Chapitre 6

# Éléments de structure des groupes finis

Dans ce chapitre, on se propose de démontrer quelques uns des résultats emblématiques de la théorie élémentaire des groupes finis : les théorèmes de Sylow, de Schur-Zassenhaus et de P. Hall. Dans chacun des cas, il s'agit de formes de réciproques au théorème de Lagrange.

Nous commençons par donner quelques propriétés des $p$-groupes, c'est-à-dire des groupes d'ordre une puissance du nombre premier $p$. Les $p$-groupes abondent par le premier théorème de Sylow que l'on a déjà vu. Leur propriété la plus importante est que toute action d'un $p$-groupe sur un ensemble fini de cardinal premier à $p$ admet un point fixe. Contrairement aux groupes simples finis, les $p$-groupes ne sont pas raisonnablement classifiables, mais cela ne les empêche pas de jouer un rôle important dans la théorie.

Les théorèmes de Sylow affirment que les $p$-Sylow du groupe fini $G$ sont conjugués et que leur nombre est un diviseur de $|G|$ congru à 1 modulo $p$. L'exemple fondamental est celui de $\mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})$, et par de nombreux aspects on essaiera de montrer que certaines propriétés de cet exemple valent encore en général.

Le théorème de Schur-Zassenhaus affirme que dans un groupe d'ordre $mn$ avec $(m,n) = 1$, tout sous-groupe distingué $N$ de $G$ d'ordre $n$ admet un complément (d'ordre $m$). En particulier, un tel groupe est un produit semi-direct. Bien que simple à formuler, tout le chapitre est orienté vers sa démonstration. On commencera par montrer, à l'aide des théorèmes de Sylow, que le cas particulier $N$ abélien, implique le cas général.

Le théorème de P. Hall affirme que dans un groupe *résoluble* d'ordre $mn$ avec $(m,n) = 1$, il existe un sous-groupe d'ordre $m$. Comme nous le verrons, il se déduit assez simplement du théorème de Schur-Zassenhaus. En fait, Hall a aussi démontré la réciproque : si $G$ est fini et si pour tout diviseur $d$ de $n = |G|$ premier avec $n/d$ il existe un sous-groupe d'ordre $d$, alors $G$ est résoluble. Il faut la théorie des représentations des groupes finis pour comprendre cette réciproque : voir le Complément § 9 Chap. 9.

Dans une dernière partie, nous revenons sur l'étude des *extensions* d'un groupe par un sous-groupe abélien : étant donné un groupe $G$ et un groupe abélien $A$, on cherche à déterminer les groupes $E$ possédant un sous-groupe distingué $A'$ vérifiant $A' \simeq A$ et $E/A' \simeq G$. Autrement dit, on cherche les groupes $E$ qui s'insèrent dans une suite exacte courte de la forme

$$1 \longrightarrow A \longrightarrow E \longrightarrow G \longrightarrow 1.$$

Un cas particulier important est celui où $A'$ est dans le centre de $E$ (extension *centrale*). Il y a beaucoup d'exemples intéressants de telles extensions : par exemple $\mathrm{SL}_n(k)$ est une extension centrale de $\mathrm{PSL}_n(k)$ par $\mu_n(k)$, $\mathrm{Sp}(1)$ en est une de $\mathrm{SO}(3)$ par $\mathbb{Z}/2\mathbb{Z}$, et les groupes $\widetilde{\mathrm{A}_4}, \widetilde{\mathrm{S}_4}$ et $\widetilde{\mathrm{A}_5}$ sont des extensions centrales des groupes des

solides de Platon par $\mathbb{Z}/2\mathbb{Z}$. Le théorème principal est que les extensions de $G$ par un groupe abélien $A$ sont classifiées par un groupe annexe $\mathrm{H}^2(G, A)$ (2-ème groupe de cohomologie de $G$ à valeurs dans $A$). Il devient alors facile de démontrer le cas abélien du théorème de Schur-Zassenhaus.

