1. Leçon 104 : Groupes Finis. Exemples et applications.

1. Rapport du jury. — *Dans cette leçon il faut savoir manipuler correctement les éléments de différentes structures usuelles (Z/nZ, S, etc.) comme, par exemple, en proposer un générateur ou une famille de générateurs, savoir calculer un produit de deux permutations, savoir décomposer une permutation en produit de cycles à supports disjoints. Il est important que la notion d'ordre d'un élément soit mentionnée et comprise dans des cas simples. Le théorème de structure des groupes abéliens finis doit être connu. Les exemples doivent figurer en bonne place dans cette leçon. Les groupes d'automorphismes fournissent des exemples très naturels. On peut aussi étudier les groupes de symétries A4, S4, A5 et relier sur ces exemples géométrie et algèbre, les représentations ayant ici toute leur place ; il est utile de connaître les groupes diédraux. S'ils le désirent, les candidats peuvent ensuite mettre en avant les spécificités de groupes comme le groupe quaternionique, les sous-groupes finis de $SU(2)$ ou les groupes $GL_n(F_q)$.*

2. Préambule : rappels des fondamentaux. —

1. *Définitions.* — :

- Rem : Définition de groupe, de groupe abélien. Groupes finis. Notations usuelles multiplicative et additive.
- Exo : *Appropriation par les manipulations* : l'élément neutre est unique, l'inverse à droite et à gauche coïncident, si tous les éléments sont symétriques le groupe est abélien, ...
- Exe : *Par la suite nous examinerons régulièrement les exemples suivants* :
  - groupes cycliques $\mathbb{Z}/n\mathbb{Z}$
  - groupes diédraux D_n
  - groupe symétrique $\mathfrak{S}_n$ et groupe alterné $\mathfrak{A}_n$
  - groupe de base des Quaternion noté $\mathbf{Q}$.

2. *Morphismes.* — :

- Def : Homomorphisme de groupe. Monomorphisme, épimorphisme et isomorphisme (notions équivalentes en cardinal fini).
- Def : Notion de noyau et d'image.
- Rem : Homomorphisme $\phi_a : \mathbb{Z} \to (G, +)$ donné par $\phi(n) = (a + ... + a)$ et notation $n \cdot x$.
- Exe : Signature d'une permutation ou orientation d'une isométrie.
- Théorème I d'isomorphisme de Emmy Noether : $G/Ker(f) \sim Im(f)$.
- Thé : Théorème de Cayley - l'homomorphisme entre G et les permutations de G

3. *Sous-groupes.* —

- Def : Sous-groupes. Propriétés minimum à vérifier (les autres découlent par héritage). Sous-groupe propre.
- Def : Noyau et Image d'un morphisme. Exemple : groupe alterné.
- Pro : L'intersection de sous-groupes est un sous-groupe.
- Def : Sous-groupe engendré par une partie; construction "par lintérieur" et "par l'extérieur". Partie génératrice d'un (sous)groupe.
- Exe :
  - quelques générateurs pour σ_n (cycles, transpositions, ...).
  - générateurs pour D_n (r et s).
  -
- Def : ordre d'un élément et exposant pour un groupe fini.
- Thé : Théorème de Lagrange - $|G| = |H|x[G : H]$
- Rem : la réciproque est fausse en général. Ainsi le groupe alterné U_4 est d'ordre 12 mais n'a aucun sous-groupe d'ordre 6. (page 23 Hauchecorne)
- Représentation graphique : treillis de sous-groupes.

