

p -groupes, Sylow et révisions

Travaux dirigés du 21 et du 24 octobre 2025

Dans tout le TD, p est un nombre premier.

✖ Exercice 1. Une forme forte de réciproque au théorème de Lagrange pour les p -groupes

Soit P un p -groupe de cardinal p^n avec $n \geq 1$.

1. Montrer que P a un sous-groupe distingué d'ordre p .

Comme P est non trivial, son centre Z est non trivial par le cours. Ainsi, Z possède un élément d'ordre p . En effet, cela découle immédiatement de Cauchy, ou même plus simplement de ce que si on a $x \in Z \setminus \{1\}$, alors x est d'ordre p^m avec $m > 0$, et donc $x^{p^{m-1}} \in Z$ est d'ordre p . Au final, le sous-groupe $H := \langle x \rangle$ est d'ordre p , inclus dans Z , et donc distingué dans G .

2. Montrer que pour tout entier $0 \leq i \leq n$, il existe un sous-groupe distingué $P_i \subseteq P$ d'ordre p^i , et que l'on peut même supposer $P_i \subseteq P_{i+1}$ pour $0 \leq i < n$.

On raisonne par récurrence sur n . C'est connu pour $n \leq 1$ par la question précédente. Soit C un sous-groupe distingué d'ordre p de P . Le groupe quotient P/C est un p -groupe d'ordre $|P|/p = p^{n-1}$. Par récurrence, il contient des sous-groupes distingués Q_i avec $|Q_i| = p^i$ pour $i < n$ et $Q_i \subseteq Q_{i+1}$ pour $i < n-1$. En utilisant la bijection croissante entre sous-groupes (distingués) de P/C et sous-groupes (distingués) de P contenant C , chaque Q_i s'écrit P_{i+1}/C où P_{i+1} est un sous-groupe distingué de P contenant C , et avec $P_i \subseteq P_{i+1}$ pour $1 \leq i < n$. On a bien sûr $|P_{i+1}| = |C||Q_i| = p^{1+i}$. On conclut en posant $P_0 = \{1\}$.

✖ Exercice 2. Le lemme de Ore

Dans cet exercice, on va montrer le lemme de Ore ainsi qu'une version plus forte dans le cas des p -groupes.

Soit G un groupe fini tel que p est le plus petit facteur premier de $|G|$.

1. On suppose que G agit sur un ensemble X à p éléments. Montrer que G_x agit trivialement sur X pour tout $x \in X$.
Le stabilisateur G_x stabilise l'ensemble $Y = X - \{x\}$ qui a $p-1$ éléments. Toute orbite O_y de G_x dans Y est de cardinal $1 \leq d \leq p-1$. On a $d \mid |G_x|$ par la formule orbite-stabilisateur et donc $d \mid |G|$ (Lagrange). Cela montre $d = 1$ par hypothèse sur $|G|$, donc $O_y = \{y\}$ et l'action est triviale.
2. (Lemme de Ore) En déduire que tout sous-groupe de G d'indice p est distingué.
Soit H un sous-groupe de G d'indice p . On fait agir G par translations sur $X = G/H$, qui a p éléments. Le stabilisateur de H pour cette action est lui-même. Par la question précédente, il agit trivialement sur G/H : on a donc $H \subseteq \text{Stab}_G(gH) = gHg^{-1}$ pour tout $g \in G$, puis H distingué dans G .

Soit maintenant P un p -groupe de cardinal p^n avec $n \geq 1$. On rappelle qu'un sous-groupe $M \subseteq G$ est dit *maximal* si on a $M \neq G$ et aucun sous-groupe de G n'est strictement compris entre M et G . Par exemple, par Lagrange, un sous-groupe d'indice premier est toujours maximal.

3. Montrer que les sous-groupes maximaux d'un p -groupe sont distingués et d'indice p .
Soient P un p -groupe et M un sous-groupe maximal de P (ce qui force $P \neq 1$). On montre que M est distingué d'indice p par récurrence sur $|P|$. C'est évident si on a $|P| = p$, car alors on a $M = \{1\}$. Soit C un sous-groupe central d'ordre p de P (voir la question 1 de l'exercice 1). Si C est inclus dans M alors M/C est un sous-groupe maximal de P/C , donc distingué dans P/C et d'indice p par hypothèse de récurrence, et donc $M = \pi^{-1}(M/C)$ est aussi distingué dans P et d'indice p . Sinon on a $C \cap M = \{1\}$ (puisque $|C \cap M| \in \{1, p\}$) et $MC = P$ par maximalité de M , donc C est un complément de M dans P . Comme C est central, on a alors $P = C \times M$ (produit direct interne). Mais dans ce cas, M est manifestement encore distingué dans P , et d'indice p .
4. Donner un exemple de p -groupe ayant un sous-groupe d'indice p^2 non distingué.
Dans D_8 , les 5 éléments d'ordre 2 sont $c^2 = (1\ 3)(2\ 4)$, $\tau = (1\ 4)(2\ 3)$, $c\tau c^{-1} = (2\ 1)(3\ 4)$, $c\tau = (2\ 4)$ et $\tau c = (3\ 1)$. Seul $\langle c^2 \rangle$ est distingué (en fait, il est central).

