Exercice

Étienne AFFALOU
ENS de Rennes - Année scolaire 2025-2026

Exercice 1 Soit G un groupe fini. Soit H un sous-groupe de G d'indice premier minimal. Alors, $H \triangleleft G$.

☞ **Solution :** On fait agir H sur G/H par translation à gauche. On a donc un morphisme φ de H dans $\mathfrak{S}(G/H) \simeq \mathfrak{S}_p$. Dans $\mathfrak{S}_p$, le stabilisateur d'un élément est isomorphe à $\mathfrak{S}_{p-1}$, donc comme notre action stabilise la classe H de G/H, l'image de φ est en fait dans le stabilisateur de H qui est isomorphe à $\mathfrak{S}_{p-1}$. On en déduit que l'ordre de $\varphi(H)$ divise $(p-1)!$, et comme l'ordre de $\varphi(H)$ divise aussi l'ordre de H, on a $|\varphi(H)| \mid \text{pgcd}(|H|, (p-1)!)$.
Mais les diviseurs premiers de $|H|$ sont plus grands que p par hypothèse alors que les diviseurs premiers de $(p-1)!$ sont plus petits que $p-1$, donc le pgcd vaut 1 et notre action par translation à gauche de H sur G/H est triviale. On en déduit que $H \triangleleft G$.

☞ **Remarque :** On retrouve le fait qu'un sous-groupe d'indice 2 est toujours distingué (ce résultat est vrai aussi dans le cas où le groupe est infini et se prouve de façon plus élémentaire).

☞ **Application :** En utilisant ce résultat et le premier théorème de Sylow, on peut montrer que si p et q sont deux nombres premiers distincts (par exemple $p < q$) et $\alpha \in \mathbb{N}^*$, un groupe fini G d'ordre pq^α n'est jamais simple.
En effet, G possède un q-Sylow H, et le sous-groupe H est d'indice p dans G, donc $H \triangleleft G$.

Exercice 2 Soit G un groupe fini. Soit p un nombre premier tel que $p \mid |G|$. Alors, G a un élément d'ordre p.

☞ **Solution :** Posons $E = \{(x_0, \cdots, x_{p-1}) \in G^p \mid x_0 \cdots x_{p-1} = 1\}$. Le groupe additif $\mathbb{Z}/p\mathbb{Z}$ agit sur l'ensemble E par $\overline{k} \bullet (x_0, \cdots, x_{p-1}) = (x_{\overline{k}}, \cdots, x_{\overline{k+p-1}})$ (correspond à l'action du p-cycle $(1, \cdots, p)$ sur les indices i des x_i). Cette action est bien définie, car si $x_0 \cdots x_{p-1} = 1$, alors en multipliant à gauche par x_0^{-1} puis à droite par x_0, on a bien $x_1 \cdots x_{p-1} x_0 = 1$ (puis on fait une récurrence). Une orbite pour cette action qui ne contient qu'un seul élément fournit un élément $x = x_1 = \cdots = x_p$ tel que $x^p = 1$. Notons r le nombre d'orbites à un élément. On sait que $r \geqslant 1$ car $1^p = 1$. Il suffit alors de montrer que $r \geqslant 2$ pour trouver un élément d'ordre p. En effet, si $x^p = 1$, alors x est d'ordre 1 ou p d'après le théorème de Lagrange, et il n'y a qu'un seul élément d'ordre 1 dans G.
On commence par remarquer que E contient $|G|^{p-1}$ éléments (on a $|G|$ choix pour les $p-1$ premières coordonnées, puis x_p est nécessairement égal à $(x_0 \cdots x_{p-1})^{-1}$). Ensuite, une orbite non triviale d'un élément X de E a p éléments, car $p = |\mathbb{Z}/p\mathbb{Z}| = |\text{Stab}_X||\text{Orb}_X|$ avec Stab_X un sous-groupe de $\mathbb{Z}/p\mathbb{Z}$ qui n'est pas $\mathbb{Z}/p\mathbb{Z}$ tout entier étant donné que $|\text{Orb}_X| \neq 1$, donc $|\text{Stab}_X| = 1$ puis $|\text{Orb}_X| = p$. En séparant les éléments de E qui sont d'orbite triviale de ceux qui ont une orbite non triviale, on obtient $|G|^{p-1} = r + ps$ où s est le nombre d'orbites non triviales. Mais $|G|^{p-1}$ est multiple de p, donc r est multiple de p (et non nul puisque $r \geqslant 1$). On en déduit que $r \geqslant 2$.

☞ **Remarque :** On retrouve le fait que dans un groupe fini d'ordre pair, il existe un élément d'ordre 2 (ce fait se démontre sans déployer toute l'artillerie des actions de groupes).

