104: groupes finis. Exemples et applications.

Pierre Lissy

May 6, 2010

1 Exemples classiques de groupes finis

1.1 Définition et premières propriétés

Définition 1. *Un groupe fini est un groupe d'ordre fini, noté n.*

Théorème 1 (Lagrange)**.** *Le cardinal de tout sous groupe de G le cardinal de G. Plus précisément,* $Card(G)/Card(H) = Card(G/H)$.

Inversément,il n'existe pas toujours de groupe d'ordre d avec d un diviseur de n.

Exemple 1. *Il n'existe pas de sous-groupe d'ordre 6 dans* A_4.

Corollaire 1. *Tout élément du groupe vérifie* $a^n = 1$. *De plus l'ordre d'un élement, qui est le cardinal du groupe engendré par cet élément, est le plus petit* k *tq* $a^k = 1$. k *divise* n.

Application 1 (Euler-Fermat)**.** $a^{\varphi(n)} \equiv 1[n]$

Proposition 1 (Cayley)**.** *Tout groupe d'ordre* n *s'injecte dans* $\mathbb{S}_n$.

Application 2. *Un groupe d'ordre* $2n$ *avec* n *impair n'est jamais simple.*

Application 3. *Un 2-Sylow ne peut être cyclique (sauf si le groupe est déjà égal à* Z_4 *ou que le 2-Sylow est d'ordre 2)*

1.2 Les groupes $\mathbb{Z}/n\mathbb{Z}$

Définition-proposition 1. *Considérons le groupe des entiers* $\mathbb{Z}$. *Ses seuls idéaux sont les ensembles* $n\mathbb{Z}$, *avec* $n \in \mathbb{N}$. *On peut donc s'intéresser au groupe quotient* $\mathbb{Z}/n\mathbb{Z} := \{a + n\mathbb{Z} | a \in \mathbb{Z}\} = \{a + n\mathbb{Z} | a \in \{0, \dots, n-1\}\}$, *ces* n *dernières classes étant distinctes. C'est donc un ensemble à* n *éléments. La classe de* a *modulo* n *sera notée* $C_n(a)$.

Remarque 1. *En fait on munit* $\mathbb{Z}/n\mathbb{Z}$ *d'une structure d'anneau. On peut donc s'intéresser à ses inversibles.*

Proposition 2. *Soit* $n \in \mathbb{N}$. *Dans* $\mathbb{Z}/n\mathbb{Z}$, $o(C_n(m)) = \dfrac{n}{n \wedge m}$. *Donc* $(\mathbb{Z}/n\mathbb{Z}, +)$ *est cyclique et ses générateurs sont les* m *tels que* $n \wedge m = 1$.

Proposition 3. $C_n(k)$ *est inversible dans* $(\mathbb{Z}/n\mathbb{Z}, *) \Leftrightarrow k \wedge n = 1 \Leftrightarrow k$ *engendre* $(\mathbb{Z}/n\mathbb{Z}, +)$.

Proposition 4. *Tous les groupes cycliques d'ordre* n *sont isomorphes à* $\mathbb{Z}/n\mathbb{Z}$. *De plus,* $\mathbb{Z}/n\mathbb{Z}$ *admet un unique sous-groupe d'ordre* d *avec* d *divise* n*: c'est le groupe engendré par* n/d.

Inversément, un groupe dont tout sous-groupe strict est cyclique n'est même pas forcément abélien, par exemple le groupe des quaternions.

Proposition 5. *Tout groupe d'ordre* p *premier est nécessairement isomorphe à* $\mathbb{Z}/\mathbb{Z}$.