Exercice 3. Une autre preuve de l'existence des p -Sylow

Soit G un groupe d'ordre $p^\alpha n$ avec $p \nmid n$ et $\alpha \geq 1$.

1. Montrer $\binom{|G|}{p^\alpha} \not\equiv 0 \pmod{p}$.

On raisonne dans l'anneau $(\mathbb{Z}/p\mathbb{Z})[X]$. L'identité $(1+X)^p = 1+X^p$ montre $(1+X)^{p^\alpha n} = (1+X^{p^\alpha})^n$. En identifiant les coefficients en X^{p^α} on en déduit $\binom{p^\alpha n}{p^\alpha} \equiv n \pmod{p}$, et on conclut car on a $n \not\equiv 0 \pmod{p}$.

2. En considérant l'action de G par translations sur l'ensemble de ses parties à p^α éléments, redémontrer que G possède un p -Sylow.

Soit $\mathcal{E}$ l'ensemble des parties à p^α éléments de G . On fait agir G sur $\mathcal{E}$ par $(g, X) \mapsto gX$. Fixons $X \in \mathcal{E}$, une partie à p^α éléments de G . Son stabilisateur dans G est

$$G_X = \{g \in G \mid gX = X\}$$

En particulier, $X \subseteq G$ est une réunion de classes à droite de G_X dans G , et on a

$$X = \bigsqcup_{i=1}^{n_X} G_X x_i$$

pour certains représentants $x_i \in X$ en nombre n_X , et on a $|G_X|n_X = |X| = p^\alpha$. D'autre part, on a montré $|\mathcal{E}| \not\equiv 0 \pmod p$ à la question 1. On en déduit par équation aux classes qu'il existe une G -orbite dans $\mathcal{E}$ de cardinal premier à p , et donc un $X \in \mathcal{E}$ avec $v_p(|G_X|) = v_p(|G|) = \alpha$ (formule orbite-stabilisateur). Pour un tel X , on nécessairement $n_X = 1$ et $|G_X| = p^\alpha$, et donc G_X est un p -Sylow de G .

✂ Exercice 4. p -Sylow des groupes symétriques

1. Soit $n \geq 1$ tel que $n < p^2$. Exhiber un p -Sylow de S_n .

Pour $n < p^2$ la valuation p -adique de $n!$ est $v_p(n!) = \sum_{k=1}^n v_p(k) = \sum_{k=1}^n 1_{p|k} = \lfloor n/p \rfloor$ (partie entière de n/p). Autrement dit, c'est le plus grand entier $k \geq 0$ tel que $kp \leq n$. Pour $1 \leq i \leq k$, notons c_i un p -cycle quelconque de S_n de support $\{(i-1)p + j \mid 1 \leq j \leq p\}$. Ce sont donc k p -cycles à supports disjoints. Ils engendrent donc un groupe abélien P , et forment même une $\mathbb{Z}/p\mathbb{Z}$ -base de ce dernier (ils sont libres car les supports sont disjoints), de sorte que l'on a $P \simeq (\mathbb{Z}/p\mathbb{Z})^k$. Pour des raisons de cardinalité, P est un p -Sylow de S_n .

2. Soit $n \geq 1$ tel que $p \nmid n+1$. Montrer que S_n et S_{n+1} ont des p -Sylow isomorphes.

Le groupe S_n s'identifie naturellement au sous-groupe H des $\sigma \in S_{n+1}$ vérifiant $\sigma(n+1) = n+1$. On a $|S_{n+1}| = (n+1)|S_n|$. Ainsi, si p ne divise pas $n+1$, tout p -Sylow de H est un p -Sylow de S_{n+1} . On conclut par conjugaison (et donc isomorphisme) des p -Sylow de S_{n+1} .

