Chapitre 2

Groupes finis

Dans tout ce chapitre, G désigne un groupe fini.

2.1 Actions de groupes finis

Rappelons que l'on suppose désormais que le groupe G est fini.

2.1.1. Pour tout ensemble fini X, nous noterons $|X|$ le cardinal de X (c'est-à-dire le nombre d'éléments de X). Il est évident que si $\mathcal{P}$ est une partition de X alors $|X| = \sum_{Y\in\mathcal{P}} |Y|$.

2.1.2 Proposition. — *(théorème de Lagrange) Soit H un sous-groupe de G. Alors $|H|$ et $|G/H|$ divisent $|G|$, et $|G| = |H|.|G/H|$.*

Démonstration. — Pour tout $x \in G$ fixé, l'application $h \to xh$ est une bijection de H sur la classe à gauche xH. Donc toutes les classes à gauche modulo H ont même cardinal $|H|$, et elles sont au nombre de $|G/H|$, d'où le résultat d'après 2.1.1.

2.1.3 Corollaire. — *Soit $|G| = p$ premier. Alors G est isomorphe à $\mathbf{Z}/p\mathbf{Z}$ (en particulier, G est commutatif).*

Démonstration. — Soit $x \neq 1$ dans G, et soit $H = \langle x\rangle$ le sous-groupe engendré par x. Alors $|H||G/H| = p$, et comme $|H| > 1$, $|H| = p$, et $H = G$. On a vu en 1.1.8 que $\langle x\rangle$ est toujours un groupe cyclique ; en fait, si $\langle x\rangle$ est fini, comme c'est le cas ici, $\langle x\rangle \simeq \mathbf{Z}/d\mathbf{Z}$, où $d > 0$ est le cardinal de $\langle x\rangle$. Donc on a bien $G = \langle x\rangle \simeq \mathbf{Z}/p\mathbf{Z}$.

2.1.4 Proposition. — *Soit X un G-ensemble fini. Alors*

$$|X| = \sum_{x\dot{\in}X/G} |G|/|G_x| \qquad \textit{(équation des classes)}$$

(ici comme dans la suite on utilisera l'abus d'écriture $\sum_{x\dot{\in}X/G}$ pour indiquer que x parcourt un ensemble de représentants *des orbites de G dans X).*

Démonstration. — Evident : on a vu en 1.6.4 que $Gx \simeq G/G_x$.

2.1.5 Proposition. — *Soit X un G-ensemble fini. Alors :*

$$|X/G| = \frac{1}{|G|} \sum_{g \in G} |X^g|$$

où pour tout $g \in G$ on note $X^g := \{x \in X \mid gx = x\}$ l'ensemble des points fixes de g dans X.

Démonstration. — Soit $Z \subset G \times X$ l'ensemble des couples (g, x) tels que $gx = x$. Nous allons exprimer $|Z|$ de deux manières différentes. D'une part, en projetant sur G :

$$|Z| = \sum_{g \in G} |\{x \in X \mid gx = x\}| = \sum_{g \in G} |X^g|$$

D'autre part, en projetant sur X :

$$|Z| = \sum_{x \in X} |\{g \in G \mid gx = x\}| = \sum_{x \in X} |G_x|$$

Mais si x parcourt une orbite Gx_0, chaque stabilisateur G_x est conjugué à G_{x_0}, donc a même cardinal que G_{x_0}, ce qui donne :

$$\sum_{x \in Gx_0} |G_x| = |Gx_0||G_{x_0}| = |G|$$

et donc $\sum_{x \in X} |G_x| = \sum_{x_0 \in X/G} \left(\sum_{x \in Gx_0} |G_x| \right) = |X/G||G|$, d'où la proposition.

2.2 p-groupes

2.2.1 Définition. — Soit p un nombre premier. On dit que G est un *p-groupe*, si $|G|$ est une puissance de p.

2.2.2 Proposition. — *Soit G un p-groupe. Alors tout sous-groupe et tout quotient de G sont des p-groupes. Le cardinal de tout G-ensemble homogène est une puissance de p.*

Démonstration. — Evident.