☞ **Application :** En utilisant cet exercice, on classifie les groupes G d'ordre $2p$ où p est un nombre premier impair. En effet, on dispose d'un élément x d'ordre p dans G, donc $\langle x \rangle$ est un sous-groupe d'ordre p qui est d'indice 2 dans G donc distingué dans G, et on a aussi un élément y d'ordre 2 dans G. On montre alors ($G = \langle x \rangle \langle y \rangle$ car l'intersection est réduite au neutre et par le second théorème d'isomorphisme) que $G = \langle x \rangle \rtimes \langle y \rangle \simeq (\mathbb{Z}/p\mathbb{Z}) \rtimes (\mathbb{Z}/2\mathbb{Z})$ et il n'y a que deux actions de $\mathbb{Z}/2\mathbb{Z}$ sur $\mathbb{Z}/p\mathbb{Z}$ qui sont l'identité (ce qui donne le produit direct $(\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \simeq \mathbb{Z}/2p\mathbb{Z}$) et moins l'identité (ce qui donne un produit semi-direct isomorphe au groupe diédral D_p).

Exercice 3 Soit G un groupe infini. Soit H un sous-groupe propre d'indice fini de G. Alors G n'est pas simple.

☞ **Solution :** Le groupe G agit sur l'ensemble G/H par translation à gauche. On a donc un morphisme de groupes φ de G dans $\mathfrak{S}(G/H)$. Ici, G est infini, et $\mathfrak{S}(G/H)$ est fini car H est d'indice fini dans G. Donc notre morphisme n'est pas injectif. Il n'est pas non plus trivial, car $G \setminus H \neq \emptyset$ (H est un sous-groupe propre) et si $g \in G \setminus H$, alors $gH \neq H$. Ainsi, $\ker(\varphi)$ est un sous-groupe propre de G, qui est distingué (noyau d'un morphisme de groupes).

☞ **Remarque :** Le résultat est faux si on suppose G fini. En effet, $\mathfrak{A}_5$ est simple mais possède des sous-groupes propres (par exemple un sous-groupe engendré par un 3-cycle).

Exercice 4 Le groupe $\mathrm{SL}_2(\mathbb{F}_3)$ n'a qu'un seul 2-Sylow.

☞ **Solution :** On commence par calculer l'ordre du groupe. Comme $\det : \mathrm{GL}_2(\mathbb{F}_3) \to (\mathbb{F}_3)^*$ est surjectif de noyau $\mathrm{SL}_2(\mathbb{F}_3)$, on a $|\mathrm{SL}_2(\mathbb{F}_3)| = |\mathrm{GL}_2(\mathbb{F}_3)|/2 = (3^2-1)(3^2-3)/2 = 8\times 3$. Un 2-Sylow de $\mathrm{SL}_2(\mathbb{F}_3)$ est donc un sous-groupe d'ordre 8 de $\mathrm{SL}_2(\mathbb{F}_3)$. On regarde donc les éléments d'ordre qui divise 8 dans $\mathrm{SL}_2(\mathbb{F}_3)$. Pour cela, on remarque que $X^8-1 = (X-1)(X+1)(X^2+1)(X^2+X-1)(X^2-X-1)$ dans $\mathbb{F}_3[X]$. Une matrice M de $\mathrm{SL}_2(\mathbb{F}_3)$ dont l'ordre divise 8 peut être d'ordre 1 (donc c'est l'identité), d'ordre 2 ce qui donne un polynôme caractéristique égal à X^2-1 qui est scindé à racines simples donc M est semblable à $-I_2$ (seule matrice possible dans $\mathrm{SL}_2(\mathbb{F}_3)$) donc $M = -I_2$ d'où une unique matrice d'ordre 2 dans $\mathrm{SL}_2(\mathbb{F}_3)$, d'ordre 4 ou d'ordre 8.
Si M est d'ordre 4, M^2 est d'ordre 2 donc $M^2 = -I_2$ donc X^2+1 est le polynôme caractéristique de M. Comme -1 n'est pas un carré de $\mathbb{F}_3$, le polynôme X^2+1 est irréductible sur $\mathbb{F}_3$ (degré 2 sans racine). Donc le polynôme minimal de M est X^2+1 et l'endomorphisme associé est cyclique. La matrice M est donc semblable à la matrice compagnon C du polynôme X^2+1. Pour connaître le nombre de classes de conjugaison pour la matrice C, il suffit de compter le nombre d'éléments dans le stabilisateur pour l'action par conjugaison, c'est-à-dire le cardinal du commutant de la matrice C qui est constitué des polynômes en C de la forme $aC+b$ avec $(a,b) \in \mathbb{F}_3^2 \setminus \{(0,0)\}$ ce qui donne 8 éléments dans le commutant. On a donc $|\mathrm{GL}_2(\mathbb{F}_3)|/8 = 6$ matrices d'ordre 4 dans $\mathrm{SL}_2(\mathbb{F}_3)$.
Enfin, si M est d'ordre 8, son polynôme caractéristique (et son polynôme minimal par irréductibilité sur $\mathbb{F}_3$) est X^2+X-1 ou X^2-X-1 ce qui donne une matrice compagnon qui n'est pas dans $\mathrm{SL}_2(\mathbb{F}_3)$. Ainsi, $\mathrm{SL}_2(\mathbb{F}_3)$ n'a pas d'élément d'ordre 8. Au final, on a seulement 8 matrices dont l'ordre divise 8 dans $\mathrm{SL}_2(\mathbb{F}_3)$. Comme $\mathrm{SL}_2(\mathbb{F}_3)$ a au moins un 2-Sylow, il n'en a qu'un seul et il est formé de ces 8 matrices.