3. Soit S un p -Sylow de S_{p^2} . Montrer que l'on a $S \simeq (\mathbb{Z}/p\mathbb{Z})^p \rtimes_{\varphi} \mathbb{Z}/p\mathbb{Z}$, où φ envoie le générateur $\bar{1}$ de $\mathbb{Z}/p\mathbb{Z}$ sur la permutation circulaire $(x_1, \dots, x_p) \mapsto (x_2, \dots, x_p, x_1)$ de $(\mathbb{Z}/p\mathbb{Z})^p$.

Les p -Sylow de S_{p^2} sont d'ordre p^m avec $m = v_p(S_{p^2}) = p+1$. Pour $i = 0, \dots, p-1$, on considère le p -cycle

$$c_i = (ip+1 \ ip+2 \ \dots \ ip+p) \in S_{p^2}$$

Ces p permutations sont des p -cycles à supports disjoints. En particulier, elles commutent deux à deux, et par unicité de la décomposition en cycles, engendrent un sous-groupe $H_1 = \langle c_1, \dots, c_p \rangle$ de S_{p^2} isomorphe à $(\mathbb{Z}/p\mathbb{Z})^p$. On a $|H_1| = p^p < p^{p+1}$ donc H_1 est encore p fois trop petit. Considérons enfin l'élément $\tau \in S_{p^2}$ défini par $\tau(i) \equiv i+p \pmod{p^2}$ pour tout i . C'est un produit de p cycles de longueur p à supports disjoints, vérifiant $\tau c_i \tau^{-1} = c_{i+1}$, les indices étant pris modulo p . En particulier, τ normalise H_1 , et on a $\langle \tau \rangle \cap H_1 = \{1\}$, car les éléments de H_1 préservent tous $\{1, \dots, p\}$, alors que 1 est le seul élément de $\langle \tau \rangle$ avec cette propriété. On en déduit que $H_2 = H_1 \langle \tau \rangle$ est un sous-groupe d'ordre p^{p+1} de S_{p^2} . C'est donc un p -Sylow de S_{p^2} , produit semi-direct interne de $\langle \tau \rangle$ et H_1 . Ensuite, on se rappelle (voir exercice 2 du TD précédent) que si $a : (\mathbb{Z}/p\mathbb{Z})^p \xrightarrow{\sim} H_1$ et $b : \mathbb{Z}/p\mathbb{Z} \xrightarrow{\sim} \langle \tau \rangle$ sont des isomorphismes alors la bijection $(\mathbb{Z}/p\mathbb{Z})^p \times \mathbb{Z}/p\mathbb{Z} \rightarrow H_1 \rtimes \langle \tau \rangle$, $(x, y) \mapsto a(x)b(y)$ est un isomorphisme de groupes $(\mathbb{Z}/p\mathbb{Z})^p \rtimes_{\varphi} \mathbb{Z}/p\mathbb{Z} \xrightarrow{\sim} H_1 \rtimes \langle \tau \rangle$, où $\varphi_{\sigma} = a^{-1} \circ \text{int}_{b(y)} \circ a$ pour tout $y \in \mathbb{Z}/p\mathbb{Z}$. En prenant a qui envoie le vecteur e_i de la base canonique de $(\mathbb{Z}/p\mathbb{Z})^p$ sur c_i et b qui envoie la classe de 1 sur τ , on obtient bien que φ envoie le générateur $\bar{1}$ de $\mathbb{Z}/p\mathbb{Z}$ sur la permutation circulaire $(x_1, \dots, x_p) \mapsto (x_2, \dots, x_p, x_1)$ de $(\mathbb{Z}/p\mathbb{Z})^p$, ce qui conclut.

Exercice 5. Zoologie

Déterminer, à isomorphisme près, les sous-groupes de Sylow de S_n pour $n \leq 8$ (on pourra se servir du 1 et du 2 de l'exercice précédent).

On rappelle que les p -Sylow d'un groupe fini G sont tous conjugués, donc isomorphes. On ne considère bien sûr que les premiers $p \leq n$ et on notera $\text{Syl}_{p,n}$ un p -Sylow de S_n . D'après les questions 1 et 2 de l'exercice 4, on a $\text{Syl}_{p,n} \simeq \mathbb{Z}/p\mathbb{Z}$ pour $p \leq n < 2p$, $\text{Syl}_{p,n} \simeq (\mathbb{Z}/p\mathbb{Z})^2$ pour $2p \leq n < 3p$ et $p \neq 2$, et $\text{Syl}_{p,n} \simeq \text{Syl}_{p,n+1}$ pour p ne divisant pas $n+1$. On raisonne au cas par cas.