2.2.3 Proposition. — *Soit G un p-groupe, soit X un G-ensemble fini, et soit X^G l'ensemble des points fixes de G dans X. Alors*

$$|X| \equiv |X^G| \mod p$$

Démonstration. — On a

$$|X| = \sum_{x \in X/G} |Gx| = |X^G| + \sum_{\substack{x \in X/G \\ G_x \neq G}} |G/G_x|$$

et la dernière somme est divisible par p.

2.2.4 Proposition. — *Soit G un p-groupe, $G \neq \{1\}$. Alors $Z(G) \neq \{1\}$.*

Démonstration. — D'après 2.2.3 appliqué à l'action de G sur lui-même par conjugaison, on a

$$|G| \equiv |Z(G)| \mod p$$

donc p divise $|Z(G)|$, et comme $|Z(G)| > 0$, on a $|Z(G)| \geq p > 1$.

2.2.5 Corollaire. — *Tout p-groupe est nilpotent.*

Démonstration. — Récurrence sur $|G|$. Si $G = \{1\}$, il n'y a rien à démontrer. Sinon, $Z = Z(G) \neq \{1\}$, et G/Z est nilpotent par l'hypothèse de récurrence. Donc G est nilpotent d'après la prop. 1.7.11 *(ii)*.

2.3 Théorèmes de Sylow

2.3.1 Définition. — (sous-groupes de Sylow) Soit $n = |G|$, p un nombre premier, et soit α l'exposant de p dans la décomposition de n en facteurs premiers (on a donc $\alpha = 0$ si p ne divise pas n). On appelle p-sous-groupe de Sylow tout sous-groupe de G de cardinal p^α ; on note $\mathcal{S}_p(G)$ l'ensemble des p-sous-groupes de Sylow de G.

2.3.2 Lemme. — *Soit A un groupe abélien fini, p un diviseur premier de $|A|$. Alors A contient un élément d'ordre p.*

Démonstration. — Cela se déduit facilement du théorème de structure des groupes abéliens finis. Mais on peut aussi faire une démonstration directe par récurrence sur $|A|$. On peut évidemment supposer que $|A| > 1$, sans quoi $|A|$ ne possède aucun diviseur premier. Si $A \simeq \mathbf{Z}/d\mathbf{Z}$ est cyclique, le résultat est immédiat : il suffit de prendre l'image dans A de d/p (noter que p divise d puisque $|\mathbf{Z}/d\mathbf{Z}| = d$.)

On peut donc supposer A non cyclique. Soit $x \neq 1$ dans A, B le sous-groupe de A engendré par x. Alors $B \neq \{1\}$, et $B \neq A$ puisque A n'est pas cyclique. Si p divise $|B|$, B contient un élément d'ordre p (en appliquant l'hypothèse de récurrence, ou en utilisant le cas cyclique), et on a fini. Sinon, p divise $|A/B|$. Par hypothèse de récurrence, il existe alors $x \in A$ tel que $\pi(x)$ soit d'ordre p dans A/B. Mais alors si H est le sous-groupe cyclique de A engendré par x, $\pi(H) \simeq \mathbf{Z}/p\mathbf{Z}$, donc p divise $|H|$ et H contient un élément d'ordre p d'après le cas cyclique.

2.3.3 Théorème. — *(Sylow) Soit p un nombre premier.*

(a) $\mathcal{S}_p(G) \neq \emptyset$.

(b) Tous les p-sous-groupes de Sylow de G sont conjugués dans G, et tout sous-p-groupe de G est contenu dans un p-sous-groupe de Sylow.

(c) $|\mathcal{S}_p(G)| \equiv 1 \mod p$.

Démonstration. — Le cas oú p ne divise pas $|G|$ est trivial ; on suppose donc que p divise $|G|$ (en particulier $|G| > 1$).

