Groupes finis remarquables

Dans cette feuille, on s'intéresse à des familles de groupes finis usuels.

1 Groupes cycliques et racines de l'unité

Lemme 1.1. *Soit $n \in \mathbb{N}^*$. Alors*

$$n = \sum_{d|n} \varphi(d)$$

où $\varphi(d)$ est l'indicatrice d'Euler de d.

Démonstration. Pour tout diviseur d de n, $\mathbb{Z}/n\mathbb{Z}$ admet un unique sous-groupe d'ordre d. En effet, ses sous-groupes correspondent aux sous-groupes de $\mathbb{Z}$ contenant $n\mathbb{Z}$, et le seul tel sous-groupe H de $\mathbb{Z}$ tel que $H/n\mathbb{Z}$ soit d'ordre d est $(n/d)\mathbb{Z}$.

Il y a donc exactement $\varphi(d)$ éléments d'ordre d dans $\mathbb{Z}/n\mathbb{Z}$ puisque ceux-ci engendrent le même sous-groupe d'ordre d. En partitionnant $\mathbb{Z}/n\mathbb{Z}$ selon les ordres de ses éléments, on obtient le résultat. □

Théorème 1.2. *Soit G un groupe fini d'ordre n. Alors G est cyclique si et seulement si pour tout diviseur d de n, G admet au plus un sous-groupe d'ordre d.*

Démonstration. On a déjà fait l'implication directe ci-dessus.

Réciproquement, soit G un groupe d'ordre n tel que pour tout diviseur d de n, G admet au plus un sous-groupe d'ordre d. Si d est un diviseur de n, notons $N(d)$ le nombre d'éléments de G d'ordre d. Si $N(d) \neq 0$, alors $N(d) = \varphi(d)$. En effet, un élément d'ordre d engendre un sous-groupe d'ordre d de G, qui est cyclique, donc admet $\varphi(d)$ générateurs, et ces $\varphi(d)$ générateurs sont exactement les éléments d'ordre d puisque le sous-groupe en question est unique. On a donc

$$n = \sum_{d|n} N(d) \leq \sum_{d|n} \varphi(d) = n,$$

d'où $N(d) = \varphi(d)$ pour tout $d \mid n$. En particulier, $N(n) = \varphi(n) > 0$. □

Corollaire 1.3. *Soit K un corps et G un sous-groupe fini de $K^\times$. Alors G est cyclique.*

Démonstration. D'après le théorème de Lagrange, tout élément x de G vérifie $x^{|G|} = 1$. Pour tout diviseur d de $|G|$, il y a au plus d racines dans K du polynôme $X^d - 1$ (division euclidienne), puisque K est un corps. Ainsi, s'il existe un sous-groupe de G d'ordre d, celui-ci est unique, ses éléments étant précisément les racines de $X^d - 1$. □

Remarque 1.4. La commutativité du corps est essentielle ci-dessus. Par exemple, le groupe non abélien $\mathbb{H}_8$ est un sous-groupe fini du groupe des inversibles de l'algèbre des quaternions.

Proposition 1.5. *Soit $n \geq 1$. L'ensemble $\mathbb{U}_n$ des racines n-ièmes de l'unité dans $\mathbb{C}$ est cyclique d'ordre n. Ses éléments sont les $e^{\frac{2i\pi k}{n}}$ avec $0 \leq k \leq n-1$.*

⚠ Même dans un corps algébriquement clos, les racines n-ièmes de l'unité ne sont pas nécessairement au nombre de n.

2 Groupes abéliens finis

Définition 2.1. *Soit G un groupe dont tous les éléments sont d'ordre fini (par exemple un groupe fini). L'**exposant** de G est le PPCM des ordres des éléments de G.*

Exemple 2.2.

1. Pour tout $n \in \mathbb{N}^*$, l'exposant de $\mathbb{Z}/n\mathbb{Z}$ est n.
2. L'exposant de $\mathfrak{S}_5$ est 30.
3. L'exposant de $\mathbb{U}$, le groupe des racines de l'unité dans $\mathbb{C}$, est infini.