Pour $n = 2$, on a $\text{Syl}_{2,2} = S_2 \simeq \mathbb{Z}/2\mathbb{Z}$.

Pour $n = 3$, on a $\text{Syl}_{2,3} \simeq \text{Syl}_{2,2} \simeq \mathbb{Z}/2\mathbb{Z}$ et $\text{Syl}_{3,3} \simeq \mathbb{Z}/3\mathbb{Z}$.

Pour $n = 4$, on a $\text{Syl}_{3,4} \simeq \text{Syl}_{3,3} \simeq \mathbb{Z}/3\mathbb{Z}$. On a $|S_4| = 24 = 3 \cdot 8$, donc $|\text{Syl}_{2,4}| = 8$. Mais comme D_4 est un sous-groupe d'ordre 8 de S_4 on a $\text{Syl}_{2,4} \simeq D_4$.

Pour $n = 5$, on a $\text{Syl}_{5,5} \simeq \mathbb{Z}/5\mathbb{Z}$, et pour $p = 2$ ou 3 , $\text{Syl}_{p,5} \simeq \text{Syl}_{p,4}$, déjà décrits.

Pour $n = 6$, on a $\text{Syl}_{5,6} \simeq \text{Syl}_{5,5} \simeq \mathbb{Z}/5\mathbb{Z}$ et $\text{Syl}_{3,6} \simeq (\mathbb{Z}/3\mathbb{Z})^2$. On a aussi $|S_6| = 620 = 2^4 \cdot 3^2 \cdot 5$, donc $|\text{Syl}_{2,6}| = 16$, et il reste donc à trouver un sous-groupe d'ordre 16 de S_6 . Mais $S_4 \times S_2$ s'identifie au sous-groupe de S_6 préservant $\{5, 6\}$, et contient $D_8 \times S_2$ d'ordre 16. On a donc $\text{Syl}_{2,6} \simeq D_8 \times \mathbb{Z}/2\mathbb{Z}$.

Pour $n = 7$, on a $\text{Syl}_{7,7} \simeq \mathbb{Z}/7\mathbb{Z}$ et $\text{Syl}_{p,7} \simeq \text{Syl}_{p,6}$ pour $p = 2, 3, 5$.

On considère enfin le cas $n = 8$. Pour $p = 3, 5, 7$ on a $\text{Syl}_{p,8} \simeq \text{Syl}_{p,7}$, déjà déterminé. On a $|S_8| = 2^7 \cdot 3^2 \cdot 5 \cdot 7$ et donc $|\text{Syl}_{2,8}| = 2^7$. Le sous-groupe de S_8 préservant $\{1, 2, 3, 4\}$ (et donc $\{5, 6, 7, 8\}$) est naturellement isomorphe à $S_4 \times S_4$. On obtient donc un sous-groupe d'ordre 2^6 de S_8 en considérant $D_8 \times D_8$. Concrètement, on peut prendre par exemple

$$D = \langle (1\ 2\ 3\ 4), (5\ 6\ 7\ 8), (1\ 4)(2\ 3), (5\ 8)(6\ 7) \rangle \simeq D_8 \times D_8$$

Ce n'est pas tout à fait un 2-Sylow car son ordre est $2^6 < 2^7$. Mais on constate qu'il est normalisé par l'involution

$$\tau = (15)(26)(37)(48)$$

En effet, la conjugaison par τ échange $(1\ 2\ 3\ 4)$ et $(5\ 6\ 7\ 8)$, ainsi que $(1\ 4)(2\ 3)$ et $(5\ 8)(6\ 7)$. On en déduit que le groupe $S := \langle D, \tau \rangle$ vérifie $S = D \langle \tau \rangle$. Comme τ n'est pas dans D (ce dernier préserve $\{1, 2, 3, 4\}$), on a que $\langle \tau \rangle$ est un complément de D dans S , et donc $|S| = 2^7$: c'est un 2-Sylow de S_8 . Par suivi des isomorphismes, on a

$$\text{Syl}_{2,8} \simeq S \simeq (D_8 \times D_8) \rtimes_{\alpha} \mathbb{Z}/2\mathbb{Z}$$

où $\alpha : \mathbb{Z}/2\mathbb{Z} \rightarrow \text{Aut}(D_8 \times D_8)$ est le morphisme envoyant $\bar{1}$ sur l'automorphisme $(x, y) \mapsto (y, x)$ de $D_8 \times D_8$.