☞ **Remarque :** Les théorèmes de Sylow seuls ne permettaient pas de conclure sur le nombre de 2-Sylow de $\mathrm{SL}_2(\mathbb{F}_3)$. On obtient seulement que ce nombre de 2-Sylow vaut 1 ou 3.

☞ **Application :** Cela permet de montrer que $\mathrm{SL}_2(\mathbb{F}_3)$ est isomorphe à un produit semi-direct $Q_8 \rtimes (\mathbb{Z}/3\mathbb{Z})$ où Q_8 est le groupe des quaternions. En effet, le 2-Sylow de $\mathrm{SL}_2(\mathbb{F}_3)$ étant seul, il est distingué, et en utilisant la classification des groupes d'ordre 8, on montre sans peine que ce 2-Sylow est isomorphe à Q_8. Il ne reste qu'à trouver une matrice de $\mathrm{SL}_2(\mathbb{F}_3)$ d'ordre 3 ($a_{1,1}=0$, $a_{1,2}=1$ et $a_{2,1}=a_{2,2}=-1$ par exemple). Pour conclure, on utilise le deuxième théorème d'isomorphisme.

Exercice 5 Soit G un groupe fini non abélien. La probabilité que deux éléments de G commutent est $\leqslant 5/8$.

☞ **Solution :** Notons $C = \{(g,h) \in G^2 \mid gh = hg\}$. Si $g \in G$, on note $C_g = \{h \in G \mid gh = hg\}$. On a alors $|C| = \sum_{g\in Z(G)} |C_g| + \sum_{g\in G\setminus Z(G)} |C_g| = n|Z(G)| + \sum_{g\in G\setminus Z(G)} |C_g|$ où $n = |G|$. Mais si $g \in G \setminus Z(G)$, C_g est un sous-groupe de G différent de G, donc son ordre est majoré par $n/2$, d'où la majoration $|C| \leqslant nz + (n-z)(n/2)$ où $z = |Z(G)|$. Mais G n'est pas abélien, donc $G/Z(G)$ n'est pas cyclique (la contraposée est un exercice classique). En particulier, comme tout groupe d'ordre inférieur ou égal à 3 est cyclique, on a $n/z = |G/Z(G)| \geqslant 4$. Notant p la probabilité recherchée, on a donc $p = |C|/n^2 \leqslant (z/n) + (1/2) - (z/2n) = (z/2n) + (1/2) \leqslant (1/8) + (1/2) = (5/8)$.

☞ **Remarque :** En utilisant la formule de Burnside, on obtient que le nombre k de classes de conjugaison est égal à $|C|/n$ donc $p = |C|/n^2 = k/n$. En particulier, $k \leqslant 5n/8$.

☞ **Bonus :** Un cas d'égalité se produit lorsque $G/Z(G)$ est d'ordre 4 et lorsque $\forall g \in G \setminus Z(G)$, on a C_g d'indice 2 dans G. C'est réalisé par exemple par le groupe Q_8 qui est d'ordre 8, car $Z(Q_8) = \{\pm 1\}$ qui est bien d'indice 4, et un élément qui n'est pas dans le centre ne commute qu'avec ± 1 et plus ou moins lui-même. Un autre exemple où on a l'égalité est le groupe diédral D_4, car $Z(D_4) = \{\mathrm{id}, r^2\}$ et un élément en dehors du centre ne commute qu'avec id, r^2, lui-même et r^2 fois lui-même.

Exercice 6 Soit p un nombre premier. Quel est le nombre de p-Sylow du groupe symétrique $\mathfrak{S}_p$?

☞ **Solution :** Vu l'ordre de $\mathfrak{S}_p$, un p-Sylow de $\mathfrak{S}_p$ est un sous-groupe de $\mathfrak{S}_p$ d'ordre p. Mais p est premier, donc un p-Sylow de $\mathfrak{S}_p$ est en fait un groupe cyclique d'ordre p. On compte donc le nombre d'éléments d'ordre p dans $\mathfrak{S}_p$, c'est-à-dire le nombre de p-cycles. Il y en a $p!/p = (p-1)!$ car il y a p écritures qui donnent un même p-cycle. Ensuite, dans un p-Sylow, il y a $p-1$ éléments d'ordre p. Cela montre que le nombre de p-Sylow de $\mathfrak{S}_p$ est $(p-1)!/(p-1) = (p-2)!$.

☞ **Remarque :** Pour $p=2$, le groupe symétrique est cyclique d'ordre 2 donc le résultat est trivial. En faisant $p=3$, on trouve en fait le groupe alterné $\mathfrak{A}_3$.

☞ **Application :** En utilisant un théorème de Sylow, on obtient que $(p-2)! \equiv 1 \bmod p$, et donc que $(p-1)! \equiv -1 \bmod p$. On trouve avec surprise une partie du théorème de Wilson, qui dit qu'un nombre entier $p \geqslant 1$ est premier si et seulement si $(p-1)! \equiv -1 \bmod p$.