Théorème 2.3 (de structure des groupes abéliens finis)**.** *Soit G un groupe abélien fini. Il existe une unique famille $(d_1, \ldots, d_r) \in \mathbb{N}^r$ telle que $d_1 \mid d_2 \mid \cdots \mid d_r$ et*

$$G \simeq \mathbb{Z}/d_1\mathbb{Z} \times \ldots \mathbb{Z}/d_r\mathbb{Z}.$$

Remarque 2.4.

1. Plus généralement, le théorème de structure des groupes abéliens de type fini dit qu'un tel groupe a la forme ci-dessus, avec éventuellement un facteur $\mathbb{Z}^r$, où $r \in \mathbb{N}$, supplémentaire. L'entier r est alors appelé le rang du groupe.
2. Ce résultat peut être démontré à l'aide du **théorème de structure des modules de type fini sur les anneaux principaux** (qui dépasse le cadre du programme mais qu'il est bon de connaître) car les groupes abéliens sont exactement les $\mathbb{Z}$-modules. De la même manière, la décomposition de Frobenius d'un endomorphisme en est également une application, car un tel endomorphisme fait de son espace vectoriel un $K[X]$-module de type fini.
3. À cause des relations de divisibilité, il est clair que d_r est l'exposant de G. Pour démarrer la démonstration, on va donc établir qu'il existe un élément qui a pour ordre l'exposant du groupe.

Lemme 2.5. *Soit G un groupe abélien fini d'exposant N. Alors il existe $g \in G$ d'ordre N.*

Démonstration. Il suffit de montrer que si m et n sont premiers entre eux et $x, y \in G$ sont d'ordres m et n respectivement, alors G admet un élément d'ordre mn. En effet, si p^r est la puissance exacte du nombre premier p divisant N, alors il existe un élément $g \in G$ d'ordre un entier d divisible exactement par p^r. Alors g^{d/p^r} est d'ordre p^r et la propriété du début permet de construire un élément d'ordre N par récurrence sur le nombre de facteurs premiers de N.

Soit donc $x, y \in G$ d'ordres m et n respectivement, avec m et n premiers entre eux. Alors xy est d'ordre mn. En effet, puisque m et n sont premiers entre eux, on a $\langle x\rangle \cap \langle y\rangle = \{e\}$ d'après le théorème de Lagrange. Si $(xy)^k = x^k y^k = e$ pour un certain $k \in \mathbb{Z}$ alors on a $x^k = y^{-k} \in \langle x\rangle \cap \langle y\rangle$ donc $x^k = y^k = e$. Par définition, cela veut dire que $m \mid k$ et $n \mid k$. Comme m et n sont premiers entre eux, le lemme de Gauss montre que $mn \mid k$. Réciproquement, $(xy)^{mn} = x^{mn} y^{mn} = e$, donc xy est bien d'ordre mn. □

Pour poursuivre la démonstration, nous utiliserons la notion de dual d'un groupe abélien.

Définition 2.6. *Soit G un groupe abélien. Le **dual** de G est*

$$\hat{G} = \{\chi : G \to \mathbb{C}^\times \text{ morphisme de groupes}\}.$$

Lemme 2.7. *Soit G un groupe abélien fini et H un sous-groupe de G. Alors tout morphisme de groupes $\chi : H \to \mathbb{C}^\times$ s'étend en un morphisme de groupes $\tilde{\chi} : G \to \mathbb{C}^\times$. Autrement dit, le morphisme de restriction $\hat{G} \to \hat{H}$ est surjectif.*