Exercice 6. Fusion

Soient G un groupe fini et P un p -Sylow de G .

1. Montrer $N_G(N_G(P)) = N_G(P)$.

On a clairement $N_G(P) \subseteq N_G(N_G(P))$, montrons l'inclusion réciproque. Soient $H = N_G(P)$ et $g \in G$ avec $gHg^{-1} = H$. On a $P \subseteq H \subseteq G$. Alors gPg^{-1} est un p -Sylow de G , et donc de H . Par conjugaison des p -Sylow dans H , il existe $h \in H$ tel que $gPg^{-1} = hPh^{-1}$. On en déduit $h^{-1}g \in N_G(P) = H$, et donc $g \in H$.

2. Montrer que deux éléments de $C_G(P)$ conjugués dans G sont conjugués dans $N_G(P)$ (Burnside).

On rappelle que pour toute partie $A \subseteq G$, $C_G(A)$ est le sous-groupe des $g \in G$ tels que $ga = ag$ pour tout $a \in A$. Soient $x, y \in C_G(P)$, ainsi que $g \in G$ vérifiant $y = gxg^{-1}$. On a $P \subseteq C_G(x) \cap C_G(y)$ par hypothèse. On a aussi $C_G(y) = gC_G(x)g^{-1}$ en appliquant int_g . On en déduit que P et $g^{-1}Pg$ sont dans $C_G(x)$. Mais ce sont des p -Sylow de G , et donc de $C_G(x)$. Ils sont donc conjugués dans $C_G(x)$: il existe $h \in C_G(x)$ tel que $g^{-1}Pg = hPh^{-1}$. On a donc $gh \in N_G(P)$, et $y = gxg^{-1} = ghxh^{-1}g^{-1}$ utilisant $h \in C_G(x)$.

✂ Exercice 7. Un argument de comptage

Dans cet exercice, on présente un argument de comptage qui, combiné aux théorèmes de Sylow, permet dans des cas favorables de montrer qu'un groupe d'ordre donné n'est pas simple.

Soit G un groupe d'ordre pm avec p premier et $p \wedge m = 1$.

1. Montrer que G possède exactement $n_p(G)(p-1)$ éléments d'ordre p .

Les p -Sylow de G sont cycliques d'ordre p . Chacun p -Sylow contient donc $p-1$ éléments d'ordre p (tous sauf le neutre). Réciproquement, chaque élément d'ordre p engendre un unique p -Sylow de G . Il y a donc $n_p(G)(p-1)$ éléments d'ordre p dans G .

2. On suppose $n_p(G) = m$ et que m est une puissance d'un nombre premier q . Montrer $n_q(G) = 1$.

Soit S l'ensemble des éléments de G qui ne sont pas d'ordre p . Par la question précédente, on a $|G| = |S| + n_p(G)(p-1)$ puis $|S| = pm - (p-1)m = m$. Mais tout q -Sylow est d'ordre m et inclus dans S . Ainsi, S est en fait l'unique q -Sylow de G , et $n_q(G) = 1$.

3. (Application 1) On suppose $|G| = pq^2$, avec q premier $\neq p$. Montrer que G possède un sous-groupe de Sylow distingué.

Si G est simple, on a $n_p(G) > 1$ et $n_q(G) > 1$ (sinon, on aurait un unique sous-groupe de Sylow qui serait donc distingué). Par Sylow, on a donc $n_q(G) = p$ et $n_p(G) = q$ ou q^2 . Mais $n_p(G) = q^2$ implique $n_q(G) = 1$ par la question précédente, une contradiction. On a donc $n_p(G) = q$. Mais on a aussi les congruences $n_q(G) \equiv 1 \pmod{q}$ et $n_p(G) \equiv 1 \pmod{p}$, et donc $p \equiv 1 \pmod{q}$ et $q \equiv 1 \pmod{p}$. C'est absurde, car ces congruences impliquent $p > q$ et $q > p$.

4. (Application 2) On suppose $|G| = pqr$, avec p, q, r premiers distincts. Montrer que G possède un sous-groupe de Sylow distingué.