Exercice 7 Si p est premier et $n \in \mathbb{N}$, un groupe d'ordre p^n a un sous-groupe d'ordre p^k pour $k \in \{0, \cdots, n\}$.

☞ **Solution :** Montrons par récurrence sur n que pour tout groupe G d'ordre p^n, G a un sous-groupe d'ordre p^k pour tout $k \in \{0, \cdots, n\}$. Les cas $n = 0$ et $n = 1$ sont évidents. Soit donc $n \in \mathbb{N}^*$, et supposons tout groupe d'ordre p^{n-1} a un sous-groupe d'ordre p^k pour tout $k \in \{0, \cdots, n-1\}$.
Soit G un groupe d'ordre p^n. Comme G est un p-groupe, son centre est non trivial donc on peut trouver un élément $x \in Z(G)$ d'ordre p (théorème de Cauchy dans le cas abélien). Ainsi, $\langle x \rangle$ est distingué dans G, et le quotient $G/\langle x \rangle$ est un groupe d'ordre p^{n-1}. Par hypothèse de récurrence, $G/\langle x \rangle$ a un sous-groupe d'ordre p^k pour tout $k \in \{0, \cdots, n-1\}$. Notant $\pi : G \to G/\langle x \rangle$ la projection canonique, les images réciproques des sous-groupes d'ordre p^k de $G/\langle x \rangle$ pour $k \in \{0, \cdots, n-1\}$ donnent des sous-groupes d'ordre p^k pour $k \in \{1, \cdots, n\}$ de G.

☞ **Remarque :** Ce résultat donne une réciproque partielle au théorème de Lagrange. Trouver un contre-exemple à la réciproque de ce théorème demande donc de choisir un groupe fini qui n'est pas un p-groupe fini.

☞ **Application :** On peut combiner ce résultat au premier théorème de Sylow qui assure l'existence d'un p-Sylow dans un groupe G dont l'ordre est multiple de p pour obtenir l'existence de sous-groupes de G d'ordre p^k pour $k \in \{0, \cdots, n\}$ où n est la valuation p-adique de $|G|$.

Exercice 8 Déterminer les groupes finis dont le groupe d'automorphismes est trivial.

☞ **Solution :** Soit G un groupe fini tel que $\mathrm{Aut}(G)$ est trivial. En particulier, tout automorphisme intérieur est égal à l'identité, donc G est abélien. On en déduit que l'application de G dans G qui envoie un élément g sur son inverse g^{-1} est un automorphisme, et donc que tout élément de G est d'ordre 2 (ou 1 pour l'élément neutre). On peut donc munir $(G, +)$ d'une structure de $\mathbb{Z}/2\mathbb{Z}$-espace vectoriel de dimension finie (car G est fini) et donc $G \simeq (\mathbb{Z}/2\mathbb{Z})^n$ pour un certain $n \in \mathbb{N}$. Si $n \geqslant 2$, on a un automorphisme non trivial qui échange les deux premières coordonnées. Donc $n \leqslant 1$, et les cas $n = 0$ et $n = 1$ conviennent bien pour la condition demandée.

☞ **Remarque :** De manière générale, si $n \in \mathbb{N}$ avec $n \geqslant 2$, le groupe $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ est isomorphe au groupe multiplicatif $(\mathbb{Z}/n\mathbb{Z})^*$. On peut ensuite étudier la structure de $(\mathbb{Z}/n\mathbb{Z})^*$ en commençant par le cas n premier, puis n puissance d'un nombre premier en distinguant le cas où le nombre premier considéré est égal à 2.

☞ **Bonus :** Soit G un groupe fini tel que $\mathrm{Aut}(G)$ est cyclique. On va montrer que G est cyclique.
Comme $\mathrm{Aut}(G)$ est cyclique, le sous-groupe $\mathrm{Int}(G)$ est encore cyclique. Mais $\mathrm{Int}(G) \simeq G/Z(G)$, donc $G/Z(G)$ est cyclique. Cela prouve que notre groupe G est abélien. En utilisant le théorème de structure des groupes abéliens finis, on peut donc décomposer G comme produit direct de groupes cycliques. En particulier, si G n'est pas cyclique, on a au moins deux facteurs $\mathbb{Z}/m\mathbb{Z}$ et $\mathbb{Z}/dm\mathbb{Z}$ où $m, d \in \mathbb{N}^*$ avec $m \geqslant 2$. Si r est le nombre de facteurs dans la décomposition donnée par le théorème de structure, on va construire deux automorphismes de G qui agissent uniquement sur nos deux facteurs, et qui valent l'identité sur les $r - 2$ autres.
On pose $\varphi : (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/dm\mathbb{Z}) \to (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/dm\mathbb{Z})$ défini par $\varphi(x, y) = (x + y, y)$ et $\psi : (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/dm\mathbb{Z}) \to (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/dm\mathbb{Z})$ défini par $\psi(x, y) = (x, y + dx)$. On vérifie que φ et ψ sont des automorphismes, et que $(\psi \circ \varphi)(0, 1) = (1, 1 + d)$ alors que $(\varphi \circ \psi)(0, 1) = (1, 1)$. Cela contredit la cyclicité de $\mathrm{Aut}(G)$.
Ainsi, le groupe G est cyclique. Si G est un groupe, on peut définir $\mathrm{Aut}^0(G) = G$ et $\forall n \in \mathbb{N}, \mathrm{Aut}^{n+1}(G) = \mathrm{Aut}(\mathrm{Aut}^n(G))$. Les résultats précédents permettent d'affirmer que si G est un groupe fini dont l'un des $\mathrm{Aut}^n(G)$ est trivial est nécessairement cyclique.