Démonstration. Montrons le résultat par récurrence sur l'indice $[G : H]$. Si $[G : H] = 1$ il n'y a rien à montrer. Supposons le résultat quand l'indice est inférieur ou égal à n et supposons $[G : H] = n + 1 > 1$. Soit $\chi \in \hat{H}, g \in G \setminus H$ tel que $\overline{g}$ soit d'ordre d dans G/H et notons $\tilde{H} = \langle H, g\rangle$. Remarquons que, puisque G est abélien, tout élément de $\tilde{H}$ s'écrit (de manière non unique en général) sous la forme hg^k avec $h \in H$ et $0 \le k < d$. On définit $\tilde{\chi} \in \hat{\tilde{H}}$ de la manière suivante : pour tout $h \in H$ et $k \in \mathbb{Z}$,

$$\tilde{\chi}(hg^k) = \chi(h)\omega^k,$$

où ω est une racine d-ième de l'unité dans $\mathbb{C}$. On vérifie que cette définition ne dépend pas du choix d'écriture hg^k et que $\tilde{\chi}$ est bien un morphisme de groupes. Par hypothèse de récurrence, puisque $[G : \tilde{H}] < [G : H] = n + 1$, on peut étendre $\tilde{\chi}$ en un élément de $\hat{G}$. □

Démonstration du théorème de structure des groupes abéliens finis. Nous allons faire une récurrence sur l'ordre du groupe. Si $|G| = 1$ il n'y a rien à prouver. Supposons le résultat pour des groupes abéliens finis d'ordres strictement inférieurs à $|G|$ et que G est d'exposant $N > 1$. D'après le Lemme 2.5, soit $g \in G$ d'ordre N et notons $H = \langle g\rangle$. Soit $\chi \in \hat{H}$ défini par $\chi(g^k) = e^{\frac{2ik\pi}{N}}$. Il est clair que χ est un isomorphisme entre H et $\mathbb{U}_N$. D'après le Lemme 2.7, on peut étendre χ en un caractère $\tilde{\chi} \in \hat{G}$. Alors on a $G \simeq \ker\tilde{\chi} \times \langle g\rangle$. En effet, puisque G est d'exposant N, on a $x^N = e$ pour tout élément $x \in G$ et donc $\tilde{\chi}(x)^N = 1$, autrement dit, $\tilde{\chi}$ est à valeurs dans $\mathbb{U}_N = \chi(H)$. Maintenant, si $x \in G$, alors il existe un unique $k \in \{0, \ldots, N-1\}$ tel que $\tilde{\chi}(x) = \chi(g^k)$ et donc $xg^{-k} \in \ker\tilde{\chi}$. Comme G est abélien, les sous-groupes H et $\ker\tilde{\chi}$ satisfont bien les propriétés caractérisant un produit direct interne.

Finalement, il est clair que $H \simeq \mathbb{Z}/N\mathbb{Z}$, et l'hypothèse de récurrence appliquée à $\ker\tilde{\chi}$ donne l'existence. Les relations divisibilité viennent du fait que l'exposant de $\ker\tilde{\chi}$ divise l'exposant de G qui est N.

L'unicité est fastidieuse (et peu intéressante). □

Corollaire 2.8. *Soit G un groupe abélien fini d'ordre n et d un diviseur de n. Alors G admet un sous-groupe d'ordre d.*

Démonstration. D'après le théorème de structure des groupes abéliens finis, il existe des entiers $d_1, \ldots, d_r$ tels que $d_1 \mid \cdots \mid d_r$ et