Par Sylow, on a $n_p(G) \mid qr$ et $n_p(G) \equiv 1 \pmod p$. Par la question 1 on sait que G contient $(p-1)n_p(G)$ éléments d'ordre p . Idem en échangeant les rôles de p, q et r . En comptant les éléments de G d'ordre premier ou 1 on a donc l'inégalité

$$(p-1)n_p(G) + (q-1)n_q(G) + (r-1)n_r(G) < |G| = pqr. \quad (\star)$$

On suppose par l'absurde $n_p(G), n_q(G)$ et $n_r(G)$ tous > 1 . Par la congruence de Sylow, ils sont alors $\geq 1+p, 1+q$ et $1+r$ respectivement. Quitte à renommer p, q , et r on peut supposer $p > q > r$. On en déduit que $n_p(G) \in \{q, r, qr\}$ ne peut pas être q ou r : c'est donc qr . L'inégalité $(\star)$ montre alors $(q-1)n_q(G) + (r-1)n_r(G) < qr$ puis $q^2 - qr + r^2 < 2$. On conclut en remarquant que $f : \mathbb{R} \rightarrow \mathbb{R}, x \mapsto x^2 - rx + r^2 - 2$ est minimale pour $x = r/2$ auquel cas elle vaut $(3/4)q^2 - 2$. Si f admet des valeurs négatives, on a donc $q \leq \sqrt{8/3} < \sqrt{12/3} = 2$: absurde.

Exercice 8. Le morphisme de transfert (d'après le cours *Groupes finis* de J.-P. Serre à l'ENSJF, 1978-1979)

Soient G un groupe et H un sous-groupe d'indice fini de G . On pose $X = G/H$ et on choisit d'abord, pour tout $x \in X$, un représentant $\tilde{x}$ de x dans G . Le groupe G agit par translations sur X . Pour $g \in G$, et $x \in X$, on note $h_{g,x}$ l'unique élément de H vérifiant $g\tilde{x} = \tilde{g\tilde{x}}h_{g,x}$ et on pose

$$\text{Ver}(g) := \prod_{x \in X} h_{g,x} \pmod{D(H)}.$$

Cela définit une application $\text{Ver} : G \rightarrow H_{\text{ab}}$ (de l'allemand *Verlagerung*).

1. Soit $x \mapsto \hat{x}$ un autre système de représentants de X . Pour $x \in X$ on note h_x l'unique élément de H tel que $\hat{x} = \tilde{x}h_x$. Pour $g \in G$ et $x \in X$, on définit aussi $h'_{g,x} \in H$ par $g\hat{x} = \widehat{g\tilde{x}}h'_{g,x}$. Montrer $h'_{g,x} = h_{g,x}^{-1}h_{g,x}h_x$.

Pour $g \in G$ et $x \in X$ fixés, on a par les définitions $g\hat{x} = g\tilde{x}h_x = \widehat{g\tilde{x}}h_{g,x}h_x$ et $\widehat{g\tilde{x}} = \widehat{g\tilde{x}}h_{g,x}^{-1}h_{g,x}h_x$, ce qui conclut.

2. (suite) En déduire que $\text{Ver}(g)$ ne dépend pas du choix de $x \mapsto \tilde{x}$.

Fixons $g \in G$. Dans le groupe abélien H_{ab} on a par la question précédente

$$\prod_{x \in X} h'_{g,x} \equiv \left(\prod_{x \in X} h_{gx} \right)^{-1} \left(\prod_{x \in X} h_{g,x} \right) \left(\prod_{x \in X} h_x \right) \equiv \prod_{x \in X} h_{g,x}$$

car $x \mapsto gx$ est une bijection de X et donc on a $\prod_{x \in X} h_{gx} \equiv \prod_{x \in X} h_x$. Ainsi, $\text{Ver}(g)$ ne dépend pas du choix de $x \mapsto \tilde{x}$.

3. Montrer que pour $g, g' \in G$ on a $h_{gg',x} = h_{g,g'x}h_{g',x}$.

On a et $gg'\hat{x} = g\widehat{g'x}h_{g',x} = \widehat{gg'x}h_{g,g'x}$, puis la relation de l'énoncé.

4. En déduire que Ver est un morphisme de groupes $G \rightarrow H_{\text{ab}}$. On appelle aussi transfert le morphisme $G_{\text{ab}} \rightarrow H_{\text{ab}}$ qui s'en déduit.

Fixons $g, g' \in G$. Comme H_{ab} est abélien on a

$$\text{Ver}(gg') = \prod_{x \in X} h_{gg',x} = \left(\prod_{x \in X} h_{g,g'x} \right) \text{Ver}(g')$$

par la question précédente. On a aussi $\prod_{x \in X} h_{g,g'x} = \prod_{x \in X} h_{g,x} = \text{Ver}(g)$ par la bijection $X \rightarrow X, x \mapsto g'x$, d'où le résultat.

