Chapitre 1

Théorèmes de Sylow

Dans ce chapitre, nous exposons les théorèmes de Sylow pour les groupes finis, exprimant l'existence, pour un groupe G de cardinal $p^r\ m$ (avec p premier ne divisant pas m), de sous-groupes de cardinal p^r, deux-à-deux conjugués, et en nombre congru à 1 modulo p. Nous montrons également en quoi ce théorème permet d'écrire tout p-groupe comme élément maximal d'une suite croissante de sous-groupes distingués − dont l'ordre est donc, nécessairement, une puissance de p. De ce dernier résultat se déduit le *théorème de Cauchy* pour les groupes, établissant l'existence, dans un groupe de cardinal p^r, d'un élément d'ordre p.

La première partie de ce chapitre est consacrée à des rappels de théorie des groupes, utiles à la démonstration des résultats principaux. Dans tout le chapitre, on considère des groupes finis dont on note la loi de composition interne de manière multiplicative. L'unique inverse de chaque élément g est noté g^{-1}.

1.1 Notions et résultats à connaître

1.1.1 Centre d'un p-groupe

Le résultat établi dans cette section est relatif à la notion suivante.

Définition 1.1. (Centre d'un groupe).
Le **centre** d'un groupe G, noté $Z(G)$ est l'ensemble des éléments de G qui commutent avec tout élément de G. Il est défini par

$$Z(G) = \{x \in G : \forall y \in G, xy = yx\}.$$

Par ailleurs, l'application suivante :

$$\begin{array}{ccc} G \times G & \longrightarrow & G \\ (h, g) & \longmapsto & hgh^{-1} \end{array}$$

définit une action (à gauche) du groupe G sur lui-même appelée *action de G par conjugaison* sur lui-même.

On rappelle alors que pour tout $x \in G$, l'ensemble des éléments de G laissant x invariant dans l'action définit ci-dessus est un sous-groupe de G appelé *centralisateur de x* :

$$Z_x = \{h \in G : hxh^{-1} = x\}$$

C'est aussi l'ensemble des éléments de G qui commutent avec x.

L'*orbite* d'un élément $x \in G$ pour cette action est l'ensemble des éléments atteints lorsqu'on fait agir tous les éléments du groupe G sur x :

$$\Omega_x(G) = \{hxh^{-1} : h \in G\}.$$

Dans un groupe abélien, par exemple :

- le centre et le stabilisateur de tout élément sont égaux au groupe tout entier,
- l'orbite de chaque élément est un singleton.

Soit T une *transversale* pour l'action de groupe définie ci-dessus, c'est-à-dire une famille d'éléments de G dont les orbites forment une partition de G. Notons que l'élément neutre e appartient à toute transversale, puisque c'est le seul élément de son orbite, et que tout élément du centre de G possède une orbite réduite à lui-même. En effet, pour tout $x \in Z(G)$ on a

$$\forall h \in G,\ (hx)h^{-1} = (xh)h^{-1} = x.$$

Ainsi, toute transversale pour l'action de G par conjugaison sur lui-même contient chaque élément du centre de G.

Si G est supposé fini, l'équation aux classes nous donne alors :

$$\operatorname{Card} G = \operatorname{Card} Z(G) + \sum_{x \in T \setminus Z(G)} \frac{\operatorname{Card} G}{\operatorname{Card} Z_x}.$$

On rappelle que pour tout entier premier p, on appelle *p-groupe* tout groupe fini dont le cardinal est une puissance de p. Le résultat suivant découle de

l'équation aux classes vue ci-dessus.

Proposition 1.2. (Non-trivialité du centre d'un p-groupe).
Soit G un p-groupe dont on note le centre $Z(G)$. Alors $Z(G)\backslash\{e\}$ est non-vide.

Démonstration.
L'équation aux classes de l'action de G sur lui-même par conjugaison donne :

$$\operatorname{Card} G = \operatorname{Card} Z(G) + \sum_{x \in \mathcal{T}\backslash Z(G)} \frac{\operatorname{Card} G}{\operatorname{Card} Z_x}$$

où $\mathcal{T}$ est une transversale pour l'action de G sur lui-même par conjugaison et Z_x est l'ensemble des éléments de G qui commutent avec x.

Or, pour $x \in \mathcal{T}\backslash Z(G)$, le centralisateur de x n'est pas G tout entier (sinon, cela signifie que x commute avec tout élément de G, donc que $x \in Z(G)$).