3. Action d'un groupe sur un ensemble. —

- Def : action à gauche. Un groupe multiplicatif G d'élément neutre e agit/opère à gauche sur un ensemble X au travers d'une application $\Phi : G \times X \to X$ vérifiant :
  - $\forall x \in X$, $\Phi(e, x) = x$
  - $\forall g_1, g_2 \in G$ et $\forall x \in X$, $\Phi(g_1 g_2, x) = \Phi(g_1, \Phi(g_2, x))$
  - soit, en notant $\Phi(g, x) = g \cdot x$, $g_1 \cdot (g_2 \cdot x) = (g_1 g_2) \cdot x$
- Rem : On définit de manière similaire les groupes opérant à droite.
- Exe : Les rotations dans l'espace qui préservent le cube unitaire opèrent sur le Rubik's cube.
- Exe : $\mathfrak{S}(X)$ opère sur X par $f \cdot x = f(x)$
- Exe : $GL(E)$ agit sur les droites de l'esp-vect E, en associant à f et à D, la droite $f(D)$.
- Exe : $GL_n(\mathbb{R})$ agit par application sur $\mathbb{R}^n$ et par conjugaison sur $M_n(\mathbb{R}^n)$.
- Pro : Il est équivalent de se donner un homomorphisme $\varphi : G \to \mathfrak{S}(X)$ en posant $g \cdot x = \varphi(g)(x)$
- Exe : G opère sur lui même :
  - Def : par translation à gauche. $s \cdot x = sx$
  - Def : par conjugaison. $g_1 \cdot g_2 = g_1 g_2 (g_1)^{-1}$
  - Def : action sur les classes modulo un sous-groupe (même non normal/distingué) : $(g_1, g_2 \cdot H) \mapsto (g_1 g_2) \cdot H$
- Def : Soit $x \in X$. On définit le stabilisateur de x : $H_x = Stab(x) := g \in G : g \cdot x = x$. C'est un sous-groupe de G.
- Exe : Si G opère sur lui-même par translation, le stabilisateur de tout élément sera le singleton $\{e\}$. Si G opère par conjugaison, le stabilisateur d'un élément g sera fait du sous-groupe de G des éléments commutant avec g, c'est à dire le "Centralisateur" de g.
- Pro : Pour toute action de G sur X nous avons : $Stab(g \cdot x) = gStab(x)g^{-1}$
- *Orbite* :
  - Def : Orbite de $x \in X$, $\mathscr{O}_x = \{y \in X : \exists g \in G g \cdot x = y\}$. Il s'agit d'une classe d'équivalence pour la relation $[x \sim y] \iff [\exists g \in G, g \cdot x = y] \iff [\mathscr{O}_x = \mathscr{O}_y]$.

- Notation équivalente : $\mathscr{O}_x = Gx$.
- Rem : $\forall g \in G$, $\forall x \in X$, $\mathscr{O}_{\{gx\}} = \mathscr{O}_{\{x\}}$
- Pro : $G/H_x \equiv \mathscr{O}_x$.
- Exe : lorsque G agit sur lui-même par conjugaison, les orbites sont les classes de conjugaison.
- Exe : Les orbites de $\mathbb{R}^n$ sous l'action naturelle de $O_n(\mathbb{R})$ sont les sphères de centre l'origine.
- App : Décomposition d'une permutation σ en produit de cycles à supports disjoints : on construit les supports disjoints comme les orbites par l'action du groupe $< \sigma >$.

