Exercices du chapitre 6

Exercice 6.1. (i) 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 $x \in Z \smallsetminus \{1\}$, alors x est d'orde 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.

(ii) On raisonne par récurrence sur n. C'est trivial pour $n \leqslant 1$. Soit C un sous-groupe distingué d'ordre p de P. Un tel C existe par le (i). 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 $Q_i \subset Q_{i+1}$ 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 $P_i \subset P_{i+1}$ pour $1 \leqslant i < n$. On a bien sûr $|P_{i+1}| = |C||Q_i| = p^{1+i}$. On conclut en posant $P_0 = \{1\}$.

Exercice 6.2. (i) 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 (Exercice 6.1 (i)). 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 $C \cap M = \{1\}$ et $MC = P$, avec C central, donc $P = C \times M$ (produit direct interne). Mais dans ce cas, M est manifestement encore distingué dans P, et d'indice p.

(ii) 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 6.3. On pose $G = \mathrm{GL}_n(k)$, $T = \mathrm{T}_n(k)$ et $U = \mathrm{U}_n(k)$. On note aussi $\epsilon_1, \ldots, \epsilon_n$ la base canonique de k^n, et $F_i = \mathrm{vect}_k(\epsilon_1, \ldots, \epsilon_i)$.

(i) On a un morphisme surjectif naturel $\mathrm{diag} : T \to (k^\times)^n$ de noyau U, c'est pourquoi U est distingué dans T, et on a donc $T \subset \mathrm{N}_G(U)$. Réciproquement, soit $g \in \mathrm{N}_G(U)$. On a $u(F_i) = F_i$ pour tout $u \in U$ et tout i, et donc $u(g(F_i)) = g(F_i)$ pour tout $u \in U$ et tout i. Cela implique $g \in \mathrm{T}_n(k)$. Une manière de le voir est de considérer l'élément $X \in \mathrm{M}_n(k)$ envoyant ϵ_i sur ϵ_{i-1} pour $i > 1$, et ϵ_1 sur 0. L'élément $u = 1 + X \in U$ a pour unique sous-espace stable de dimension i le sous-espace F_i. En effet, si E_i est un tel sous-espace, on a $X_{|E_i}$ nilpotent, donc $X^i(E_i) = 0$, puis $E_i \subset \ker X^i$, mais ce dernier est égal à F_i, et donc $E_i = F_i$ pour des raisons de dimension. Appliqué à $E_i = g(F_i)$, on a montré $g(F_i) = F_i$.

(ii) Soit $g \in G$ normalisant $\mathrm{T}_n(k)$. On voit comme ci-dessus $t(g(F_i)) = g(F_i)$ pour tout $t \in \mathrm{T}_n(k)$, et appliqué à $t = 1 + X$ comme ci-dessus on a encore $g \in \mathrm{T}_n(k)$.

Exercice 6.4. (i) Un groupe d'ordre p^n avec p premier possède au moins un sous-groupe d'ordre p^i pour tout $0 \leqslant i \leqslant n$ d'après l'Exercice 6.1. Ainsi, G possède un sous-groupe H d'ordre p^2. Un tel sous-groupe est nécessairement distingué d'après l'Exercice 6.2, ou encore d'après le Lemme de Ore (Exercice 4.22). Mais on sait qu'un groupe d'ordre p^2 est abélien d'après le cours. Par hypothèse, on a $g^p = 1$ pour tout $g \in G$, et donc H est abélien p-élémentaire. On a donc $H \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

(ii) Soit $g \in \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ vérifiant $g^p = 1$. On a $(g-1)^p = 0$ dans $\mathrm{M}_2(\mathbb{Z}/p\mathbb{Z})$ car $p \mid \mathrm{C}_p^k$ pour $k = 1, \ldots, p-1$. On en déduit que $g-1$ est nilpotente. On a donc $(g-1)^2 = 0$. Mais $g-1$ n'est pas nul car g est d'ordre $p > 1$, donc $g-1$ est d'indice de nilpotence 1, et donc conjuguée à $\left[\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right]$ dans $\mathrm{M}_2(\mathbb{Z}/p\mathbb{Z})$.