1.3 Groupes symétriques et alternées

Définition 2. *Soit E un ensemble. Le groupe symétrique est le groupe (pour la composition) des bijections de E dans E, noté $Bij(E)$. Si E est fini, son groupe des bijections est isomorphe à celui de $\{1,\dots,|E|\}$, noté $\mathcal{S}_{|E|}$. Un élément de $\mathcal{S}_n$ est appelé une permutation.*

Théorème 2. *Les transpositions engendrent $\mathcal{S}_n$. De plus, toute permutation s'écrit comme produit d'au plus $n-1$ transpositions.*

Théorème 3. *Les cycles engendrent S_n. Plus précisément, toute permutation s'écrit de manière unique (à l'ordre près) comme produit de cycles à support disjoints commutant deux à deux.*

Définition-proposition 2. *Soit $\sigma \in \mathcal{S}_n$. On note $i(\sigma)$ le nombre d'inversions dans la permutation σ (ie. le nombre de couples (i,j) avec $i<j$ tels que $\sigma(i) > sigma(j)$). Alors*

$$\begin{array}{rccc} \varepsilon: & \mathcal{S}_n & \to & (\{-1,1\}) \\ & \sigma & \mapsto & (-1)^{i(\sigma)} \end{array}$$

est un morphisme de groupe non trivial, appelé signature. On a la formule $\varepsilon(\sigma) = \prod_{i<j} \frac{\sigma(j)-\sigma(i)}{j-i}$. C'est l'unique morphisme de groupe non trivial de $\mathcal{S}_n$ vers $\{-1,1\}$. De plus, ε vaut -1 sur les transpositions et pour un p-cycle a, $\varepsilon(a) = (-1)^{p+1}$.

Définition 3. *Une permutation de signature 1 est dite paire, une permutation de signature -1 est dite impaire.*

Définition-proposition 3. *Le sous-groupe des permutations de signature 1 (ie. $Ker\varepsilon$) est appelé le groupe alterné de $\mathcal{S}_n$, noté $\mathcal{A}_n$. Son cardinal est $n!/2$ (sauf si n=1) et s'est le seul sous-groupe d'indice 2 de $\mathcal{S}_n$.[2][page 80]*

Théorème 4. *Les A_n sont simples pour $n=3$ et $n \geqslant 5$. A_4 contient un unique sous-groupe strict distingué non trivial isomorphe au groupe de Klein.*

Corollaire 2. *Le centre de S_n est trivial, $D(S_n) = D(A_n) = A_n$.*

Proposition 6. *Classes de conjugaisons = permutations du même type.*

1.4 Groupes diédraux

Définition 4. *Le groupe diédral D_n est le groupe des isométries laissant invariantes le polygône régulier à n côtés.*

Proposition 7. *Le groupe diédral est composé de n rotations et de n symétries orthogonales,il est de cardinal $2n$. L'ensemble des rotations forment un sous-groupe distingué de D_n.*

Proposition 8. *Soit r la rotation d'angle $2\pi/n$ et s une réfléxion quelconque s. Alors r et s engendrent D_n.*

Proposition 9. *Les rotations sont d'ordre n, les réfléxions d'ordre 2. Les conjugués d'une rotation sont elle-même et son opposé. Les réflexions sont toutes conjuguées dans le cas impair, dans le cas pair il y a deux classes de conjugaison: celles qui passent par les sommets et celles qui passent par les milieux des sommets. Le centralisateur d'une rotation est l'ensemble des rotations, celui d'une réfléxion dans le cas impair est la réflexion et l'identité, dans le cas impair c'est le gorupe engendré par la réfléxion et $-Id$.*

Proposition 10. *Sous-groupes distingués: les r^d avec $d|n$, dans ce cas le quotient est D_d. Les autres sous-groupes distingués sont dans le cas pair $< r^2, s >$ et $< r^2, rs >$, avec pour quotient $\mathbb{Z}/2\mathbb{Z}$.*

Proposition 11. *Le centre de D_n est réduit au neutre si n impair, le centre de D_2 est D_2 tout entier, le centre de D_{2n} est Id et $-Id$. Le sous-groupe dérivé est le groupe engendré par R^2.*

1.5 Groupe des quaternions

Définition 5. *On considère l'ensemble des matrices Id et son opposé, .; Muni du produit matriciel c'st un groupe.*