Ainsi, en réduisant l'équation aux classes modulo p, on a $\operatorname{Card} Z(G) \equiv 0[p]$. Comme $Z(G)$ contient e, il ne peut être réduit à cet élément. □

L'équation aux classes pour l'action de conjugaison est un outil utile pour évaluer le caractère abélien d'un groupe fini. On en a une illustration ici pour montrer que $Z(G)$ n'est pas trivial si G est un p-groupe. Nous en verrons une autre dans le chapitre consacré au théorème de Wedderburn, où nous montrerons que le centre du groupe multiplicatif d'un corps fini s'étend en fait à l'ensemble de ce groupe multiplicatif.

1.1.2 Théorème de Cayley pour les groupes

Nous rappelons ici le théorème de Cayley que nous invoquerons plus loin dans ce chapitre. C'est ce résultat affirmant que tout groupe fini G est isomorphe à un sous-groupe du groupe symétrique $\mathcal{S}_n$ où n est l'ordre de G. Dans la démonstration des théorèmes de Sylow, nous combinerons le théorème de Cayley au fait que $\mathcal{S}_n$ est lui-même isomorphe au sous-groupe des matrices de permutation de $\mathrm{GL}_n(\mathbb{F}_p)$, permettant de conclure la première étape de la preuve.

Proposition 1.3. (Théorème de Cayley).
Soit G un groupe quelconque. Alors G est isomorphe à un sous-groupe du groupe des permutations sur G.

En particulier, si G est un groupe fini d'ordre $n \in \mathbb{N}^*$, alors G est isomorphe à un sous-groupe du groupe symétrique $\mathcal{S}_n$.

Démonstration.
Pour tout $g \in G$ on définit l'application $\tau_g : G \to G$ de translation à gauche par g, définie pour tout $x \in G$ par $\tau_g(x) = gx$.
On vérifie sans peine que τ_g est une application bijective, donc une permutation de G.
Notons $\mathcal{S}(G)$ le groupe des permutations de G muni de la loi de composition.
Soit $T : G \to \mathcal{S}(G)$ l'application qui à g associe τ_g.
T est un morphisme injectif de groupes, car :

- pour tous $g, g' \in G$ et $x \in G$, on a $T(gg')(x) = \tau_{gg'}(x) = gg'x = \tau_g(\tau_{g'}(x))$ d'où $T(gg') = T(g) \circ T(g')$ donc T est un morphisme de groupes ;
- si $g \in \operatorname{Ker} T$, alors pour tout $x \in G$, on a $gx = x$ ce qui donne $g = e$ d'où l'injectivité de T.

Ainsi, G est isomorphe à son image $T(G)$ par T qui est un sous-groupe de $\mathcal{S}(G)$. □

1.1.3 Ordre de $\mathrm{GL}_n(\mathbb{F}_q)$

Considérons un entier $p \geqslant 2$ premier, un entier $r \in \mathbb{N}^*$ et posons $q = p^r$. On rappelle (cf. chapitre 13 - *loi de réciprocité quadratique*) qu'il existe un corps fini de cardinal q, unique à isomorphisme (de corps) près, qu'on note $\mathbb{F}_q$.

Ainsi, $\mathrm{GL}_n(\mathbb{F}_q)$ désigne le groupe (multiplicatif) des matrices inversibles de taille n à coefficients dans le corps $\mathbb{F}_q$.

Proposition 1.4. (Dénombrement des bases de $\mathbb{F}_q^n$).
Le $\mathbb{F}_q$-espace vectoriel $\mathbb{F}_q^n$ compte un nombre de bases égal à

$$\prod_{k=0}^{n-1} (q^n - q^k)$$

qui est aussi l'ordre du groupe $\mathrm{GL}_n(\mathbb{F}_q)$.

Démonstration.
Soit $(e_1, \dots, e_n)$ une base de $\mathbb{F}_p^n$. On se livre alors au dénombrement suivant :
- le vecteur e_1 ne peut être nul : il y a donc $q^n - 1$ choix possibles pour ce vecteur.
- étant donné le vecteur e_1, le vecteur e_2 ne peut être choisi sur $\mathbb{F}_q e_1$, qui compte q vecteurs. Il y a donc $q^n - q$ choix possibles pour e_2.
- étant donné les vecteurs e_1 et e_2, le vecteur e_3 ne peut être choisi sur $\mathbb{F}_q e_1 + \mathbb{F}_q e_2$ qui compte q^2 vecteurs. Il y a donc $q^n - q^2$ choix possibles pour e_3.
- etc.

En itérant ce raisonnement, on retrouve le cardinal recherché. □

Du cardinal de $\mathrm{GL}_n(\mathbb{F}_q)$ on déduit celui du groupe spécial linéaire $\mathrm{SL}_n(\mathbb{F}_q)$, comme l'indique le corollaire suivant.