(a) On raisonne par récurrence sur $|G|$. S'il existe un sous-groupe strict $H \subset G$ tel que $|G/H|$ soit premier à p, on a $\mathcal{S}_p(H) \subset \mathcal{S}_p(G)$, donc on conclut par hypothèse de

récurrence. Sinon, on conclut que le cardinal de tout G-ensemble homogène fini non-trivial est divisible par p. En particulier, chaque classe de conjugaison non-triviale de G a un cardinal divisible par p, d'où (en notant $\mathrm{Cl}(G)$ l'ensemble des classes de conjugaison de G) :

$$|G| = |Z(G)| + \sum_{x \in \mathrm{Cl}(G)} |G/Z_G(x)| \equiv |Z(G)| \mod p$$

ce qui prouve que p divise $|Z(G)|$, et donc que $Z(G) \neq \{1\}$. D'après 2.3.2, $Z(G)$ contient un sous-groupe N d'ordre p. Soit $G' = G/N$, et soit S' un p-sous-groupe de Sylow de G' ; alors si α est l'exposant de p dans $|G|$, l'exposant de p dans $|G'|$ est $\alpha - 1$, donc $|S'| = p^{\alpha-1}$. Alors si on pose $S = \pi^{-1}(S')$, on a $|S| = p|S'| = p^\alpha$, donc $S \in \mathcal{S}_p(G)$.

(b) Soit H un sous-p-groupe de G, et $S \in \mathcal{S}_p(G)$. Considérons l'action de H sur $G/S = X$. D'après 2.2.3 on a :

$$|X| = |X^H| \mod p$$

Mais $|X|$ est premier à p, donc $|X^H| \neq 0 \mod p$, et *a fortiori* $X^H \neq \emptyset$. Mais alors il existe $x = \pi(g) \in X$ tel que $H \subset G_x$. Clairement, $G_{\pi(1)} = S$; d'après la prop. 1.3.9*(ii)*, on a alors $G_x = gSg^{-1}$, donc H est bien contenu dans un conjugué de S. Si maintenant H est lui-même un p-sous-groupe de Sylow, H et gSg^{-1} ont même cardinal, donc l'inclusion est une égalité, et H est bien conjugué à S.

(c) D'après *(b)*, $X = \mathcal{S}_p(G)$ est un G-ensemble homogène pour l'action de G par conjugaison. Soit $S \in \mathcal{S}_p(G)$, et montrons que $X^S = \{S\}$. En effet, si S' est un point fixe pour l'action de S sur X, en d'autres termes si S normalise S', on a $S \subset N_G(S')$. Mais alors S et S' sont deux p-sous-groupes de Sylow de $N_G(S')$, donc d'après *(b)* appliqué à ce sous-groupe, S et S' sont conjugués *dans* $N_G(S')$. Mais S' est distingué dans $N_G(S')$; donc le seul sous-groupe de $N_G(S')$ conjugué à S' est S' lui-même, d'où $S = S'$ comme annoncé. Comme $|X| = |X^S| \mod p$, on en déduit bien que $|X| \equiv 1 \mod p$.

2.3.4. Les théorèmes de Sylow, que nous avons regroupés ici en un seul énoncé, constituent le premier moyen non-trivial pour analyser la structure des groupes finis. Ils permettent en particulier de classifier à isomorphisme près les groupes de "petit" cardinal.

2.3.5 Exemple. — (groupes à six éléments)On a déjà vu que pour tout nombre premier p, il n'y a à isomorphisme près qu'un seul groupe d'ordre p, à savoir $\mathbf{Z}/p\mathbf{Z}$. De même, les groupes d'ordre p^2 sont nilpotents, et ont donc un centre non trivial (cf. prop. 2.2.4). On en déduit facilement (exercice) qu'un tel groupe est *commutatif* ; alors il est isomorphe soit à $\mathbf{Z}/p^2\mathbf{Z}$, soit à $\mathbf{Z}/p\mathbf{Z} \oplus \mathbf{Z}/p\mathbf{Z}$, et ces deux groupes ne sont pas isomorphes (pourquoi ?) Ainsi, le premier entier pour lequel il peut exister des groupes non-commutatifs est 6. Nous allons montrer qu'à isomorphisme près il existe un unique tel groupe, à savoir $\mathfrak{S}_3$.