Exercice 9 Soit $n \in \mathbb{N}$, $n \geqslant 2$. Quel est le nombre minimum de transpositions engendrant $\mathfrak{S}_n$?

☞ **Solution :** On sait que les $n - 1$ transpositions de la forme $(i\ i+1)$ pour $i \in \{1, \cdots, n-1\}$ engendrent $\mathfrak{S}_n$.
Montrons que le nombre minimum de transpositions engendrant $\mathfrak{S}_n$ est égal à $n - 1$. Pour cela, on considère $\{\tau_1, \cdots, \tau_r\}$ une partie génératrice constituée de transpositions. On construit ensuite le graphe non orienté dont les sommets sont étiquetés par les entiers de l'ensemble $\{1, \cdots, n\}$, et dont les arrêtes sont les $\{i, j\}$ pour $(i\ j) \in \{\tau_1, \cdots, \tau_r\}$. Si ce graphe n'est pas connexe, en prenant un i et j dans deux composantes connexes différentes, on remarque que la transposition qui échange i et j n'est pas dans $\langle \{\tau_1, \cdots, \tau_r\} \rangle$. Notre graphe est donc nécessairement connexe, et possède n sommets. Il a donc au moins $n - 1$ arrêtes, et $r \geqslant n - 1$.

☞ **Remarque :** On peut aussi se demander quel est le nombre minimal de permutations engendrant $\mathfrak{S}_n$. La transposition $(1\ 2)$ et le n-cycle $(1\ \cdots\ n)$ suffisent. En effet, en conjuguant $(1\ 2)$ par les puissances notre n-cycle, on retrouve toute les transpositions de la forme $(i\ i+1)$.

Exercice 10 Soit $n \in \mathbb{N}$, $n \geqslant 2$. Quel est le nombre de p-Sylow de $\mathrm{GL}_n(\mathbb{F}_p)$?

☞ **Solution :** Tout d'abord, on a $|\mathrm{GL}_n(\mathbb{F}_p)| = (p^n-1)(p^n-p)\cdots(p^n-p^{n-1}) = p^{n(n-1)/2}(p^n-1)(p^{n-1}-1)\cdots(p-1)$. Ainsi, un p-Sylow de $\mathrm{GL}_n(\mathbb{F}_p)$ est un sous-groupe d'ordre $p^{n(n-1)/2}$ de $\mathrm{GL}_n(\mathbb{F}_p)$. Le groupe U_n des matrices triangulaires supérieures avec des 1 sur la diagonale de $\mathrm{GL}_n(\mathbb{F}_p)$ est d'ordre $p^{n(n-1)/2}$ car on peut mettre n'importe quel élément de $\mathbb{F}_p$ dans chaque entrée de la matrice au dessus de la diagonale. On sait que les p-Sylow sont conjugués, donc pour connaître le nombre de p-Sylow, il suffit de connaître le nombre d'orbites pour l'action de $\mathrm{GL}_n(\mathbb{F}_p)$ par conjugaison sur l'ensemble de ses p-Sylow. La relation orbite-stabilisateur affirme qu'il suffit de connaître l'ordre du stabilisateur d'un p-Sylow, par exemple U_n.
Soit $g \in \mathrm{GL}_n(\mathbb{F}_p)$ telle que $gU_ng^{-1} = U_n$. Notant E_k le sous-espace vectoriel de $\mathbb{F}_p^n$ engendré par les k premiers vecteurs de la base canonique pour $k \in \{1, \cdots, n\}$ on remarque que les E_k sont stables par tous les éléments de U_n. On en déduit que les $g(E_k)$ sont stables par U_n, puis que $g(E_k) = E_k$ pour tout $k \in \{1, \cdots, n\}$. Ainsi, g est triangulaire supérieure et inversible. Inversement, une matrice triangulaire de $\mathrm{GL}_n(\mathbb{F}_p)$ stabilise bien U_n.
Le groupe des matrices triangulaires supérieures de $\mathrm{GL}_n(\mathbb{F}_p)$ est d'ordre $p^{n(n-1)/2}(p-1)^n$ (on a $p-1$ choix pour chaque coefficient diagonal, et p choix pour chaque coefficient au-dessus de la diagonale). Le nombre d'orbites pour l'action par conjugaison de $\mathrm{GL}_n(\mathbb{F}_p)$ sur l'ensemble de ses p-Sylow est donc égal à $|\mathrm{GL}_n(\mathbb{F}_p)|/p^{n(n-1)/2}(p-1)^n = p^{n(n-1)/2}(p^n-1)(p^{n-1}-1)\cdots(p-1)/p^{n(n-1)/2}(p-1)^n$, et le nombre de p-Sylow de $\mathrm{GL}_n(\mathbb{F}_p)$ est donc $(p+1)(p^2+p+1)\cdots(p^{n-1}+\cdots+p+1)$.

