104 GROUPES FINIS. EXEMPLES ET APPLICATIONS.

I. Généralités et outils des groupes finis

[Per96, Ch1, p9–18]

I. A. Vocabulaire des groupes finis

Définition 1. [Groupe, sous-groupe, morphisme, ordre]
- $(G, \times)$ est un groupe si G est un ensemble muni d'une loi de composition interne $\times$ associative, admettant un élément neutre 1 et telle que tout élément admet un élément inversible.
  G est dit commutatif ou abélien si $xy = yx$ pour $x, y \in G$.
  G est dit fini s'il est de cardinal fini.
- $H \subset G$ est un sous-groupe de G s'il est stable pour la loi de G et que c'est un groupe pour la loi induite.
- $\phi : G \longrightarrow G'$ est un morphisme de groupes si G, G' sont des groupes et si $\phi(g_1 g_2) = \phi(g_1)\phi(g_2)$ pour tout $g_1, g_2 \in G$.
- Pour $g \in G$, on appelle ordre d'un élément $g \in G$ le plus petit entier n non nul tel que $g^n = 1$. On le note $o(g)$ et on a $|\langle g \rangle| = o(g)$.

Exemple 2. $\mathbb{Z}/n\mathbb{Z}, \mathfrak{S}_n$ sont des groupes finis. L'ordre de $\overline{1}$ est n, l'ordre de $(a_1\ a_1\ \dots\ a_\ell)$ est ℓ.

Soit $(G, .)$ un groupe fini d'ordre $n \in \mathbb{N}^*$.

Définition 3. [Classes à gauche]
Pour $H < G$, on définit $G/H = \{gH \mid g \in G\}$ l'ensemble des classes à gauche modulo H.
On note $[G : H] = |G/H|$.

Théorème 4. [Théorème de Lagrange]
L'ordre de tout sous-groupe de G divise n. En particulier, l'ordre d'un élément de G divise n.

Exemple 5. Pour $g \in G$, on a $o(g) \mid n$.

Définition 6. [Groupe distingué, groupe quotient, groupe simple]
$H < G$ est dit distingué si pour tout $g \in G$, $gH = Hg$. Dans ce cas, on note alors $H \lhd G$ et on remarque que G/H est muni naturellement d'une structure de groupe.

Exemple 7. Si $[G : H] = 2$, H est distingué dans G.

Définition 8. [Groupe cyclique]
G est dit cyclique si $G = \langle g \rangle$ pour un $g \in G$ (on rappelle que G est fini).

Remarque 9. Un groupe cyclique est abélien.

Exemple 10. Le groupe $\mathbb{U}_n$ des racines n-ièmes de l'unité est cyclique d'ordre n.

Définition 11. [Exposant d'un groupe]
On note $e(G)$ le PPCM des ordres des éléments de G.

Exemple 12. Si G est abélien, il existe $g \in G$ tel que $o(g) = e(G)$.

I. B. Actions de groupes

Définition 13. [Action d'un groupe sur un ensemble, vocabulaire des actions]
On dit que G opère à gauche sur X si on a une application $G \times X \longrightarrow X, (g, x) \longmapsto g.x$ telle que $\forall g, h \in G, \forall x \in X, g.(h.x) = (gh).x$ et $\forall x \in X, 1.x = x$.
Pour $x \in X$, on appelle orbite de x et on note $O(x)$ l'ensemble $G.x = \{g.x \mid x \in X\}$. On note $\mathcal{O}$ l'ensemble des orbites de X. C'est une partition de X.
On appelle stabilisateur de $x \in X$ le groupe $\mathrm{Stab}(x) = \{g \in G \mid g.x = x\}$.
Pour $g \in G$, on note $\mathrm{Fix}(g) = \{x \in X \mid g.x = x\}$.

Exemple 14. G opère sur lui-même par conjugaison : $g.h = ghg^{-1}$. On note $\mathrm{Int}(G) = \{\mathrm{Int}(g), g \in G\}$ l'ensemble des automorphismes intérieurs de G, où $\mathrm{Int}(g) : h \longmapsto ghg^{-1}$.
On remarque alors que G agit sur tout sous-groupe distingué H de G par cette opération.

Dans la suite de cette partie on suppose X fini.