En effet, soit G un groupe d'ordre 6. Alors le cardinal de $\mathcal{S}_3(G)$ doit être à la fois un diviseur de $|G|$ (et même de $|G|/3$; pourquoi ?) à cause de l'action transitive de G sur $\mathcal{S}_3(G)$, 2.3.3*(b)*, et congru à 1 modulo 3 d'après 2.3.3*(c)* ; on voit aussitôt que la seule possibilité est $|\mathcal{S}_3(G)| = 1$. En d'autres termes, G possède un unique 3-sous-groupe de Sylow N, nécessairement distingué ; si H est un 2-sous-groupe de Sylow de G, il est clair

que $G = NH$. Donc G est un produit semidirect de $\mathbf{Z}/3\mathbf{Z}$ par $\mathbf{Z}/2\mathbf{Z}$. Si le produit est direct, $G \simeq \mathbf{Z}/3\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z} \simeq \mathbf{Z}/6\mathbf{Z}$. Sinon, le produit semidirect est associé à un homomorphisme non-trivial de $\mathbf{Z}/2\mathbf{Z}$ vers $\mathrm{Aut}\,(\mathbf{Z}/3\mathbf{Z})$. Or, $\mathrm{Aut}\,(\mathbf{Z}/3\mathbf{Z})$ est un groupe à deux éléments (il s'identifie au groupe multiplicatif du corps $\mathbf{F}_3$ à trois éléments), donc il n'y a clairement qu'un et un seul homomorphisme non-trivial $\tau : H \to \mathrm{Aut}\,(N)$, d'où l'unicité de G, et donc $G \simeq \mathfrak{S}_3$ puisque $\mathfrak{S}_3$ est non-commutatif. Si on écrit $N = \{1, x, x^2\}$, $H = \{1, y\}$, avec $x^3 = y^2 = 1$, on voit que $\tau_y(x) = x^{-1}$, *i.e.* $yxy = x^{-1}$. Dans le groupe $\mathfrak{S}_3$, x est réalisé par une permutation cyclique, et y par une transposition.

2.3.6 Exercice. — Analyser de même la structure des groupes d'ordre pq, avec p, q premiers, $p < q$. Donner des exemples de valeurs de p et q pour lesquelles tous les groupes d'ordre pq sont isomorphes à $\mathbf{Z}/pq\mathbf{Z}$.

2.4 Suites de Jordan-Hölder

2.4.1 Définition. — On dit que G est *simple*, si $G \neq \{1\}$, et si G ne posséde aucun sous-groupe distingué non-trivial (*i.e.* distinct de $\{1\}$ et de G lui-même.) Bien entendu, cette définition est valable également pour les groupes infinis.

2.4.2. Le nom de groupes simples n'est pas à prendre au sens de "non compliqués", mais plutôt au sens de "non composés", au sens chimique du terme : les groupes simples jouent un peu le rôle d'"atomes" de la théorie des groupes, alors que les groupes généraux en seraient les molécules. Comme en chimie, il est possible dans certains contextes de classifier entièrement les groupes simples, alors que la classification de tous les groupes est certainement une entreprise sans espoir (les lecteurs non convaincus pourront par exemple s'essayer à la classification des groupes à 16 éléments, tous nilpotents, et si ça ne suffisait pas, 32, 64, ...) C'est ainsi que les groupes simples *finis* ont été entièrement classifiés ; c'est un des monuments des mathématiques du vingtième siècle. Le résultat est que ce sont les groupes cycliques $\mathbf{Z}/p\mathbf{Z}$ pour p premier, les groupes alternés $\mathfrak{A}_n$ pour $n \geq 5$, tout un ensemble de groupes que l'on regroupe sous le terme de groupes *de type de Lie*, ou encore de groupes de Chevalley, et qui sont des sous-groupes des groupes de matrices inversibles sur les corps finis, associés à diverses conditions géométriques (c'est là la vaste majorité des groupes simples), et enfin 26 groupes tout-à-fait inclassables, des "miracles de la nature" comme dit Jacques Tits, appelés pour cette raison *sporadiques*, qui complètent la liste. C'est évidemment un peu plus compliqué que la table de Mendeleïeff, mais c'est tout de même utilisable pour des démonstrations cas par cas si on est courageux.

Si le groupe G n'est pas simple, il possède un sous-groupe distingué non-trivial N. Alors N et G/N sont des groupes de cardinal plus petit que G ; si l'on a en vue la démonstration d'un certain résultat par récurrence sur $|G|$, on peut souvent se ramener au cas de N et G/N. On n'est donc coincé que dans le cas simple, ce qui explique l'importance de ces groupes.