☞ **Remarque :** On a pris $n \geqslant 2$ car $\mathrm{GL}_1(\mathbb{F}_p) \simeq (\mathbb{F}_p)^*$ a $p-1$ éléments et n'a donc pas de p-Sylow non trivial. Ainsi, les p-Sylow de $\mathrm{GL}_n(\mathbb{F}_p)$ ne sont jamais distingués lorsque $n \geqslant 2$.

☞ **Application :** On utilise souvent le sous-groupe U_n pour démontrer l'existence d'un p-Sylow dans $\mathrm{GL}_n(\mathbb{F}_p)$ pour ensuite en déduire le premier théorème de Sylow. En effet, si G est un groupe fini d'ordre n, on a toujours $G \hookrightarrow \mathfrak{S}_n \hookrightarrow \mathrm{GL}_n(\mathbb{F}_p)$. Il s'agit alors d'expliquer pourquoi l'image de G (qui est un sous-groupe de $\mathrm{GL}_n(\mathbb{F}_p)$) admet elle aussi un p-Sylow.

Exercice 11 Soient $n \in \mathbb{N}$, V abélien fini d'ordre impair. Les sous-groupes de $Q_8 \times (\mathbb{Z}/2\mathbb{Z})^n \times V$ sont distingués.

☞ **Solution :** On note $G = Q_8 \times (\mathbb{Z}/2\mathbb{Z})^n \times V$. Soit H un sous-groupe de G. Montrons que H est distingué dans G. Pour cela, il suffit de montrer que $\forall g \in G, \forall h \in H$, on a $\exists k \in \mathbb{N}$ tel que $ghg^{-1} = h^k$ (en effet, on aura bien $ghg^{-1} \in H$). Soit donc $g \in G$ et $x = (h, u, v) \in H$. On se demande s'il existe $k \in \mathbb{N}$ tel que $gxg^{-1} = x^k$. Les groupes $(\mathbb{Z}/2\mathbb{Z})^n$ et V étant abéliens, on a $gxg^{-1} = (q, u, v)$ avec $q \in Q_8$.
Supposons que $gxg^{-1} = x^k$ pour un certain $k \in \mathbb{N}$. On a alors $(h^k, u^k, v^k) = (q, u, v)$. Mais q est un conjugué de h, donc par la connaissance du groupe quaternionique, on a $q = h$ ou $q = h^3$. Si $q = h$, on peut choisir $k = 1$. Sinon, on obtient a priori trois conditions sur k qui sont $k \equiv 3$ [4] (les éléments de Q_8 sont au plus d'ordre 4), $k \equiv 1$ [2] (les éléments de $(\mathbb{Z}/2\mathbb{Z})^n$ sont d'ordre 2) et $k \equiv 1$ [m] (condition donnée par V). On se rend compte que vu la première condition, $k \equiv 1$ [2] est superflue. On recherche donc un entier k tel que $k \equiv 3$ [4] et $k \equiv 1$ [m]. Mais m est impair, donc 4 et m sont premiers entre eux. Ce système de congruence a donc une solution k par le lemme chinois. En prenant un tel entier k, on a alors $x^k = (h^k, u^k, v^k) = (q, u, v) = gxg^{-1}$, d'où le résultat.

☞ **Remarque :** Un groupe non abélien dont tous les sous-groupes sont distingués est dit hamiltonien. Nous venons de démontrer que les groupes $Q_8 \times (\mathbb{Z}/2\mathbb{Z})^n \times V$ sont hamiltoniens. Inversement, un groupe fini hamiltonien est isomorphe à un groupe de la forme $Q_8 \times (\mathbb{Z}/2\mathbb{Z})^n \times V$, mais ce résultat est nettement plus difficile.

☞ **Application :** Ces groupes fournissent des contre-exemples à la réciproque du fait qu'un groupe abélien a tous ses sous-groupes distingués. Le plus simple est le groupe des quaternions Q_8 dont tous les sous-groupes sont distingués car ceux d'ordre 4 sont d'indice 2, et celui d'ordre 2 est égal au centre.

Exercice 12 Classifier les groupes finis d'ordre 87.