(iii) Soit $H \subset G$ le sous-groupe défini au (i). Soit $g \in G \smallsetminus H$. On a $g \neq 1$, donc g est d'ordre p car G est d'exposant p. On a $\langle g\rangle \cap H = \{1\}$(car $g \notin H$ et p est premier), donc $|\langle g\rangle H| = pp^2 = p^3$, puis $K := \langle g\rangle$ est un complément de H. Comme H est distingué, G est produit semi-direct interne de $K \simeq \mathbb{Z}/p\mathbb{Z}$ par $H \simeq (\mathbb{Z}/p\mathbb{Z})^2$. Considérons, comme toujours en situation de produit semi-direct interne, le morphisme de conjugaison

$$\alpha : K \to \mathrm{Aut}(H), k \mapsto \alpha_k, \text{ avec } \alpha_k(h) := \mathrm{int}_k(h) = khk^{-1} \text{ pour } h \in H.$$

On a $(\alpha_g)^p = \alpha_{g^p} = \mathrm{id}_H$ et donc α_g est un automorphisme de H d'ordre divisant p. Si on a $\alpha_g = \mathrm{id}_H$ alors $ghg^{-1} = h$ pour tout $h \in G$ et donc G est commutatif : absurde. Donc α_g est un élément d'ordre p de $\mathrm{Aut}(H) \simeq \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$. Dans une $\mathbb{Z}/p\mathbb{Z}$-base bien choisie du groupe abélien p-élémentaire $H \simeq (\mathbb{Z}/p\mathbb{Z})^2$, cet automorphisme a pour matrice t, par le (ii). Autrement dit, pour un isomorphisme $a : (\mathbb{Z}/p\mathbb{Z})^2 \xrightarrow{\sim} H$ bien choisi, on a $a^{-1}\circ\alpha_g\circ a = t$. On fixe l'isomorphisme $b : \mathbb{Z}/p\mathbb{Z} \to \langle g\rangle, \overline{k} \mapsto g^k$. Par suivi des isomorphismes (Proposition 7.8 Chap. 5), on a donc bien un isomorphisme

$$G \simeq (\mathbb{Z}/p\mathbb{Z})^2 \rtimes_{\alpha'} \mathbb{Z}/p\mathbb{Z},$$

avec $\alpha' : \mathbb{Z}/p\mathbb{Z} \to \mathrm{Aut}((\mathbb{Z}/p\mathbb{Z})^2) = \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ défini par $\alpha'(\overline{1}) = a^{-1} \circ \alpha_g \circ a = t$.

(iv) Le (iii) montre que tout groupe non abélien abélien d'ordre p^3 et d'exposant p est isomorphe au groupe $\Gamma := (\mathbb{Z}/p\mathbb{Z})^2 \rtimes_{\alpha'} \mathbb{Z}/p\mathbb{Z}$ avec α' comme ci-dessus. À isomorphisme près, il y a donc au plus un tel groupe d'ordre p^3. Mais par l'exercice 3.8 Chap. 3, le groupe $\mathrm{U}_3(\mathbb{Z}/p\mathbb{Z})$ convient. Cela termine la démonstration. On a montré au passage que Γ, qui est clairement d'ordre p^3 et non abélien (car $\alpha' \neq 1$), est d'exposant p. Cela peut bien sûr se vérifier directement !

Exercice 6.5. (i) Pour tout $x \in G$ on a $x^{p^3} = 1$ par Lagrange. Mais G n'est pas d'exposant p par hypothèse, donc il existe $x \in G$ d'ordre p^2 ou p^3. Comme G n'est pas abélien (donc non cyclique), un tel x est d'ordre p^2. Le sous-groupe H qu'il engendre est d'incide p dans G donc distingué d'après l'Exercice 6.2, ou encore d'après le Lemme de Ore (Exercice 4.22).