Corollaire 15. [Équation aux classes]
Si $|G| < +\infty$, choisissons pour chaque orbite O un représentant x_O. Alors on a :

$$|X| = \sum_{O \in \mathcal{O}} |O| = \sum_{O \in \mathcal{O}} \frac{|G|}{|\mathrm{Stab}(x_O)|}$$

Application 16. Notons $X^G = \{x \in X \mid \forall g \in G, g.x = x\} = \{x \in X \mid \mathrm{Fix}(x) = G\}$. Alors si G est un groupe d'ordre p^k où p est premier et $k > 1$, on a $\left|X^G\right| \equiv X \mod p$.

Exemple 17. [Action par conjugaison] Si G agit par conjugaison sur lui-même, notons $Z_h(G) = \left\{g \in G \mid ghg^{-1} = h\right\}$. Alors $|G| = |Z(G)| + \sum_{O \in \mathcal{O} \mid |O| \geq 2} \frac{|G|}{|Z_{x_O}(G)|}$.

Application 18. Le centre d'un groupe d'ordre p^k où p est premier et $k \geq 1$ est non trivial.

I. C. Sous-groupes de Sylow

Soit p un nombre premier diviseur de $n \in \mathbb{N}^*$. On notera $n = p^a m$ où $p \nmid m$.

Définition 19. [p-groupe, p-sous-groupe de Sylow]
Si n est une puissance de p ($m = 1$), on dit que G est un p-groupe.
Plus généralement, on appelle p-sous-groupe de Sylow (ou p-Sylow) un sous-groupe de G de cardinal p^a.

Théorème 20. [Théorème de Sylow 1] *Il existe au moins un p-Sylow dans G.*

Corollaire 21. *Il existe au moins un sous-groupe de G d'ordre p^i pour tout $i \in [\![1, a]\!]$.*

Théorème 22. [Théorème de Sylow 2]
(i) Si $H < G$ est un p-groupe, alors il existe un p-Sylow S tel que $H < S$,
(ii) Les p-Sylow de G sont tous conjugués,
(iii) Notons Σ le nombre de p-Sylow de G. Alors $\Sigma \mid m$ et $\Sigma \equiv 1 \mod p$.

Application 23. Un groupe d'ordre 40 a 4 éléments d'ordre 5.

Corollaire 24. *Soit S un p-Sylow de G. Alors $S \lhd G \iff S$ est l'unique p-Sylow de G.*

Application 25. Tout groupe d'ordre 63 ou 255 n'est pas simple.

II. Exemples fondamentaux

Soit $n \in \mathbb{N}^*$ et p un entier premier.

II. A. Le groupe $\mathbb{Z}/n\mathbb{Z}$ [Rom17, §1.4, p14–15]

Définition 26. [Le groupe $\mathbb{Z}/n\mathbb{Z}$]
En remarquant que $n\mathbb{Z}$ est distingué dans $\mathbb{Z}$, on définit le groupe quotient $\mathbb{Z}/n\mathbb{Z}$.

Proposition 27. *$\mathbb{Z}/n\mathbb{Z}$ est cyclique, de générateurs les $\overline{d}$ tels que $d \wedge n = 1$.*

Proposition 28. *Tout groupe cyclique d'ordre n est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.*

Exemple 29. Un groupe de cardinal p est isomorphe à $\mathbb{Z}/p\mathbb{Z}$.

Proposition 30. *[Per96, §1.7, p24] On a $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$. En particulier, $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ est abélien de cardinal $\varphi(n)$.*
De plus, $\mathrm{Aut}(\mathbb{Z}/p\mathbb{Z}) \simeq (\mathbb{Z}/p\mathbb{Z})^\times \simeq (\mathbb{Z}/(p-1)\mathbb{Z})$.

II. B. Le groupe $\mathfrak{S}_n$ [Rom17, Ch2, p39]

Définition 31. [Groupe symétrique $\mathfrak{S}_n$]
On note $\mathfrak{S}_n$ le groupe des permutations de $[\![1, n]\!]$.

Théorème 32. [Théorème de Cayley]
Si G est d'ordre n, il est isomorphe à un sous-groupe de $\mathfrak{S}_n$.