1. *Quelques propriétés.* —

- Pro : Pour chaque $x \in X$, l'application de G $Stab(x) \to \mathscr{O}_x$ qui à $\dot{g}$ associe $g \cdot x$ est bijective (et bien définie). Et donc si G est fini, $Card(\mathscr{O}_x) = Card(G)/Card(Stab(x))$.
- Cor : *Formule des classes* - Si X et G sont finis, si $(x_i)_{i\in I}$ est l'ensemble des orbites sous l'action de G, $Card(X) = \Sigma_{i\in I} Card(G)/Card(Stab(x_i))$.
- Def : le "Fixé" par $g \in G$ est le sous-ensemble des $x \in X$ qui sont fixés par g, ie tels que $g \cdot x = x$. On le note $fix(g)$.
- Def : On peut aussi définir le fixateur d'une partie A de G ou de G lui-même.
- Cor : *Formule de Burnside* - Si X et G sont finis, le nombre r d'orbites différentes de X sous l'action de G est donné par : $r = \dfrac{1}{Card(G)} \Sigma_{g\in G} Card(fix(g))$.
- Développement 1 : *théorèmes de Sylow*
  - Déf : On dit que G est un p-groupe si l'ordre de G est une puissance de $p \in \mathbb{P}$. Si G est d'ordre $p^n m$ avec $m \wedge p = 1$, on dit qu'un sous-groupe H de G est un p-Sylow de G si H est d'ordre p^n .
  - Rem 1 : Soit S un sous-groupe de G ; S est un p-Sylow de G si et seulement si S est un p-groupe et $(G : S)$ est premier à p.
  - Rem 2 : Tout conjugué d'un p-Sylow de G est un p-Sylow de G.
  - The 1 : Tout groupe fini possède au moins un p-Sylow.
  - Lem : Soit H un sous-groupe de G et soit S un p-Sylow de G. Alors il existe $g \in G$ tel que $H \cap gSg^{-1}$ soit un p-Sylow de H.
  - Cor : Si G a des p-Sylow et si H est un sous-groupe de G, alors H a aussi des p-Sylow.
  - Soit G un groupe fini d'ordre n. On peut plonger G dans le groupe symétrique $\mathfrak{S}_n$ d'après Cayley. D'autre part, $\mathfrak{S}_n$ se plonge dans $GL_n(\mathbb{K})$ (où $\mathbb{K}$ est un corps fini de caractéristique p) : si $\sigma \in \mathfrak{S}_n$ et si $(e_i)_{1lei\leq n}$ est une base de $\mathbb{K}^n$, on associe à σ la transformation linéaire f définie par $f(e_i) = e_{\sigma(i)}$. Donc G se plonge dans $GL_n(\mathbb{K})$.
  - Il reste à montrer que $GL_n(\mathbb{K})$ a un p-Sylow. Pour cela considérons le groupe P constitué des matrices triangulaires supérieures à coefficients diagonaux égaux à 1. C'est un sous-groupe de $GL_n(\mathbb{K})$ d'ordre $|P| = qn(n-1)/2 = pfn(n-1)/2$. Donc P est un p-Sylow de $GL_n(\mathbb{K})$.
  - The 2: Soit G un groupe de cardinal $n = p^\alpha m$ avec $p \wedge m = 1$.
    - Si H est un p-groupe de G il est inclus dans un p-Sylow de G.
    - Tous les p-Sylow sont conjugués entre eux.
    - Le nombre de p-Sylow divise n et aussi il est congru à 1 modulo p.
  - App : quelques applications des théorèmes de Sylow
    - Exo : des groupes d'ordre 63 ou 255 ne sont pas simples.
    - Cor : (Cauchy comme corollaire) Si p divise l'ordre de G, alors G contient un élément d'ordre p.
    - Cor : un p-Sylow est normal/distingué ssi il est le seul (puisque les autres lui sont conjugués).
    - Cor : Soit p le plus petit nombre premier divisant $Card(G)$. Tout sous-groupe d'indice p est distingué.
    - Exe : Il n'existe qu'un seul groupe (à isomorphisme près) tel que $Card(G) = pq$ $(p, q \in \mathbb{P}$, $p \neq q$ et $p \wedge (q-1) = 1)$: $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$. (En effet $\mathbb{Z}/p\mathbb{Z}$ est distingué/normal).
    - Rem : Si on analyse $\mathfrak{S}_3$ dont le cardinal est 2×3 et où 2 divise $(3-1)$ nous n'avons pas la structure $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.

4. Groupes cycliques (monogènes finis). — : .

- Def : Un groupe G est cyclique lorsqu'il est fini et engendré par un seul élément, ie $\exists a \in G$ tel que $G =< a >$. Un tel élément est un *générateur* de G et on a $Card(G) = \omega(a)$.
- Pro : $G =< a > \sim \mathbb{Z}/\omega(a)\mathbb{Z}$ à travers la fonction $\phi(n) = n \cdot a$ qui est bijective en cardinal fini.
- $G = \{a, a^2, \cdots, a^n\}$ et $a^n = 1_G$.
- $\forall k \in \{1, \cdots, n\} \omega(a^k) = \dfrac{n}{n \wedge k}$.
- On a donc $\varphi(n)$ automorphismes donnés chacun par $\phi(a) = a^k$ avec $k \wedge n = 1$.
- Pro : si G est cyclique, nous avons *un et un seul* sous-groupe H qui est d'ordre d pour chaque $d|n$.
- Exe : Le groupe des racines n-ièmes de l'unité $\mathbb{U}_n$ est cyclique d'ordre n, engendré par $exp(2i\pi/n)$.
- Pro : Le groupe des inversibles de l'anneau $\mathbb{Z}/p\mathbb{Z}$ est cyclique d'ordre p-1.
- Rem : Trouver les inversibles passe alors par une décomposition en facteurs premiers, opération lourde.