Proposition 12. *H_8 possède un sous-groupe d'ordre 2 et 3 sous-groupes d'ordre 4.*

Proposition 13. *Tout les sous-groupes sont distingués.*

Remarque 2. *H_8 est indécomposable puisque tous ses sous-groupes stricts contiennent Id et $-Id$.*

2 Actions sur les groupes finis

2.1 Formule des classes et applications

Théorème 5 (Formule des classes)**.** *Supposons G et X finis. Soit ω un ensemble de représentants des orbites de X. Alors $|X| = \sum_{x\in\omega} \frac{|G|}{Stab(x)}$.*

Application 4. *En utilisant l'action de conjugaison, on montre que le centre d'un p-groupe n'est jamais trivial.[1] On en déduit que si G un groupe d'ordre p^α. Alors $\forall i \leqslant \alpha$, il existe un sous-groupe distingué d'ordre p^i. Un p-groupe n'est donc jamais simple (sauf si c'est $\mathbb{Z}/p\mathbb{Z}$).*

Application 5 (Théorème de Cauchy)**.** *[2][page 45] Soit G un groupe d'ordre n et p un facteur premier de n. Alors on montre en faisant agir $\mathbb{Z}/p\mathbb{Z}$ sur G^p qu'il existe des éléments d'ordre p dans G.*

Application 6 (Théorème de Wedderburn)**.** *[1][page 82]Soit k un corps fini. On montre en faisant agir k^* sur lui-même par conjugaison que l'hypothèse de commutativité dans la définition des corps découle des autres axiomes.*

2.2 Formule de Burnside et applications

Théorème 6. *Soit G un groupe fini agissant sur un ensemble fini X. Soit $g \in G$. on note $fix(g)$ l'ensemble des points fixes de g pour l'action de G sur X. Alors le nombre d'orbites vaut $\frac{1}{|G}\sum_{g\in G} |fix(G)|$*

Application 7. *On se donne 4 perles rouges, 3 perles bleues et 2 perles jaunes. On peut à l'aide de ses éléments fabriquer 76 colliers différents. Si on se donne 4 perles rouges, 6 perles bleues et 4 perles jaunes, on peut fabriquer 7575 colliers différents. ATTENTION peut-être erreur du combes? à réfléchir (multiplier par 7 pour les symétries...)*

Application 8 (sous-groupes du groupe des déplacements[2][page 171)**.** *]Tout sous-groupe fini d'ordre supérieur ou égal à 2 de l'ensemble des déplacements de l'espace est isomoprhe soit au sous-groupes des racines n-ièmes de l'unité, soit au groupe diédral $D_{n/2}$, soit à $\mathcal{A}_4$ ou $\mathcal{A}_5$ ou $\mathcal{S}_5$.*

2.3 Théorèmes de Sylow et applications

Théorème 7 (Théorèmes de Sylow)**.** *[1][page 19] Soit G un groupe d'ordre $p^\alpha m$ avec $p \wedge m = 1$. Alors G admet au moins un sous-groupe d'ordre p^α, ces sous-groupes sont tous conjugués et leur nombre est un diviseur de m, congru à 1 modulo p.*

Application 9. *Le seul sous-groupe simple d'ordre 60 est A_5.*

Application 10.

2.4 Produits semi-directs et applications

Définition 6. *Soit N et H deux groupes etφ une action de H sur N définie par automorphismes. La loi suivante sur $N \times H$: $(n,h)(n',h') = (n\varphi(h)n', hh')$ définit une loi de groupe $N \times H$ appelé produi semi-direct de N par H noté $N \rtimes_\varphi H$.*

Remarque 3. *N est un sous-groupe distingué de $N \rtimes_\varphi H$ au contraire de H qui n'en est pas un en général. On a même:*

Théorème 8. *$N \rtimes_\varphi H$ abélien $\Leftrightarrow$ φ trivial $\Leftrightarrow$ H distingué.*