Proposition 33. *Les familles suivantes engendrent $\mathfrak{S}_n$:*
- *les transpositions $((i\,j))_{1 \le i < j \le n}$,*
- *les transpositions $((1\,i))_{2 \le i \le n}$,*
- *les transpositions $((i\,i+1))_{1 \le i \le n-1}$,*
- *la transposition $(1\,2)$ et le cycle $(1\,2\,\ldots\,n)$.*

Proposition 34. *Toute permutation σ de $\mathfrak{S}_n$ se décompose en un produit de cycles à supports disjoints. Ce produit est unique à l'ordre des cycles près. En particulier, la suite $(\ell_1, \ell_2, \ldots, \ell_m)$ des longueurs des cycles est unique si on impose $\ell_1 \ge \ell_2 \ge \cdots \ge \ell_m$. On appelle cette suite le type de σ.*

Proposition 35. [Classes de conjugaisons de $\mathfrak{S}_n$]
Deux permutations de $\mathfrak{S}_n$ sont conjuguées si et seulement si elles ont même type.

Proposition 36. *Il existe deux morphismes de $\mathfrak{S}_n$ dans $\mathbb{C}^*$: l'identité et le morphisme $\mathcal{E}$ qui envoie toute transposition sur -1.*

Définition 37. On appelle $\mathcal{E}$ l'application signature. On définit le groupe alterné $\mathfrak{A}_n$ comme étant le noyau de $\mathcal{E}$.

Proposition 38. *Pour $n \ge 5$, $\mathfrak{A}_n$ est simple.*

Corollaire 39. *Pour $n \ge 5$, les seuls sous-groupes distingués de $\mathfrak{S}_n$ sont $\{\mathrm{Id}\}$, $\mathfrak{A}_n$ et $\mathfrak{S}_n$.*

III. Applications

III. A. Constructions de groupes finis

[Per96, §1.6, p20]

Idée : à partir des groupes que nous connaissons, créer des groupes finis « plus complexes ».

Définition 40. [Produit direct]
- Soit G un groupe et $N, H < G$ tels que N, H commutent, $N \cap H = \{1\}$ et $G = NH$. Alors on dit que G est le produit direct de N par H.
- Soit N et H des groupes. Le produit direct de N et H est le produit cartésien $G = N \times H$, muni de la loi $(n, h).(n', h') = (nn', hh')$.

Lemme 41. [Lemme chinois]
$\mathbb{Z}/mn\mathbb{Z} \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ si et seulement si $m \wedge n = 1$.

Définition 42. [Produit semi-direct]
- Soit G un groupe, $N \lhd G$ et $H < G$ tel que $N \cap H = \{1\}$ et $G = NH$. Alors on dit que G est le produit semi-direct de N par H.
- Soit N et H des groupes et $\phi : H \longrightarrow \mathrm{Aut}(N)$. On définit le produit $(n, h).(n', h') = (n\phi(h)(n'), hh')$ sur $G = N \times H$. $(G, .)$ est alors une groupe appelé produit semi-direct de N par H. On note $G = N \rtimes_\phi H$.

Exemple 43. $\mathfrak{S}_n = \mathfrak{A}_n \rtimes \mathbb{Z}/2\mathbb{Z}$ et le produit n'est pas direct.

Exemple 44. Contre-exemple : $\mathbb{Z}/8\mathbb{Z}$ et le groupe des quaternions $\mathbb{H}_8$ ne peuvent être écrits comme un produit semi-direct non trivial.

III. B. Le groupe diédral

[Aud06, Ch3/5, p360] [Rom17, §3.4.3/6.1, p87/180]

Exemple 45. Isométries du plan conservant un segment $[A, B]$ de centre O :
Id l'identité,
ρ la rotation d'angle π et de centre O,
s la symétrie d'axe (AB),
$s\rho$ la symétrie d'axe la droite orthogonale à (AB) passant par O.
On vérifie que ces isométries forment un groupe isomorphe au groupe de Klein $(\mathbb{Z}/2\mathbb{Z})^2$.

Définition 46. [Déplacement, antidéplacement]
Un déplacement (resp. antidéplacement) est un isomorphisme dont la partie linéaire est de déterminant 1 (resp. -1).

Soit G groupe fini d'isométries. On note G^+ ses déplacements et G^- ses antidéplacements.