$$G \simeq \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_r\mathbb{Z}.$$

En particulier,

$$n = \prod_{i=1}^{r} d_i.$$

Notons

$$n = \prod_{i=1}^{s} p_i^{\alpha_i}$$

la décomposition en facteurs premiers de n. Puisque d est un diviseur de n, ses facteurs premiers sont parmi $p_1, \ldots, p_s$ et pour $1 \le i \le s$, $\beta_i = v_{p_i}(d) \le v_{p_i}(n) = \alpha_i$. Pour $1 \le i \le s$, on a $v_{p_i}(n) = \sum_{j=1}^{r} v_{p_i}(d_j)$ et donc il existe $j_i \in \{1, \ldots, r\}$ maximal tel que $v_{p_i}(d) \le \sum_{j=1}^{j_i} v_{p_i}(d_j)$. Si on note $k_i = \sum_{j=1}^{j_i} v_{p_i}(d_j) - \beta_i$, alors $\mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_{j_i}\mathbb{Z}$ contient un sous-groupe H_i d'ordre $p_i^{\beta_i}$, de la forme $\mathbb{Z}/p_i^{v_{p_i}(d_1)}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_i^{v_{p_i}(d_{j_i}-1)} \times \mathbb{Z}/p_i^{v_{p_i}(d_{j_i})-k_i}\mathbb{Z}$. Finalement, puisque G est abélien, la caractérisation des produits directs internes donne que G contient un sous-groupe isomorphe à $\prod_{i=1}^{s} H_i$, d'ordre d. □

3 Groupes diédraux

Définition 3.1. *Soit $n \geq 2$. Le **groupe diédral** $\mathcal{D}_n$ d'indice n est le groupe des isométries préservant un polygone régulier à n côtés.*

Proposition 3.2. *Pour tout $n \geq 2$, $\mathcal{D}_n$ est un groupe d'ordre $2n$, isomorphe au groupe engendré par la matrice de rotation*

$$R = \begin{pmatrix} \cos\left(\frac{2\pi}{n}\right) & -\sin\left(\frac{2\pi}{n}\right) \\ \sin\left(\frac{2\pi}{n}\right) & \cos\left(\frac{2\pi}{n}\right) \end{pmatrix}$$

et la matrice de symétrie

$$S = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

On a $\mathcal{D}_2 \simeq (\mathbb{Z}/2\mathbb{Z})^2$ et pour $n \geq 3$, $\mathcal{D}_n$ est non abélien.

Démonstration. Un peu de géométrie ne fait jamais de mal : Les sommets du polygone sont ses points extrémaux (milieux d'aucune paire de points). Une injection affine préservant les points extrémaux, les éléments de $\mathcal{D}_n$ permutent les n sommets du polygone. Quitte à conjuguer par une translation, on peut supposer que le polygone est centré en 0. Ce centre étant l'isobarycentre des sommets du polygone, celui-ci est laissé fixe par les éléments de $\mathcal{D}_n$, et on peut donc les voir comme des applications linéaires. Appelons $A_0, \dots, A_{n-1}$ les n sommets du polygone dans l'ordre. Les vecteurs $\overrightarrow{OA_0}$ et $\overrightarrow{OA_1}$ formant une base de $\mathbb{R}^2$, on en déduit qu'un élément de $\mathcal{D}_n$ est entièrement déterminé par les images de A_0 et A_1. Maintenant, comme les isométries préservent les distances, les éléments de $\mathcal{D}_n$ envoient deux sommets successifs sur deux sommets successifs, et il y a donc au plus $2n$ éléments dans $\mathcal{D}_n$, envoyant (A_0, A_1) sur (A_i, A_{i+1}) pour $1 \leq i \leq n$, et (A_0, A_1) sur (A_i, A_{i-1}). Finalement, il y en a exactement $2n$ puisque R^i et R^iS répondent au cahier des charge. On obtient alors l'isomorphisme voulu, et le fait que $\mathcal{D}_n$ est engendré par R et S. Enfin, pour $n = 2$, $RS = SR^{-1} = SR$ donc R et S commutent, et S, R et RS sont d'ordre 2, d'où $\mathcal{D}_2 \simeq (\mathbb{Z}/2\mathbb{Z})^2$. Pour $n \geq 3$, $RS = SR^{-1} \neq SR$ et donc $\mathcal{D}_n$ est non abélien. □

Exercice 1. *Montrer que $\mathcal{D}_3 \simeq \mathfrak{S}_3$.*

4 Exercices

Exercice 2. *Déterminer tous les groupes abéliens d'ordre 720.*

Exercice 3. *Combien existe-t-il de groupes abéliens d'ordre p^n, où p est un nombre premier et $n \in \mathbb{N}^*$? En déduire une formule pour le nombre de groupes abéliens d'ordre $n \in \mathbb{N}^*$.*

Exercice 4.