On regarde maintenant le morphisme de restriction $\text{Res} : H_{\text{ab}} \rightarrow G_{\text{ab}}$ qui est le morphisme naturel $hD(H) \mapsto hD(G)$.

5. Soit $g \in G$. Pour chaque orbite Ω_i de $\langle g \rangle$ agissant sur G/H , on choisit un représentant g_iH de Ω_i et on pose $n_i = |\Omega_i|$. Montrer

$$g_i^{-1}g^{n_i}g_i \in H \text{ et } \text{Ver}(g) \equiv \prod_i g_i^{-1}g^{n_i}g_i \pmod{D(H)}$$

Par définition, Ω_i est une orbite de $\langle g \rangle$ et contient l'élément g_iH . Pour ne pas avoir à distinguer les cas où le groupe monogène $\langle g \rangle$ est cyclique ou infini, il sera plus commode de faire agir le groupe $\mathbb{Z}$ sur $X = G/H$ par $(n, x) \mapsto g^n x$. Ses orbites sont bien sur toujours les Ω_i . Le stabilisateur S_i de $g_iH \in \Omega_i$ dans $\mathbb{Z}$ vérifie donc $\mathbb{Z}/S_i \simeq \Omega_i$ (formule orbite-stabilisateur). Ainsi, S_i est non nul, et donc de la forme $d_i\mathbb{Z}$ où $d_i = |\mathbb{Z}/S_i| = |\Omega_i| = n_i$. Donc n_i est le plus

petit entier $n \geq 1$ avec $g^n g_i H = g_i H$, soit encore $g_i^{-1} g^n g_i \in H$. De plus, les n_i éléments de Ω_i sont les $g^n g_i H$ avec $1 \leq n \leq n_i$. On choisit enfin pour représentants de X les éléments $x_{n,i} := g^n g_i$ avec $1 \leq n \leq n_i$. On peut calculer $\text{Ver}(g)$ à l'aide de ce système de représentants par la question 2. On a $g x_{n,i} = x_{n+1,i}$ pour $n < n_i$, autrement dit le $h_{g,x_{n,i}}$ vaut 1, et

$$g x_{n_i,g} = g^{n_i+1} g_i = g g_i g_i^{-1} g^{n_i} g_i = x_{1,i} g_i^{-1} g^{n_i} g_i$$

et donc $h_{g,x_{n_i,i}} = g_i^{-1} g^{n_i} g_i \in H$. On a donc bien $\text{Ver}(g) \equiv \prod_i g_i^{-1} g^{n_i} g_i$.

6. En déduire que $\text{Res} \circ \text{Ver} : G_{\text{ab}} \rightarrow G_{\text{ab}}$ est le morphisme $g \mapsto g^{|G/H|}$.

On a $g_i^{-1} g^{n_i} g_i \equiv g^{n_i}$ dans G_{ab} , et donc $\text{Res}(\text{Ver}(g)) \equiv \prod_i g^{n_i} = g^{\sum_i n_i} = g^{|G/H|}$.

Soient G un groupe fini et P un p -Sylow de G . On suppose que P est dans le centre de son normalisateur $N_G(P)$ (en particulier, P est abélien). On va montrer que P admet un complément distingué dans G (c'est le théorème du complément de Burnside).

7. Soient $g \in P$, $h \in G$, ainsi que n le plus petit entier ≥ 1 tel que $h^{-1} g^n h \in P$. En utilisant la question 2 de l'exercice 6, montrer $h^{-1} g^n h = g^n$. En déduire que $\text{Ver} : G \rightarrow P$ vérifie $\text{Ver}(g) = g^{|G/P|}$ pour tout $g \in P$.

Les éléments g^n et $h g^n h^{-1}$ sont dans P et manifestement conjugués dans G . Comme P est abélien, il est inclus dans son centralisateur. Par la question 2 de l'exercice 6, g^n et $h g^n h^{-1}$ sont donc conjugués dans $N_G(P)$. Ainsi, il existe $k \in N_G(P)$ vérifiant $k g^n k^{-1} = h g^n h^{-1}$. Comme $g^n \in P$ est dans le centre de $N_G(P)$ par hypothèse, on a $k g^n k^{-1} = g^n$, ce qui conclut la première partie de la question. Pour la deuxième, on dit que si $g \in P$, on a $g_i^{-1} g^{n_i} g_i = g^{n_i}$ pour tout i (par ce qui précède), et on conclut avec la formule de la question 5.