Proposition 47.
- *Il existe un point fixe à toutes les isométries de G,*
- *G^+ est cyclique, engendré par une rotation ρ.*
- *Si G contient un antidéplacement σ, alors $[G : G^+] = 2$ et $G^- = \sigma G^+$. σ est une réflexion dont l'axe contient le centre de ρ. On a $G = \langle \sigma, \rho \rangle$.*

Exemple 48. Le groupe des isométries du plan préservant un polygône régulier à n côtés de centre O contient : contient les rotations d'ordre n autour du centre et les n réflexions par rapport aux droites joignant :
i) n rotations de centre O et d'angle $\frac{k2\pi}{n}$ pour $k \in [\![0, n-1]\!]$,
ii) n symétries d'axe 2 sommets ou 2 milieux de côtés opposés si n est pair, 1 sommet et le milieu du côté opposé si n est impair.
C'est le groupe diédral D_{2n}.

III. C. Classifications

[Szp09, §6.VI/6.VII, p254/276-278]

Idée : on se donne un groupe fini. Peut-on le décomposer en produits de groupes « faciles » déjà construits ?

Exemple 49. Pour p premier, un groupe d'ordre p^2 est isomorphe à $\mathbb{Z}/p^2\mathbb{Z}$ ou à $(\mathbb{Z}/p\mathbb{Z})^2$.

Proposition 50. *On a équivalence :*
- *tous les sous-groupes de Sylow de G sont distingués,*
- *G est le produit direct de ses sous-groupes de Sylow.*

Proposition 51. *Soit G de cardinal pq où $p < q$ sont premiers.* [Per96, §1.7, p27-28]
- *si $p \nmid q - 1$, $G \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$,*
- *si $p \mid q - 1$, $G \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$ ou $G \simeq \mathbb{Z}/q\mathbb{Z} \rtimes_\phi \mathbb{Z}/p\mathbb{Z}$, où ϕ est une action non triviale de $\mathbb{Z}/p\mathbb{Z}$ sur $\mathbb{Z}/q\mathbb{Z}$.*

Théorème 52. [Structure des groupes abéliens] [Rom17, §1.9, p30]
Supposons G abélien fini d'ordre n. Alors il existe un unique entier ℓ et une unique suite $d_1 \geq d_2 \geq \cdots \geq d_\ell$ d'entiers supérieurs à 2 tels que $d_{i+1} \mid d_i$ pour tout $i \leq \ell - 1$ et

$$G \simeq \prod_{i=1}^{\ell} \mathbb{Z}/d_i\mathbb{Z}$$

Exemple 53. Structures possibles d'un groupe abélien de cardinal 120 ou 600.

Application 54. En utilisant les propriétés vues dans cette leçon, on obtient une classification des groupes de petits ordres. Voir le tableau en annexe.

ANNEXE

Classification des groupes de petits ordres :

n	Groupes de cardinal n (à isomorphisme près)
1	$\{1\}$
2	$\mathbb{Z}/2\mathbb{Z}$
3	$\mathbb{Z}/3\mathbb{Z}$
4	$\mathbb{Z}/4\mathbb{Z}$, $(\mathbb{Z}/2\mathbb{Z})^2$
5	$\mathbb{Z}/5\mathbb{Z}$
6	$\mathbb{Z}/6\mathbb{Z}$, D_6
7	$\mathbb{Z}/7\mathbb{Z}$
8	$\mathbb{Z}/8\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, $(\mathbb{Z}/2\mathbb{Z})^3$, D_8, $\mathbb{H}_8$
9	$\mathbb{Z}/9\mathbb{Z}$, $(\mathbb{Z}/3\mathbb{Z})^2$
10	$\mathbb{Z}/10\mathbb{Z}$, D_{12}
11	$\mathbb{Z}/11\mathbb{Z}$
$\vdots$	
15	$\mathbb{Z}/15\mathbb{Z}$
21	$\mathbb{Z}/21\mathbb{Z}$, $\mathbb{Z}/7\mathbb{Z} \rtimes \mathbb{Z}/3\mathbb{Z}$
25	$\mathbb{Z}/25\mathbb{Z}$, $(\mathbb{Z}/5\mathbb{Z})^2$
35	$\mathbb{Z}/35\mathbb{Z}$
36	$\mathbb{Z}/36\mathbb{Z}$, $(\mathbb{Z}/6\mathbb{Z})^2$
39	$\mathbb{Z}/39\mathbb{Z}$, $\mathbb{Z}/13\mathbb{Z} \rtimes \mathbb{Z}/3\mathbb{Z}$
49	$\mathbb{Z}/49\mathbb{Z}$, $(\mathbb{Z}/7\mathbb{Z})^2$
51	$\mathbb{Z}/51\mathbb{Z}$
120	$\mathbb{Z}/120\mathbb{Z}$, $\mathbb{Z}/60\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/30\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})^2$