2.4.3 Proposition. — *(i) Les seuls groupes simples* commutatifs *(finis ou non) sont les* $\mathbf{Z}/p\mathbf{Z}$*, p premier.*

(ii) Soit G un groupe simple non commutatif. Alors $Z(G) = \{1\}$, $D(G) = G$.

Démonstration. — *(i)* Tout sous-groupe d'un groupe commutatif est distingué, donc un groupe simple commutatif est nécessairement *monogène* : alors il isomorphe soit à $\mathbf{Z}$, soit à un groupe $\mathbf{Z}/d\mathbf{Z}$, $d > 0$. Clairement, le groupe $\mathbf{Z}$ n'est pas simple (pourquoi ?), et de même, on voit aussitôt que $\mathbf{Z}/d\mathbf{Z}$ ne peut être simple que si (et seulement si) d est premier.

(ii) Exercice.

2.4.4 Exercice. — Soit G un groupe simple, et soit C une classe de conjugaison non-triviale de G. Montrer que C engendre le groupe G.

2.4.5 Définition. — On appelle *suite de composition*, ou *suite de Jordan-Hölder*, de G toute suite finie décroissante $G_0 = G \supset G_1 \supset \ldots \supset G_s = \{1\}$ de sous-groupes de G telle que G_j soit distingué dans G_{j-1}, et que G_{j-1}/G_j soit *simple* pour $1 \leq j \leq s$. On dit que s est la *longueur* de la suite, et que les G_{j-1}/G_j en sont les *sous-quotients*. On remarque que G est trivial si et seulement si il possède une suite de composition de longueur 0, et simple si et seulement si il possède une suite de composition de longueur 1.

2.4.6 Remarque. — Soit N un sous-groupe distingué de G. Alors les sous-groupes de G/N sont en correspondance bijective avec les sous-groupes de G contenant N, *via* l'application $H' \to \pi^{-1}(H')$, d'inverse $H \to H/N$. Il est facile de voir que H' est distingué dans G/N si et seulement si $\pi^{-1}(H')$ est distingué dans G. En particulier, G/N est *simple* si et seulement si N est maximal pour l'inclusion dans l'ensemble des sous-groupes distingués propres de G.

2.4.7 Proposition. — *Supposons $G \neq \{1\}$. Alors G possède des sous-groupes distingués propres maximaux.*

Démonstration. — C'est clair : dans tout ensemble ordonné *fini*, il existe des éléments maximaux.

2.4.8 Corollaire. — *Le groupe G possède des suites de composition.*

Démonstration. — Dans toute suite de composition $G_0 = G \supset G_1 \supset \ldots \supset G_s = \{1\}$ de G, le groupe G_1 est distingué maximal ; inversement, si G_1 est distingué propre maximal dans G toute suite de composition $G_1 \supset G_2 \supset \ldots \supset G_s = \{1\}$ de G_1 définit une suite de composition de G par adjonction de $G_0 = G$ à gauche. Faisons alors une récurrence sur $|G|$: d'aprés la proposition, il existe N distingué propre maximal dans G, et l'on applique l'hypothèse de récurrence à N.

2.4.9 Théorème. — *(Jordan-Hölder) Toutes les suites de composition de G ont même longueur, et les mêmes sous-quotients à isomorphisme près et à l'ordre près. (On pourra remarquer l'analogie avec la décomposition d'un entier en facteurs premiers).*

Démonstration. — Nous nous appuierons sur le lemme suivant :

Lemme. — *Soit $G_0 = G \supset G_1 \supset \ldots \supset G_s = \{1\}$ une suite de composition de G, et soit N un sous-groupe distingué propre maximal de G. Pour tout $0 \leq j \leq s$, posons*

$N_j = N \cap G_j$. Alors il existe un unique indice $i \in \{1, \dots, s\}$ pour lequel $N_i = N_{i-1}$; on a $G_{i-1}/G_i \simeq G/N$, et les N_j, $j \neq i$, forment une suite de composition de N, de longueur $s-1$, et de sous-quotients G_{j-1}/G_j, $j \neq i$.