Remarque 4. *Si N est distingué dans G et que H est un sous-groupe de G alors NH est un groupe.*

Théorème 9. *Soit G un groupe, H et N, avec N distingué dans G, $NH = G$ et $N \cap H = 1$. Alors G s'écrit comme produit semi-direct*

Application 11. *Tout sous-groupe d'ordre p^2 est commutatif et isomorphe à $\mathbb{Z}/p^2\mathbb{Z}$ ou $\mathbb{Z}/p\mathbb{Z}^2$.*

Exemple 2. *valable pour 4,9,32,49,64..*

Application 12. *Tout sous-groupe d'ordre pq est isomorphe à $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$ si p et q-1 sont premiers entre eux, si p divise q-1 alors on a deux classes d'isomorphie, $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$ et au produit semi-direct $\mathbb{Z}/p\mathbb{Z} \rtimes \mathbb{Z}/q\mathbb{Z}$*

Exemple 3. *Sous-groupes d'ordre 6: S_3 et $\mathbb{Z}/3\mathbb{Z}$. Sous-groueps d'ordre 15,33,51,35: seulement cveux abéliens. Sous-groupes d'ordre 10,14,22,26,34,38: l'abélien et le produit semi-direct*

Application 13. *P impair premier. Tout groupe d'ordre p^3 est isomorphe soit à $\mathbb{Z}/p^3\mathbb{Z}$ ou $\mathbb{Z}/p\mathbb{Z}^2 \times \mathbb{Z}/\mathbb{Z}^2$ ou $\mathbb{Z}/p^3\mathbb{Z}$ ou au produit semi-direct $\mathbb{Z}/p\mathbb{Z}^2 \rtimes \mathbb{Z}/\mathbb{Z}^2$ ou au produit semi-direct $\mathbb{Z}/p\mathbb{Z}^2 \rtimes \mathbb{Z}/\mathbb{Z}$.*

Exemple 4. *Groupes d'ordre 27: les 3 abéliens et les produits semi-directs.*

Remarque 5. *Il existe des groupes qui ne sont pas décomposables en produits semi-directs de la forme $\mathbb{Z}/\mathbb{Z}$, par exemple parmi les 5 groupes d'ordre 8,on en a trois abéliens, le diédral D_4 et le groupe des quaternions H_8 pas décomposable.*

Proposition 14. *Le groupe diédral est isomorphe à un produit semi-direct $\mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$. Le groupe symétrique est isomorphe à un produit semi-direct $\mathbb{A}_n \rtimes \mathbb{Z}/2\mathbb{Z}$.*

3 Groupes abéliens

3.1 Lemme chinois

Théorème 10. *Soient $p_1, \ldots, p_n$ des entiers premiers entre eux deux à deux. Alors en tant qu'anneaux, $\mathbb{Z}/p_1p_2\ldots p_n \simeq \mathbb{Z}/p_1\mathbb{Z} \times \mathbb{Z}/p_2\mathbb{Z} \times \ldots \times \mathbb{Z}/p_n\mathbb{Z}$. Inversément, si $\mathbb{Z}/p_1p_2\ldots p_n \simeq \mathbb{Z}/p_1\mathbb{Z} \times \mathbb{Z}/p_2\mathbb{Z} \times \ldots \times \mathbb{Z}/p_n\mathbb{Z}$ alors les nombres $p_1, \ldots, p_n$ sont premiers entre eux deux à deux.*

Exemple 5. $\mathbb{Z}/6\mathbb{Z} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.

