué dans $\mathfrak{S}_n$.

$\boxed{\text{THM 51 : Pour } n=3 \text{ et } n \geq 5, \mathfrak{A}_n \text{ est simple.}}$ DEV 1 [ROM]

REM 52 : $\mathfrak{A}_4$ n'est pas simple car $V_4 = \{Id, (12)(34); (13)(24); (14)(23)\}$ est distingué dans $\mathfrak{A}_4$.

PROP 53 : Si $n \geq 3$, $Z(\mathfrak{S}_n) = \{Id_{[\![1;n]\!]}\}$.

COR 54 : Si $n \neq 4$, les sous-groupes distingués de $\mathfrak{S}_n$ sont $\{Id_{[\![1;n]\!]}\}$; $\mathfrak{A}_n$ et $\mathfrak{S}_n$.

REM 55 : Si $n=4$, il faut rajouter V_4 à cette liste

2) Le groupe diédral [ROM] [PER]

[Rai]

DEF 56 : On dit que G est diédral de type D_{2n} lorsqu'il est engendré par deux éléments : ρ d'ordre n et $\sigma \neq \rho$ d'ordre 2 tel que $\rho\sigma\rho\sigma = Id$ i.e $\rho\sigma$ est d'ordre 2.

THM 57 : Si G est un groupe diédral de type D_{2n}, on a :
$G = \{Id, \rho, \dots, \rho^{n-1}\} \cup \{\sigma, \sigma\rho, \dots, \sigma\rho^{n-1}\}$ et il est d'ordre $2n$. De plus deux groupes diédraux de type $2n$ sont isomorphes.

REM 58 : Le groupe diédral d'ordre $2n$ possède une interprétation géométrique : il peut se voir comme le groupe des isométries du plan euclidien conservant un polygône régulier à n côtés. Il contient les n rotations $\rho(0, \frac{2k\pi}{n})$ pour $k \in [\![0, n-1]\!]$ et les n réflexions par rapport aux droites passant par O (centre du n-gone) et les sommets ou les milieux des côtés du n-gone.

PROP 59 : Le groupe diédral est non abélien.

PROP 60 : Le sous-groupe constitué des rotations est distingué et isomorphe à $\mathbb{Z}/n\mathbb{Z}$. Comme $\#D_{2n} = 2n$, on a la suite exacte $1 \to \mathbb{Z}/n\mathbb{Z} \to D_n \to \mathbb{Z}/2\mathbb{Z} \to 1$ et un isomorphisme $D_{2n} \simeq \mathbb{Z}/2\mathbb{Z} \ltimes \mathbb{Z}/n\mathbb{Z}$

peut être retiré

3) Le groupe des quaternions [DEL]

DEF 61 : On définit le groupe des quaternions par :
$\mathbb{H}_8 \simeq \langle a, b \,/\, a^4 = e, b^2 = a^2, ba = a^3 b \rangle$

PROP 62 : C'est un groupe à 8 éléments dont un élément d'ordre 1 (e), un élément d'ordre 2 (a^2), et 6 éléments d'ordre 4.

REM 63 : Les groupes D_8 et $\mathbb{H}_8$ ne sont pas isomorphes.

PROP 64 : $\mathbb{H}_8$ possède 6 sous-groupes tous abéliens et distingués dans $\mathbb{H}_8$.

REM 65 : Un tel groupe est appelé hamiltonien.

4) Autour du groupe linéaire [ROM] [CAL CVAL]

Soit K un corps commutatif à $q = p^m$ éléments (p premier) et E un K-espace vectoriel de dimension finie $n \in \mathbb{N}^*$. On identifie $GL(E)$ et $GL_n(K)$.

THM 66 : Soit G un sous-groupe de $GL(E)$. LASSE :
- G est fini
- G est d'exposant fini

PROP 67 : On a : $\#GL(E) = \prod_{k=1}^{n-1}(q^n - q^k) = q^{\frac{n(n-1)}{2}} \prod_{k=1}^{n-1}(q^k - 1)$
$\#SL(E) = q^{n-1} \prod_{k=1}^{n-1}(q^n - q^{k-1}) = q^{\frac{n(n-1)}{2}} \prod_{k=2}^{n}(q^k - 1)$

DEV 2

LEMME 68 (Fitting) : Soit $u \in \mathcal{L}(E)$. Les suites $(\ker(u^k))_{k\in\mathbb{N}}$ et $(\operatorname{Im}(u^k))_{k\in\mathbb{N}}$ sont respectivement croissante et décroissante et stationnent à partir du même rang n_0. On a $E = \ker(u^{n_0}) \oplus \operatorname{Im}(u^{n_0})$ et $v = u_{|\ker(u^{n_0})}$ est nilpotent, $w = u_{|\operatorname{Im}(u^{n_0})}$ est bijectif. Cette décomposition munie de v, w est la décomposition de Fitting de u.

PROP 69 : Il y a $n_d = q^{d(d-1)}$ matrices nilpotentes de taille $d \times d$ à coefficients dans $\mathbb{F}_q$.