Démonstration. — Récurrence sur s. Pour que N puisse exister, il faut que $s \geq 1$; si $s = 1$, G est simple, donc $N = \{1\}$ et il n'y a rien à démontrer. Supposons $s > 1$. Posons $H = N \cap G_1$; alors H est distingué dans G comme intersection de sous-groupes distingués. Si $H = G_1$, on a $G_1 \subset N$, donc $N = G_1$ par maximalité de G_1. Alors clairement $i = 1$ est l'unique indice tel que $N_{i-1} = N_i$, et bien sûr $G_0/G_1 = G/N$. De même, si $H = N$ on a $N \subset G_1$, donc $N = G_1$ et on est dans le même cas que précédemment.

Supposons donc que $H \neq G_1$, $H \neq N$. Alors $N_1 = H \neq N_0$. Le groupe N/H s'identifie à un sous-groupe distingué non trivial de G/G_1 (image de N par la surjection canonique $\pi : G \to G/G_1$), et comme G/G_1 est simple, ceci implique que $N/H \simeq G/G_1$; en particulier, on voit que N/H est simple. Par le même raisonnement, on prouve que $G_1/H \simeq G/N$, et donc que H est distingué propre maximal dans G_1. Mais alors on peut applique l'hypothèse de récurrence à la suite de composition $G_1 \supset G_2 \supset \ldots \supset G_s = \{1\}$ de G_1, qui est de longueur $s-1$, et au sous-groupe H, pour conclure à l'existence d'un unique indice $i \in \{2, \dots, s\}$ tel que $N_{i-1} = N_i$ (noter que $N_j = H_j$ pour $j \geq 1$) ; pour cet indice on a $G_{i-1}/G_i \simeq G_1/H \simeq G/N$, et les $H_j = N_j$, $1 \leq j \leq s$, $j \neq i$, forment une suite de composition de $H = N_1$ de sous-quotients G_{j-1}/G_j, $2 \leq j \leq s$, $j \neq i$. En adjoignant N_0 à gauche de cette suite, on a bien une suite de composition de N, de sous-quotients G_{j-1}/G_j, $j \neq i$, d'où le lemme.

Passons maintenant à la démonstration du théorème. Si G possède une suite de composition de longueur $s \neq 1$, il est simple ou trivial, et il n'y a rien à démontrer (dans ces deux cas, il y a une unique suite de composition). On suppose donc $s > 1$, et le théorème démontré pour tous les groupes possédant une suite de composition de longueur $< s$. Soient

$$G_0 = G \supset G_1 \supset \ldots \supset G_s = \{1\}$$
$$G'_0 = G' \supset G'_1 \supset \ldots \supset G'_t = \{1\}$$

deux suites de composition de G, où l'on peut supposer $t \geq s$ à cause de l'hypothèse de récurrence. Alors d'après le lemme appliqué à $N = G'_1$, il existe un unique indice $i \in \{1, \dots, s\}$ tel que $G'_1 \cap G_i = G'_1 \cap G_{i-1}$; on a $G/G'_1 \simeq G_{i-1}/G_i$, et les $G'_1 \cap G_j$, $j \neq i$, forment une suite de composition de G'_1 don les sous-quotients sont les G_{j-1}/G_j, $j \neq i$. Donc on peut appliquer l'hypothèse de récurrence à G'_1. Or les G'_j, $1 \leq j \leq t$, forment une suite de composition de G'_1 de longueur $t-1$; on a donc $t-1 = s-1$, d'où $t = s$, et les G'_{j-1}/G'_j, $j > 1$, sont isomorphes à l'ordre près aux G_{j-1}/G_j, $j \neq i$, d'où le résultat.

2.4.10 Exercice. — Supposons que les suites de composition de G soient de longueur 2. Montrer alors que si G possède deux suites de composition distinctes, il est isomorphe au produit direct de deux groupes simples. Dans ce cas, montrer que si les deux groupes simples ne sont pas isomorphes, il y a exactement deux suites de composition ; si $G = G_1 \times G_1$ avec G_1 simple, le nombre de suites de composition est égal à $|\mathrm{Aut}\,(G_1, G_1)| + 2$.