Enfin, dans un complément, nous discutons de la structure des groupes *nilpotents* finis (une condition plus forte que la résolubilité) et montrons que ce sont exactement les produits directs de $p$-groupes. Nous caractérisons, suivant Burnside, Dickson et Pazderski, les entiers $n \geqslant 1$ tels que tout groupe d'ordre $n$ est cyclique (resp. abélien, resp. nilpotent). Nous étudions enfin le nombre minimal de générateurs d'un $p$-groupe, suivant Frattini et Burnside, ainsi que la structure du groupe des automorphismes d'un $p$-groupe, suivant P. Hall.

## 1. $p$-groupes

Dans toute cette partie $p$ désigne un nombre premier.

Définition 1.1. *Un $p$-groupe est un groupe fini d'ordre $p^n$ avec $n \geqslant 0$.*

Un produit fini de $p$-groupes est un $p$-groupe. Parmi les $p$-groupes rencontrés jusqu'à présent, on a les $\mathbb{Z}/p^n\mathbb{Z}$ avec $n \geqslant 1$, et les 2-groupes non abéliens $\mathrm{D}_8$ et $\mathrm{H}_8$. Les $p$-groupes abondent d'après le premier théorème de Sylow : tout groupe d'ordre $p^n m$ avec $(p, m) = 1$ possède un sous-groupe qui est un $p$-groupe d'ordre $p^n$ (un tel sous-groupe est appelé $p$-Sylow de $G$). Par exemple, $\mathrm{D}_8$ est un 2-Sylow de $\mathrm{S}_4$. L'exemple le plus important de $p$-groupe est peut-être le suivant.

Exemple 1.2. *Le sous-groupe unipotent supérieur*

$$\mathrm{U}_n(\mathbb{Z}/p\mathbb{Z}) \subset \mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})$$

*constitué des matrices triangulaires supérieures $(m_{i,j})$ avec $m_{i,i} = 1$ pour tout $i$ est d'ordre $p^{\frac{n(n-1)}{2}}$. D'après la Proposition 3.15 Chap. 5, $\frac{n(n-1)}{2}$ est aussi la valuation en $p$ de $|\mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})|$, de sorte que $\mathrm{U}_n(\mathbb{Z}/p\mathbb{Z})$ est un $p$-Sylow de $\mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})$.*

Nombreuses propriétés des $p$-groupes se déduisent de la propriété suivante, qui généralise la Propsition 1.9 Chap. 1 (Cas $G = \mathbb{Z}/p\mathbb{Z}$).

Proposition 1.3. *Soit $G$ un $p$-groupe agissant sur un ensemble fini $X$. On note $\mathrm{Fix}\, X = \{x \in X \mid gx = x \ \forall g \in G\}$ l'ensemble des points fixes de $X$ sous l'action de $G$. On a la congruence $|X| \equiv |\mathrm{Fix}\, X| \bmod p$.*

Démonstration — En effet, pour $x \in X$ l'orbite $\mathrm{O}_x$ de $x$ est de cardinal $|G|/|G_x|$, qui est un diviseur de $|G|$. Il y a donc deux cas : soit $|\mathrm{O}_x| = 1$, *i.e.* $x \in \mathrm{Fix}\, X$, soit $|\mathrm{O}_x| \equiv 0 \bmod p$. On conclut par l'équation aux classes. □

Proposition 1.4. *Pour tout $p$-groupe $P \subset \mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})$ il existe $g \in \mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})$ tel que $gPg^{-1}$ est inclus dans $\mathrm{U}_n(\mathbb{Z}/p\mathbb{Z})$.*

Démonstration — Soit $V$ le $\mathbb{Z}/p\mathbb{Z}$-espace vectoriel $(\mathbb{Z}/p\mathbb{Z})^n$. Le groupe $\mathrm{GL}(V) = \mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})$ agit naturellement sur l'ensemble des hyperplans vectoriels de $V$. Il y

a autant d'hyperplans vectoriels que de droites dans l'espace vectoriel dual. Il y a donc