☞ **Solution :** Soit G un groupe fini d'ordre 87. Comme $87 = 3 \times 29$ avec 3 et 29 deux nombres premiers, le premier théorème de Sylow (ou simplement l'exercice 2) assure l'existence d'un sous-groupe H d'ordre 3 et d'un sous-groupe K d'ordre 29, tous les deux cycliques. Mais le nombre de 3-Sylow est congru à 1 modulo 3 et divise 29, donc vaut 1. On montre de la même manière que K est le seul sous-groupe d'ordre 29 de G. Mais les éléments de G sont d'ordre 1, 3, 29 ou 87. On a exactement 1 élément d'ordre 1, 2 d'ordre 3 et 28 d'ordre 29. Il reste donc 56 éléments d'ordre 87 dans G. Notre groupe G est donc nécessairement cyclique isomorphe à $\mathbb{Z}/87\mathbb{Z}$.

☞ **Remarque :** Si φ est l'indicatrice d'Euler, on vérifie bien que $\varphi(87) = 2 \times 28 = 56$. Parmi les groupes finis d'ordre plus petit que 100, cette méthode s'applique aux groupes d'ordre 15, 33, 35, 51, 65, 69, 85, 87, 91 et 95.

☞ **Application :** La suite naturelle à cet exercice est la classification des groupes d'ordre pq où p et q sont deux nombres premiers, avec par exemple $p < q$. La connaissance des automorphismes de $\mathbb{Z}/q\mathbb{Z}$ nous donne le résultat suivant. Si p ne divise pas $q-1$, alors un groupe d'ordre pq est cyclique d'ordre pq. Sinon, on obtient deux possibilités et le groupe est soit cyclique d'ordre pq, soit produit semi-direct non trivial de $\mathbb{Z}/q\mathbb{Z}$ par $\mathbb{Z}/p\mathbb{Z}$.

EXERCICE 13 Les groupes $\mathrm{PGL}_2(\mathbb{F}_5)$ et $\mathfrak{S}_5$ sont isomorphes.

☞ **Solution :** On commence par remarquer que le groupe $\mathrm{GL}_2(\mathbb{F}_5)$ agit sur l'ensemble des droites vectorielles de $(\mathbb{F}_5)^2$. Les points de $(\mathbb{F}_5)^2$ n'apparaissent que sur une seule droite vectorielle à la fois, à l'exception de $(0,0)$. Ainsi, si on note k le nombre de droites vectorielles de $(\mathbb{F}_5)^2$, on a $|(\mathbb{F}_5)^2| = 25 = 4\times k+1$ d'où $k=6$. On a donc un morphisme de $\mathrm{GL}_2(\mathbb{F}_5)$ dans $\mathfrak{S}_6$ en numérotant les droites. On rend ce morphisme injectif en quotientant par le noyau de l'action, qui est l'ensemble des éléments de $\mathrm{GL}_2(\mathbb{F}_5)$ qui stabilisent toutes les droites. Ce noyau est donc l'ensemble des homothéties de $\mathrm{GL}_2(\mathbb{F}_5)$, et on a un morphisme injectif $\mathrm{PGL}_2(\mathbb{F}_5) \hookrightarrow \mathfrak{S}_6$. Maintenant, on regarde les ordres des groupes en jeu pour se rendre compte que $|\mathrm{PGL}_2(\mathbb{F}_5)| = |\mathrm{GL}_2(\mathbb{F}_5)|/4 = (5^2-1)(5^2-5)/4 = 120 = |\mathfrak{S}_6|/6$. L'image de $\mathrm{PGL}_2(\mathbb{F}_5)$ par notre morphisme est donc un sous-groupe d'indice 6 de $\mathfrak{S}_6$. Donc $\mathrm{PGL}_2(\mathbb{F}_5) \simeq \mathfrak{S}_5$.

☞ **Remarque :** Tout le début de la preuve se reproduit dans un cadre tout à fait général. Pour la fin, on préfère les cas favorables où l'ordre du groupe projectif linéaire est en fait égal à l'ordre du groupe symétrique, comme par exemple pour le cas de $\mathrm{PGL}_2(\mathbb{F}_3)$ et $\mathfrak{S}_4$. On en déduit même un isomorphisme entre $\mathfrak{A}_4$ et $\mathrm{PSL}_2(\mathbb{F}_3)$ (en effet, $\mathfrak{A}_4$ est le seul sous-groupe d'indice 2 de $\mathfrak{S}_4$). De retour au cadre de cet exercice, on conclut en utilisant un lemme non trivial qui dit qu'un sous-groupe d'indice n de $\mathfrak{S}_n$ est isomorphe à $\mathfrak{S}_{n-1}$ dès que $n \in \mathbb{N}$ avec $n \geqslant 2$.