5. Groupes Abéliens. — :

1. *Propriétés.* — :

- Pro : Si G est abélien, l'ordre du produit de deux éléments est le ppcm des deux ordres. *Prop*: l'exposant d'un groupe abélien est le ppcm des ordres de ses éléments.

.

Développement : *théorème de Kronecker de structure des groupes abéliens :*

– Thé : il existe $d_1|d_2|\cdots|d_r$ tels que $G \sim (\mathbb{Z}/d_1\mathbb{Z} \times \cdots \mathbb{Z}/d_n\mathbb{Z})$
– Ces entiers sont uniques. Ils sont appelés facteurs invariants de G.
– Exe : $Card(G) = 600 = 2^3 \times 3 \times 5^2$. Les seules possibilités sont $\mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/60\mathbb{Z}$, $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/120\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/300\mathbb{Z}$ et $\mathbb{Z}/600\mathbb{Z}$.
– Exe : $\mathbb{Z}/36\mathbb{Z}$. On note le faux cas 2, 2, 3, 3 et aussi 4, 9.

6. Groupes non abéliens. — :

– Exe : $\mathfrak{S}_n$, $\mathfrak{A}_n$, $GL(E)$, Q ne sont pas abéliens.
– Exe : tous les groupes d'ordre 8.
– Si G n'est pas abélien nous n'avons pas forcément une structure de groupe héritée sur l'ensemble G/H des classes d'équivalence à gauche d'un sous-groupe H
– Sous-groupe normaux/distingués :
  • $\forall x, xH = Hx$ et donc les classes d'équivalence à gauche et à droite coïncident.
  • Alors G/H a une structure de groupe.
  • Théorème II d'isomorphisme de Emmy Noether : H et J sous-groupes de G. J normal. HJ est un groupe et on a un isomorphisme entre $H/(H \cap J) \sim HJ/J$
  • Théorème III d'isomorphisme de Emmy Noether : H et J sous-groupes normaux de G avec $H \subset J$. Alors H est normal dans J, J/H est un sous-groupe normal de G/J et $(G/H)/(J/H) \sim G/J$.
– Def : Un groupe est dit "simple" si ses seuls sous-groupes distingués sont triviaux.
– Les sous-groupes non-simples (ayant donc un sous-groupe distingué N non trivial) peuvent être catalogués par récurrence dans la mesure où ils peuvent être ramenés au produit (semi-)direct de deux groupes de moindre cardinal suivant la suite exacte suivante : $1 \to N \to G \to G/N \to 1$.
– Développement - Le sous-groupe alterné est simple à partir de n=5

1. *Sous-groupes canoniques.* —

– Def : Centre d'un groupe - $Z(G) = \{x \in G : \forall y \in G xy = yx\}$
– Pro : $Z(G)$ est abélien et normal.
– Exe : $Z(Q) = \{1, -1\}$; $Z((S)_n) = \{1\}$ pour $n \geq 3$.
– Exe : $Z(D_{2m} = \{1, r^m\}$ et $Z(D_{2m+1} = \{1\}$.
– Exe : $Z(GL(n, \mathbb{R}) = \{\lambda \cdot Id\}$.
– Groupe dérivé (engendré par les commutants $[xy] = xyx^{-1}y^{-1}$). $G' = \{[x_1y_1] \cdots [x_ky_k] : x_i, y_i \in G; n \geq 0\}$.
– Rem : Ce sous-groupe mesure l'écart au caractère abélien.
– Pro : G' est un sous-groupe normal/distingué de G.
– Exe : $(S)_n = \{1\}$. $Q' = \{1, -1\}$. $D'_n =< r^2 >$.
– Def : On appelle Abélien d'un groupe G le quotient G/G'. C'est un groupe Abélien.
– Exe : $Ab(D_{n=2p+1})$ et $Ab(D_{n=2p})$

2. *Sources :* —

– Hauchecorne
– Invitation à l'algèbre
– Perrin

January 10, 2018

Bruno Nitrosso, EPP et candidat libre