$$\frac{p^n-1}{p-1} = 1 + p + \cdots + p^{n-1}$$

hyperplans. En particulier, leur nombre est premier à $p$. Si $P$ est un $p$-groupe inclus dans $\mathrm{GL}(V)$, il préserve donc un hyperplan. L'image de $P$ dans $\mathrm{GL}(H)$ est encore un $p$-groupe (c'est un quotient de $P$), donc par récurrence sur $\dim V$, il existe un suite croissante $V_i$ de sous-espaces de $V$ avec $\dim V_i = i$ pour $i = 1, \ldots, n-1$, préservée par $P$. Choisissons une base $e_1, \ldots, e_n$ de $V$ telle que $e_1, \ldots, e_i$ engendre $V_i$. Dans cette base, $P$ est constitué de matrices triangulaires supérieures : on a montré qu'il existe $g \in \mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})$ avec $gPg^{-1} \subset \mathrm{T}_n(k)$. On peut donc supposer $P \subset \mathrm{T}_n(k)$. On conclut car le morphisme $P \to ((\mathbb{Z}/p\mathbb{Z})^\times)^n$, $(p_{i,j}) \mapsto (p_{i,i})$ est trivial car $|P|$ et $((\mathbb{Z}/p\mathbb{Z})^\times)^n$ sont d'ordre premiers entre eux, QED. □

COROLLAIRE 1.5. *Tout $p$-groupe fini est isomorphe à un sous-groupe de $\mathrm{U}_n(\mathbb{Z}/p\mathbb{Z})$ pour $n$ assez grand.*

DÉMONSTRATION — En effet, on sait que tout groupe fini $P$ se plonge dans $\mathrm{S}_n$ avec $n = |P|$, qui lui-même se plonge dans $\mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})$ pour tout $p$ (matrices de permutations). On conclut par la proposition ci-dessus. □

Appliquons maintenant la Proposition 1.3 à l'action d'un groupe sur lui-même par conjugaison. On en déduit :

PROPOSITION 1.6. *Si $P$ est un $p$-groupe non trivial, alors son centre $\mathrm{Z}(P)$ est non trivial.*

DÉMONSTRATION — En effet, d'après la Proposition 1.3 on a $|\mathrm{Z}(P)| \equiv |P| \equiv 0 \bmod p$. On en déduit $|\mathrm{Z}(P)| = p^m$ avec $m \geqslant 1$. □

Par exemple, un petit exercice montrerait que le centre de $\mathrm{U}_n(\mathbb{Z}/p\mathbb{Z})$ est d'ordre $p$ (matrices $m$ telles que $m_{i,j} = 0$ pour $(i,j) \neq (1,n)$ et $i \neq j$).

COROLLAIRE 1.7. *Un groupe d'ordre $p^2$ est abélien, donc isomorphe à*

$$(\mathbb{Z}/p\mathbb{Z})^2 \quad \text{ou} \quad \mathbb{Z}/p^2\mathbb{Z}.$$

DÉMONSTRATION — En effet, pour un tel groupe $P$ on a $P/\mathrm{Z}(P)$ d'ordre 1 ou $p$ car $\mathrm{Z}(P) \neq 1$. Dans tous les cas $P/\mathrm{Z}(P)$ est cyclique et donc $P$ est abélien. La dernière assertion s'en déduit soit par la classification des groupes abéliens finis, soit directement en observant que si $P$ n'a pas d'élément d'ordre $p^2$, alors il est abélien $p$-élémentaire par Lagrange. □

REMARQUE 1.8. Il existe des groupes d'ordre $p^3$ non abéliens, comme le $p$-groupe $\mathrm{U}_3(\mathbb{Z}/p\mathbb{Z})$, aussi appelé *groupe de Heisenberg*. En fait, nous verrons en exercice qu'il n'existe à isomorphisme près que deux groupes non abéliens d'ordre $p^3$. Pour $p = 2$, ce sont $\mathrm{H}_8$ et $\mathrm{D}_8 \simeq \mathrm{U}_3(\mathbb{Z}/2\mathbb{Z})$. Pour $p > 2$, $\mathrm{U}_3(\mathbb{Z}/p\mathbb{Z})$ est le seul ayant la propriété que tous ses éléments non triviaux sont d'ordre $p$. L'autre peut être défini par $\mathbb{Z}/p^2\mathbb{Z} \rtimes_\alpha \mathbb{Z}/p\mathbb{Z}$ avec $\alpha_{\overline{k}}(x) = (1+p)^k x$ pour $\overline{k} \in \mathbb{Z}/p\mathbb{Z}$ et $x \in \mathbb{Z}/p^2\mathbb{Z}$. Il s'avère que *classifier* les $p$-groupes n'est pas une question (possédant une réponse) raisonnable. Par exemple,