☞ **Bonus :** On démontre que pour $n \in \mathbb{N}$ avec $n \geqslant 2$, un sous-groupe d'indice n de $\mathfrak{S}_n$ est isomorphe à $\mathfrak{S}_{n-1}$.
Les cas $n=2$ et $n=3$ se traitent sans problème. Ensuite, un sous-groupe H d'indice 4 de $\mathfrak{S}_4$ est d'ordre 6. Ainsi, H est soit isomorphe à $\mathfrak{S}_3$, soit isomorphe à $\mathbb{Z}/6\mathbb{Z}$. Mais $\mathfrak{S}_4$ ne contient pas d'élément d'ordre 6, donc $H \simeq \mathfrak{S}_3$. Il ne reste plus que le cas $n \geqslant 5$. Soit H un sous-groupe de $\mathfrak{S}_n$ d'indice n. L'action de $\mathfrak{S}_n$ par translation à gauche sur $\mathfrak{S}_n/H$ fournit un morphisme de groupes $\varphi : \mathfrak{S}_n \to \mathfrak{S}(\mathfrak{S}_n/H)$. Mais $\ker(\varphi) \subset H$ car $\ker(\varphi)$ est distingué dans $\mathfrak{S}_n$ (en général, le noyau de cette action est l'intersection des gHg^{-1} pour $g \in G$). Ainsi, $\ker(\varphi)$ est un sous-groupe distingué de $\mathfrak{S}_n$ dont l'ordre est inférieur à $(n-1)!$, avec $(n-1)! < n!/2$. Mais les sous-groupes distingués de $\mathfrak{S}_n$ sont $\{1\}, \mathfrak{A}_n$ et $\mathfrak{S}_n$ car $n \geqslant 5$. Donc $\ker(\varphi) = \{1\}$, et φ est injectif, puis un isomorphisme (ordre des groupes). Ainsi, H est isomorphe à $\varphi(H)$, où $\varphi(H)$ est le stabilisateur de la classe de H dans $\mathfrak{S}_n/H$. En tant que stabilisateur d'un point dans un groupe isomorphe à $\mathfrak{S}_n$, le groupe $\varphi(H)$ est isomorphe à $\mathfrak{S}_{n-1}$.

☞ **Application :** Ce résultat permet de démontrer que $\mathrm{Aut}(\mathfrak{S}_6) \neq \mathrm{Int}(\mathfrak{S}_6)$. Notons H la copie de $\mathrm{PGL}_2(\mathbb{F}_5)$ dans $\mathfrak{S}_6$ que nous avons trouvée dans l'exercice. Le groupe $\mathfrak{S}_6$ agit transitivement par translation à gauche sur $\mathfrak{S}_6/H$. Comme dans le bonus, l'action donne un isomorphisme $\varphi : \mathfrak{S}_6 \to \mathfrak{S}(\mathfrak{S}_6/H) \simeq \mathfrak{S}_6$ car H est d'indice 6, et $\varphi(H)$ est le stabilisateur de la classe de H dans $\mathfrak{S}_6/H$. L'action de $\mathrm{PGL}_2(\mathbb{F}_5)$ sur les droites est transitive, donc H agit transitivement sur un ensemble à 6 éléments. Mais $\varphi(H)$ n'agit pas transitivement sur $\mathfrak{S}_6/H$, donc φ n'est pas un automorphisme intérieur. En effet, si φ était intérieur, il s'écrirait $\varphi : x \mapsto \sigma x \sigma^{-1}$ comme H agit transitivement sur $\{1,\cdots,6\}$, pour tout $i,j \in \{1,\cdots,6\}$, $\exists h \in H$ tel que $h(\sigma^{-1}(i)) = \sigma^{-1}(j)$. Ainsi, $\varphi(h)(i) = \sigma h \sigma^{-1}(i) = j$ et $\varphi(H)$ agit transitivement (en identifiant $\mathfrak{S}_6/H$ et $\{1,\cdots,6\}$).

EXERCICE 14 Soit G un groupe fini simple d'ordre pair $\neq 2$. Les 2-Sylow de G ne sont jamais cycliques.

☞ **Solution :** Notons n l'ordre de G. Par le théorème de Cayley, G s'injecte dans $\mathfrak{S}_n$. En composant avec la signature, on obtient un morphisme φ de G dans $\{\pm 1\}$. Comme $|G| > 2$, on ne peut pas avoir $\ker(\varphi) = \{e_G\}$. Par simplicité de G, $\ker(\varphi)$ ne peut valoir que G tout entier. Ainsi, φ est à valeurs dans $\mathfrak{A}_n$. Soit H un 2-Sylow de G. Supposons un court instant que H est cyclique engendré par $h \in H$. Les orbites de l'action par translation à gauche de H sur G sont de cardinal $|H|$ par la relation orbite-stabilisateur. On en déduit que $|G| = k|H|$ avec k impair, et que h agit comme un 2^ℓ cycle sur chaque orbite avec $\ell \in \mathbb{N}^*$. Ainsi, la signature de $\varphi(h)$ vaut $(-1)^{(2^\ell-1)k} = (-1)^k = -1$. C'est absurde car $\varphi(G) \subset A_n$. Ainsi, H ne peut pas être cyclique.

☞ **Remarque :** Une formulation du théorème de Feit-Thompson énonce que tout groupe simple fini non abélien est d'ordre pair. Il est donc naturel de s'intéresser aux propriétés des groupes simples finis d'ordre pair.

☞ **Application :** En particulier, ℓ ne peut pas être égal à 1 car un groupe d'ordre 2 est nécessairement cyclique. On en déduit que l'ordre de G est nécessairement multiple de 4. Ainsi, un groupe d'ordre $2m$ avec m impair différent de 1 n'est jamais simple.