1. *Soit $n \in \mathbb{N}^*$. Montrer que $\widehat{\mathbb{Z}/n\mathbb{Z}} \simeq \mathbb{Z}/n\mathbb{Z}$.*
2. *Soit G et H des groupes abéliens. Montrer quue $\widehat{G \times H} \simeq \hat{G} \times \hat{H}$.*
3. *Soit G un groupe abélien fini. Montrer que $G \simeq \hat{G}$.*

4. *Montrer également que* $\hat{\hat{G}} \simeq G$ *sans passer par un isomorphisme* $G \simeq \hat{G}$*. (Indication : S'inspirer de la dualité des espaces vectoriels de dimension finie.)*

Exercice 5. *Est-ce que le groupe* $\mathbb{U}$ *des racines de l'unité dans* $\mathbb{C}$ *est égal au cercle unité* $\mathbb{S}^1$ *? Montrer que* $\mathbb{S}^1 \simeq \mathbb{R}/\mathbb{Z}$*. Donner une description similaire de* $\mathbb{U}$*.*

Exercice 6. *Montrer que* $\mathcal{D}_4$ *et* $\mathbb{H}_8$ *sont des groupes non abéliens d'ordre* 8 *non isomorphes et que ce sont les seuls groupes non abéliens d'ordre* 8*.*

Exercice 7. *Pour* $n \geq 3$*, déterminer* $Z(\mathcal{D}_n), D(\mathcal{D}_n)$ *et les classes de conjugaison de* $\mathcal{D}_n$*.*

Exercice 8. *Pour tout* $n \geq 2$*, montrer que* $\mathcal{D}_n \simeq \mathbb{Z}/n\mathbb{Z} \rtimes_\varphi \mathbb{Z}/2\mathbb{Z}$ *pour un morphisme* $\varphi : \mathbb{Z}/2\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ *à déterminer.*

Exercice 9. *Soit* p *un nombre premier.*

1. *Donner tous les groupes abéliens d'ordre* p^3*.*
2. *Soit* G *un groupe non abélien d'ordre* p^3*. Montrer que* $Z(G) = D(G) \simeq \mathbb{Z}/p\mathbb{Z}$ *et* $G/D(G) \simeq (\mathbb{Z}/p\mathbb{Z})^2$*.*
3. *On définit*
$$A_p = \left\{ \begin{pmatrix} 1+pm & a \\ 0 & 1 \end{pmatrix} \in \mathcal{M}_2(\mathbb{Z}/p^2\mathbb{Z}) \mid a \in \mathbb{Z}/p^2\mathbb{Z}, m \in \mathbb{Z}/p\mathbb{Z} \right\}$$
et
$$H_p = \left\{ \begin{pmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix} \mid x, y, z \in \mathbb{Z}/p\mathbb{Z} \right\}$$
Montrer que A_p *et* H_p *sont des groupes non abéliens d'ordre* p^3*.*
4. *Soit* $S = \begin{pmatrix} 1+p & 0 \\ 0 & 1 \end{pmatrix}$ *et* $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$*. Calculer* $[S,T]$ *et montrer que* A_p *est engendré par* S *et* T*. Exprimer* A_p *sous forme de produit semi-direct.*
5. *Soit* $A = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ *et* $B = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$*. Calculer* $[A,B]$ *et montrer que* H_p *est engendré par* A *et* B*. Montrer que tout élément non trivial de* H_p *est d'ordre* p*. En déduire que* $H_p \not\simeq A_p$ *quand* $p \neq 2$*.*
6. *Montrer que* $A_2 \simeq H_2 \simeq \mathcal{D}_4$*.*

Remarque. On peut montrer que, pour p premier impair, tout groupe d'ordre p^3 est isomorphe à A_p ou H_p.