Corollaire 1.5. (Cardinal de $\mathrm{SL}_n(\mathbb{F}_q)$).
Le cardinal de $\mathrm{SL}_n(\mathbb{F}_q)$ est donné par

$$\mathrm{Card}(\mathrm{SL}_n(\mathbb{F}_q)) = \frac{\mathrm{Card}(\mathrm{GL}_n(\mathbb{F}_q))}{q-1} = q^{n-1} \prod_{k=0}^{n-2} (q^n - q^k).$$

Démonstration.
Pour établir cela, on s'intéresse à l'application déterminant, qui est un morphisme de groupes surjectif,

$$\det : \mathrm{GL}_n(\mathbb{F}_q) \longrightarrow \mathbb{F}_q^*.$$

Ainsi, comme les ensembles concernés sont finis, on a

$$\mathrm{Card}(\mathrm{Ker}\det) = \frac{\mathrm{Card}(\mathrm{GL}_n(\mathbb{F}_q))}{\mathrm{Card}(\mathbb{F}_q^*)}$$

avec $\mathrm{Card}(\mathbb{F}_q^*) = q - 1$. □

1.1.4 Étude d'une action à gauche

Dans la démonstration des théorèmes de Sylow, nous allons faire agir à gauche un sous-groupe H d'un groupe F sur l'ensemble des classes à droite F/S où S est aussi un sous-groupe du groupe F. Il est donc important de bien s'approprier les propriétés de cette action classique.

Pour cela, on considère un groupe F et deux sous-groupes H et S de F.

L'action du sous-groupe S à droite sur le groupe F est définie sur $S \times F$ par

$$(s, f) \longmapsto fs.$$

Les *orbites* ou *classes* générées par cette action sont donc les ensembles de la forme

$$fS = \{fs : s \in S\}$$

où f parcourt F. Ainsi, l'ensemble F/S de ces classes est donné par

$$F/S = \{fS : f \in F\}.$$

Suite à cela, il est possible de faire agir H à gauche sur l'*ensemble* F/S par l'application

$$(h, fS) \longmapsto (hf)S$$

qui définit bien une action de groupe.

Proposition 1.6. (Stabilisateur d'une orbite).
Pour $f \in F$, le **stabilisateur** de l'orbite fS, c'est-à-dire l'ensemble des $a \in F$ tels que $a\ (fS) \subset fS$, est l'ensemble

$$(f\ S\ f^{-1}) \cap H.$$

C'est un sous-groupe de F.

Démonstration.
La démonstration de la structure de sous-groupe de F ne pose aucune difficulté. Concentrons-nous sur l'égalité qu'il suffit de démontrer par double inclusion.
Fixons $f \in F$.

- Soit $y \in H$ un élément du stabilisateur de fS. Pour tout $s \in S$, il existe alors $s' \in S$ tel que $yfs = fs'$. Donc $y = fs's^{-1}f \in fSf^{-1} \cap H$.
- Soit $y \in fSf^{-1} \cap H$ et $s \in S$. Soit $s_0 \in S$ tel que $y = fs_0f^{-1}$. Alors $yfs = fs_0s \in fS$, d'où y stabilise fS.

□

1.2 Théorèmes de Sylow et application

1.2.1 Enoncé et démonstration des théorèmes

Les théorèmes que nous traitons ici font référence à la notion de sous-groupe de Sylow, dont nous donnons la définition ci-dessous.

Définition 1.7. (Sous-groupe de Sylow).
Soit G un groupe fini de cardinal $n = p^k\ m$ avec $p \geqslant 2$ premier et p ne divisant pas m. Un **p-sous-groupe de Sylow**, ou plus simplement **p-Sylow**, de G, est un sous-groupe de G d'ordre p^k.

Avec les mêmes notations que la définition, les théorèmes de Sylow garantissent l'existence d'un p-Sylow au groupe G. Plus encore, ils établissent des rapports de conjugaisons entre les p-Sylow de G et donnent une estimation de leur nombre. L'énoncé ci-dessous rassemble ces résultats.

Théorème 1.8. (Théorèmes de Sylow).
Soit G un groupe fini de cardinal $n = p^k\ m$ avec $p \geqslant 2$ premier et p ne divisant pas m. Alors on a les deux énoncés suivants :

i. **Premier théorème de Sylow :** G admet au moins un p-Sylow.

ii. **Second théorème de Sylow :** étant donné un p-Sylow S du groupe G, les p-Sylow de G sont les conjugués de S. De plus, si K est le nombre de p-Sylow de G, alors $K \equiv 1[p]$ et $K|m$.