8. Conclure en considérant $\ker(\text{Ver})$.

Posons $\varphi = \text{Ver}|_P : P \rightarrow P$. On a $\varphi(g) = g^{|G/P|}$ par la question précédente. C'est un morphisme de groupes (car P est abélien), qui est injectif par Lagrange car $|G/P|$ est premier à $|P|$, et donc bijectif. Soit $N = \ker(\text{Ver})$, c'est un sous-groupe distingué de G . Les remarques que l'on vient de faire montrent que N est un complément de P . En effet, on a d'une part $N \cap P = \ker \varphi = \{1\}$. D'autre part, soit $g \in G$. On a $\text{Ver}(g) = \text{Ver}(p)$ pour un certain $p \in P$ par surjectivité de φ , puis $g p^{-1} \in N$ et $g \in NP$.

On va maintenant voir quelques conséquences du théorème de Burnside. Soient G un groupe fini tel que p est le plus petit facteur premier de $|G|$ et soit P un p -Sylow de G .

9. On suppose P cyclique. Montrer que P admet un complément distingué.

Soit N le normalisateur de P dans G . Considérons le morphisme $\varphi : N \rightarrow \text{Aut}(P)$, $n \mapsto (\text{int}_n)|_P$. Il est trivial sur P car P est abélien, et il se factorise donc en un morphisme $\bar{\varphi} : N/P \rightarrow \text{Aut}(P)$, $nP \mapsto (\text{int}_n)|_P$. On a $P \simeq \mathbb{Z}/p^m\mathbb{Z}$ pour un certain $m \geq 1$, et donc $\text{Aut}(P) \simeq (\mathbb{Z}/p^m\mathbb{Z})^\times$ est d'ordre $\varphi(p^m) = p^{m-1}(p-1)$. Mais $|N/P|$ a tous ses facteurs premiers $> p$ par hypothèse. Il est donc premier à $|\text{Aut}(P)|$, de sorte que tout morphisme $N/P \rightarrow \text{Aut}(P)$ est trivial par Lagrange. Ainsi, $\bar{\varphi}$, puis φ , est trivial. Mais cela veut dire que P est dans le centre de N . Par le théorème de Burnside, P a donc un complément distingué dans G .

10. On suppose $P \simeq (\mathbb{Z}/p\mathbb{Z})^2$. Montrer que soit P admet un complément distingué, soit $p = 2$ et $|G| \equiv 0 \pmod{3}$.

On a cette fois-ci $\text{Aut}(P) \simeq \text{GL}_2(\mathbb{Z}/p\mathbb{Z})$ de cardinal $p(p-1)^2(p+1)$ (le cardinal de $\text{GL}_2(\mathbb{Z}/p\mathbb{Z})$ peut se calculer en disant qu'un élément de $\text{GL}_2(\mathbb{Z}/p\mathbb{Z})$ est la donnée de deux vecteurs de $(\mathbb{Z}/p\mathbb{Z})^2$ non-colinéaires, et on a $p^2 - 1$ possibilités pour choisir le premier (on évite 0), puis $p^2 - p$ possibilités pour choisir le deuxième (on évite la droite engendrée par le premier vecteur), d'où $(p^2 - 1)(p^2 - p)$ possibilités). On conclut de la même manière sauf si $|N/P|$ a un diviseur premier ℓ divisant $p+1$. On aurait $\ell > p$ par hypothèse de minimalité de p , et aussi $\ell \leq p+1$, et donc $\ell = p+1$, $p = 2$ (car p et $p+1$ ont parités distinctes) et $\ell = 3$.

11. En déduire que si G est simple non abélien on a soit $p^3 \mid |G|$, soit $12 \mid |G|$.

Supposons G simple non abélien. Le sous-groupe P n'a pas de complément N distingué car sinon on aurait $N = \{1\}$ par simplicité de G , puis $G = P$, puis G abélien car le centre d'un p -groupe est non trivial (et donc $G \simeq \mathbb{Z}/p\mathbb{Z}$ par simplicité de G). Supposons que p^3 ne divise pas $|G|$. On a donc $|P| = p$ ou $|P| = p^2$. Cela montre que soit P est cyclique, soit $P \simeq (\mathbb{Z}/p\mathbb{Z})^2$. Par la question 9, on est donc dans ce second cas. Par la question 10, on a $p = 2$ et $3 \mid |G|$, puis $2^2 \cdot 3 = 12$ divise $|G|$.