Corollaire 3. *Soient $p_1, \ldots, p_n$ des entiers premiers entre eux deux à deux. Alors en tant que groupes, $(\mathbb{Z}/p_1p_2\ldots p_n)^* \simeq (\mathbb{Z}/p_1\mathbb{Z} \times \mathbb{Z}/p_2\mathbb{Z} \times \ldots \times \mathbb{Z}/p_n\mathbb{Z})^*$*

Remarque 6. *On cherche à résoudre le système de congruence suivant:*

$$\begin{cases} x \equiv a[n] \\ x \equiv b[m] \end{cases}$$

avec $n \wedge m$=1. Le lemme chinois nous assure qu'il existe une solution x_0. De plus, toutes les autres solutions du système sont alors de la forme $x_0 + nmt$ avec $t \in \mathbb{Z}$. Il reste donc à trouver une solution particulière: si u est un inverse de n modulo m (que l'on peut calculer explicitement avec l'algorithme d'Euclide étendu), on peut montrer que $a + n(b-a)u$ convient.

Exemple 6.

$$\begin{cases} x \equiv 10[47] \\ x \equiv 5[111] \end{cases}$$

Les solutions sont de la forme $4334 + 5217t$.

3.2 Structure des groupes abéliens

Théorème 11. *Tout groupe abélien est isomorphe à un produit direct de $\mathbb{Z}/n\mathbb{Z}$. Tout groupe abélien fin iest isomporhe au produit direct de ses p-Sylow.*

Exemple 7. *Il y a 7 sous-groupes abéliens de cardinal 32. Il y a 5 sous-groueps abéliens de cardinal 16.*

Proposition 15. *Pour les groupes abéliens, il existe des sous-groupes de cardinal d avec d un diviseur de n.*

4 Groupes finis en algèbre linéaire

4.0.1 Groupes spéciaux linéaires projectifs [1]

Théorème 12. *1. $PSL_2(\mathcal{F}_2) \simeq \mathcal{S}_3$*

2. $PSL_2(\mathcal{F}_3) \simeq \mathcal{A}_4$

3. $PSL_2(\mathcal{F}_4) \simeq \mathcal{A}_5$

4. $PSL_2(\mathcal{F}_5) \simeq \mathcal{A}_5$

4.1 Théorème de Burnside

En général si tous les éléments du groupe vérifient $x^n = Id$ le groupe n'est pas fini.

Exemple 8. *Les suites de F_2 pour l'addition.*

Théorème 13. *Tout sous-groupe de $GL_n(\mathbb{C})$ d'exposant fini est fini.*

4.2 Sous-groupes finis des groupes orthogonaux

Théorème 14. *Soit G un sous-groupe fini de $O_2(\mathbb{R})$.*

1. *Soit $G \subset SO(E)$. Alors G est formée de rotation d'angle $2k\pi/n$. G est alors un groupe cyclique d'ordre n, et est donc isomorphe à Z/nZ.*

2. *Soit $G \not\subset So(E)$. Alors G est de cardinal pair et est un certain groupe diédral (ou $Z/2Z$ si il contient juste une symétrie et Id).*

Lemme 1 (Formule des classes)**.** *Soit G un groupe agissant sur un ensemble X. Supposons G et X finis. Soit ω un ensemble de représentants des orbites de X. Alors $|X| = \sum_{x\in\omega} \frac{|G|}{Stab(x)}$.*

Définition 7. *On appelle pôle d'un rotation u différente de l'identité l'intersection de l'axe de U et de la sphère unité. C'est un ensemble à n éléments. Soit G un sous-groupe fini de $SO(3, R)$ non trivial de cardinal n . On note X l'ensemble des pôles des éléments de G privé de l'identité. X est un ensemble de cardinal au moins 2 et inférieur à $2(n-1)$*

Proposition 16. *G agit sur X de la manière évidente, ie $g.x = g(x)$.*

En utilisant cette action, la formule des classes et la formule de Burnside, on démontre

Théorème 15. *Les sous-groupes finis de $SO(3, R)$ sont soient des groupes cycliques, soient isomorphes à un groupe diédral, soit isomorphes à un des trois groupes d'isométries des solides platoniciens.*

References

[1] Perrin

[2] Combes

[3] Quérré

[4] Lelong-Ferrand Arnaudiès Algèbre