Quelques treillis de groupes

SPEECH

La notion de groupe est historiquement fondamentale (géométrie, étude des racines des polynômes, …). Pédagogiquement, c'est la première structure algébrique qui apporte une richesse mathématique. Dans cette leçon, on essaye de construire des groupes de petits cardinaux.
Tout d'abord, quelques rappels de vocabulaire et le théorème de Lagrange qui est un résultat fondamental. Puis on introduit les actions de groupes qui sont des outils importants en théorie des groupes, et mènent notamment à l'équation aux classes. La théorie de Sylow, l'étude des p-groupes, a aussi un rôle majeur, car elle permet de donner des informations sur un groupe à partir de son cardinal. Le premier théorème de Sylow sera proposé en développement.
Ensuite, on s'intéresse à deux exemples fondamentaux : $\mathbb{Z}/n\mathbb{Z}$, avec notamment un isomorphisme classique avec les groupes cycliques, et $\mathfrak{S}_n$, dont l'intérêt de l'étude est appuyé par le théorème de Cayley. La simplicité de $\mathfrak{A}_n$ pour $n \geq 5$ sera proposée en développement.
Enfin, dans la dernière partie, on regarde comment créer de nouveaux groupes à partir de groupes simples connus, notamment via les produits (semi)-directs. Le produit semi-direct nous permet notamment de parler de groupe diédral. Puis inversement on s'intéresse à la classification des groupes de petits cardinaux.

COMMENTAIRES

Autres références possibles : [Ale99, Com98, Dem09]

QUESTIONS

Q Un groupe d'ordre 12 ou 30 est-il simple ?

R Pour $n = 12$, on a nécessairement 1 ou 4 3-Sylow. S'il y en a 1, le groupe n'est pas simple. Sinon, il y a 8 éléments d'ordre 3 car les 3-Sylow sont d'intersections $\{1\}$, donc il y a un seul 2-Sylowqui contient les 3 éléments restants et 1. Donc le groupe n'est pas simple non plus. Pour $n = 30$, c'est similaire.

Q Énumérer les groupes de cardinal 12. Y en a-t-il des non commutatifs ?

R Il y a 5 groupes de cardinal 12 (à isomorphisme près). 2 sont abéliens, les autres, comme le groupe diédral D_{12}, ne le sont pas.

Q Soit H non distingué. Peut-on munir G/H d'une structure de groupe ?

Q Tous les sous-groupes de $\mathbb{Z}$ sont distingués, est-ce normal ?

R Oui car $\mathbb{Z}$ est abélien.

Q Un groupe dont tous les sous-groupes sont distingués est-il abélien ?

R Par forcément : prendre l'exemple de $\mathbb{H}_8$!

Q Donner les groupes abéliens de cardinal 120, à isomorphisme près.

Q Soit $H \lhd G$, $S \lhd H$ un p-Sylow de H. Montrer que $S \lhd G$.

Q Pourquoi les groupes suivant sont-ils différents : $\mathbb{Z}/n\mathbb{Z}$, $\mathfrak{S}_n$, D_n, $\mathcal{GL}_n(\mathbb{K})$?

Q Soit A est un anneau intègre et G un sous-groupe fini de $A^\times$. Montrer que G est cyclique.

BIBLIOGRAPHIE

[Ale99] M. Alessandri : *Thèmes de géométrie*. Dunod, 1999.

[Aud06] M. Audin : *Géométrie*. EDP Sciences, 2006.

[Com98] F. Combes : *Algèbre et géométrie*. Bréal, 1998.

[Dem09] M. Demasure : *Cours d'algèbre*. Cassini, 2009.

[Per96] D. Perrin : *Cours d'algèbre*. Ellipses, 1996.

[Rom17] J.-E. Rombaldi : *Mathématiques pour l'agrégation : Algèbre et géométrie*. De Boeck, 2017.

[Szp09] A. Szpriglas : *Algèbre L3*. Pearson Education, 2ème édition, 2009.