Démonstration.
La démonstration s'articule en trois temps : nous commençons par démontrer l'existence d'un p-Sylow au groupe G, puis nous montrons la conjugaison des p-Sylow deux-à-deux et nous finissons par les propriétés concernant le nombre de p-Sylow.

- *Existence d'un p-Sylow.*

Ce point sera traité en deux étapes. Tout d'abord, nous montrons que si un groupe fini F admet un p-Sylow, alors tout sous-groupe H de F admet un sous-groupe de Sylow. Puis, nous montrons que G est isomorphe à un sous-groupe de $\mathrm{GL}_n(\mathbb{F}_p)$, pour lequel nous exhiberons un p-Sylow de manière explicite.

Soit F un groupe fini et H un sous-groupe de F. Supposons que F admette un p-Sylow S et montrons qu'il existe $a \in F$ tel que $aSa^{-1} \cap H$ est un p-Sylow de H.

Pour cela, considérons l'action de H à gauche sur l'ensemble F/S, constitué des classes de F dans l'action à droite de S sur F. Notons que F/S n'est pas forcément muni d'une structure de groupe puisque S n'est pas supposé être un sous-groupe distingué de F.

Comme rappelé précédemment, les éléments de F/S sont les ensembles aS où $a \in F$ et le stabilisateur d'une classe donnée aS ($a \in F$) pour l'action de H à gauche est

$aSa^{-1} \cap H$.

Étant donné une transversale $(a_k)_{1 \leqslant k \leqslant J}$ de l'action à gauche de H sur F/S, on écrit alors l'équation aux classes :

$$\operatorname{Card}(F/S) = \sum_{k=1}^{J} \operatorname{Card}(a_k S) = \sum_{k=1}^{J} \frac{\operatorname{Card} H}{\operatorname{Card}(a_k S a_k^{-1} \cap H)}$$

Pour tout $a \in F$, le groupe $(aSa^{-1}) \cap H$ est un sous-groupe de aSa^{-1} qui est d'ordre égal à une puissance de p, puisque de même ordre que le groupe S. D'après le théorème de Lagrange, le groupe $(aSa^{-1}) \cap H$ est donc aussi d'ordre égal à une puissance de p. Donc, si aucun des $(a_k S a_k^{-1}) \cap H$ n'est un p-Sylow de H, alors p divise la somme, donc $\operatorname{Card}(F/S)$.

Or, S est un p-Sylow de F, donc p ne peut diviser $\operatorname{Card}(F/S)$. Ainsi, il existe $1 \leqslant k \leqslant J$ tel que $a_k S a_k^{-1} \cap H$ est un p-Sylow de H. Ainsi, H admet un p-Sylow.

Montrons désormais que G est isomorphe à un sous-groupe de $\mathrm{GL}_n(\mathbb{F}_p)$. Le théorème de Cayley nous permet d'affirmer que G, de cardinal n, est isomorphe à un sous-groupe de $\mathcal{S}_n$, le groupe symétrique d'ordre n.

Or, $\mathcal{S}_n$ est isomorphe au groupe Σ des matrices de permutation à coefficients dans $\mathrm{GL}_n(\mathbb{F}_p)$, qui est un sous-groupe de $\mathrm{GL}_n(\mathbb{F}_p)$. Donc G est isomorphe à un sous-groupe de $\mathrm{GL}_n(\mathbb{F}_p)$.

Il nous reste donc à montrer que $\mathrm{GL}_n(\mathbb{F}_p)$ admet un p-Sylow. D'après la proposition 1.4, l'ordre du groupe $\mathrm{GL}_n(\mathbb{F}_p)$ vaut $\prod_{k=0}^{n-1} (p^n - p^k)$. Ainsi, un p-Sylow éventuel de $\mathrm{GL}_n(\mathbb{F}_p)$ serait d'ordre $p^{n(n-1)/2}$. L'ensemble des matrices triangulaires supérieures avec une diagonale de 1 convient bien : c'est un sous-groupe de $\mathrm{GL}_n(\mathbb{F}_p)$ d'ordre $p^{n(n-1)/2}$.

- *Conjugaison des p-Sylow deux-à-deux.*

Soient S et T deux p-Sylow de G. D'après le raisonnement ci-dessus, il existe $a \in G$ tel que $aSa^{-1} \cap T$ est un p-Sylow de T.

Or, T est son propre p-Sylow. Donc $aSa^{-1} = T$, ce qui montre que S et T sont conjugués.

Réciproquement, si S est p-Sylow de G, il est clair que pour tout $a \in G$, aSa^{-1} est un sous-groupe de G d'ordre p^k, donc un p-Sylow de G.