Exercice 10. *Soit* p *un nombre premier. Un* p*-**groupe abélien élémentaire** est un groupe abélien fini* G *tel que* $g^p = e$ *pour tout* $g \in G$*.*

1. *Montrer de deux manières différentes qu'un* p*-groupe abélien élémentaire est de la forme* $(\mathbb{Z}/p\mathbb{Z})^n$ *pour un certain entier* $n \in \mathbb{N}$*.*
2. *Soit* G *un* p*-groupe abélien élémentaire. Déterminer* $\mathrm{Aut}(G)$*.*

Exercice 11. *Soit G un groupe fini. On appelle sous-groupe maximal de G tout sous-groupe strict de G, maximal pour l'inclusion, et on note $\Phi(G)$ l'intersection des sous-groupes maximaux de G.*

1. *Déterminer $\Phi(G)$ dans les cas suivants : $G = \mathbb{Z}/n\mathbb{Z}, G = \mathfrak{S}_3, G = \mathbb{H}_8$.*
2. *Montrer que $\Phi(G)$ est un sous-groupe distingué de G.*
3. *Montrer que les éléments de $\Phi(G)$ sont exactement les éléments **superflus** de G, c'est-à-dire les $g \in G$ tels que pour toute partie $S \subset G$, si $\langle S, g\rangle = G$ alors $\langle S\rangle = G$.*
4. *Supposons que G est un p-groupe fini pour un certain nombre premier p. Montrer que chaque sous-groupe maximal de G est distingué dans G. (Indication : Faire agir G, puis un sous-groupe maximal de G, par conjugaison sur l'ensemble des sous-groupes maximaux de G.)*
5. *En déduire que $G/\Phi(G)$ est abélien et conclure que c'est un p-groupe abélien élémentaire.*

Exercice 12. *Soit G un groupe fini résoluble. Montrer qu'il existe une famille de sous-groupes $(G_i)_{0\leq i\leq r}$ telle que $G_0 = \{e\}, G_r = G$, $G_i \triangleleft G_{i+1}$ et G_{i+1}/G_i est cyclique pour $0 \leq i < r$. On dit qu'un tel groupe est **polycyclique**.*

Exercice 13. *Soit G un groupe fini. On dit qu'il est **nilpotent** lorsque ses sous-groupes de Sylow sont distingués dans G.*

1. *Montrer qu'un groupe abélien est nilpotent et qu'un p-groupe est nilpotent.*
2. *Montrer qu'un groupe nilpotent est produit direct de ses sous-groupes de Sylow.*
3. *En déduire que le centre d'un groupe nilpotent G est non trivial, et que si G est d'ordre n et d est un diviseur de n, alors G admet un sous-groupe d'ordre d.*
4. *Montrer qu'un groupe nilpotent est résoluble. Montrer que la réciproque est fausse.*
5. *Pour quelles valeurs de $n \geq 2$ les groupes $\mathfrak{A}_n, \mathfrak{S}_n, \mathcal{D}_n$ sont-ils nilpotents ? Résolubles ?*

Remarque. La terminologie vient du fait que si N est un sous-anneau nilpotent d'un anneau unitaire A, alors $1 + N$ est un groupe multiplicatif nilpotent. Ainsi, le groupe des matrices unipotentes (triangulaires supérieures avec des 1 sur la diagonale) de taille $n \times n$ sur un anneau unitaire quelconque est nilpotent.

Exercice 14 (Le boss final)**.** *Classifier tous les groupes d'ordre au plus* 15.

Ordre du groupe	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Nombre de groupes	1	1	1	2	1	2	1	5	2	1	1	5	1	2	1

Remarque. Il y a 14 groupes d'ordre 16, dont des horreurs du style $\langle a, x, y \mid a^4 = y^4 = x^2 = e, a^2 = y^2, xax = a^{-1}, ay = ya, xy = yx\rangle$ qui ne peut s'écrire comme un produit semi-direct, on ne s'amusera donc pas à les classifier.