(ii) Soient $g \in G \smallsetminus H$ et $K = \langle g\rangle$. Le groupe H étant distingué d'indice p on a d'une part $G/H \simeq \mathbb{Z}/p\mathbb{Z}$ et donc $g^p \in H$, et d'autre part $G = HK$ car H est maximal. Toutefois, on ne sait pas si on a $H \cap K = \{1\}$ ou non, ou ce qui revient au même, si on a $g^p = 1$ ou non. Quoiqu'il en soit, comme H est distingué on dispose d'un morphisme de groupes $\alpha : G \to \mathrm{Aut}(H), h \mapsto (\mathrm{int}_g)_{|H}$. L'identité $g^p \in H$ et la commutativité de H montrent $\alpha(g)^p = \alpha(g^p) = \mathrm{id}_H$. Mais G n'étant pas commutatif, on a aussi $\alpha(g) \neq \mathrm{id}_H$. On en déduit que $\alpha(g)$ est un automorphisme de H d'ordre p. Mais H est cyclique d'ordre p^2, et donc on sait d'après le cours que tout automorphisme de H est de la forme $\varphi_k(h) = h^k$ avec $k \in (\mathbb{Z}/p^2\mathbb{Z})^\times$, et mieux, que l'application $(\mathbb{Z}/p^2\mathbb{Z})^\times \to \mathrm{Aut}(H), \overline{k} \mapsto \varphi_k$, est un isomorphisme de groupes. On a donc $\alpha(g) = \varphi_k$ pour un unique $k \in (\mathbb{Z}/p^2\mathbb{Z})^\times$ d'ordre p. Toujours par le cours sur les groupes cycliques, pour tout $q \in \mathbb{Z}$ premier à p, l'élément g^q engendre encore K, c'est pourquoi nous pouvons remplacer g par g^q si nécessaire sans changer la situation. Ainsi, quitte à remplacer g par g^{p-1}, et donc k par k^{p-1}, on peut supposer que $k \equiv 1 \bmod p$. Mais alors on a $k \equiv 1 + pu \bmod p^2$ avec $u \neq 0 \bmod p$. Quitte à remplacer en sus g par g^q avec $qu \equiv 1 \bmod p$, on peut supposer que l'on a $k \equiv 1+p \bmod p^2$. Autrement dit, on a $ghg^{-1} = h^{1+p}$ pour tout $h \in H$.

(iii) Soit $h \in H$. Pour $i \geqslant 1$ on a l'identité

$$(hg)^i \;=\; h\, ghg^{-1}\, g^2hg^{-2} \cdots g^{i-1}hg^{1-i}\, g^i.$$

On a aussi $g^ihg^{-i} = h^{(1+p)^i}$ par le (ii), ainsi que la congruence

$$\sum_{i=0}^{p-1}(1+p)^i \;\equiv\; p + (\sum_{i=0}^{p-1} i)\; p \;\equiv\; \frac{p(p+1)}{2} \bmod p^2.$$

On a déjà vu que l'on a $g^p \in H$. Comme G n'est pas abélien, g est d'ordre p ou p^2 (mais pas p^3), de sorte que $g^p \in H$ est d'ordre 1 ou p. Fixons γ un générateur de H. On a $g^p = \gamma^k$ pour un certain $k \equiv 0 \bmod p$. D'autre part, la formule ci-dessus montre

$$(\gamma^q\, g)^p = \gamma^{qp(p+1)/2+k} \quad \text{pour tout } q \in \mathbb{Z}.$$

On cherche $q \in \mathbb{Z}$ tel que $q\,p(p+1)/2 + k \equiv 0 \bmod p^2$. Comme on a $p > 2$ et $k \equiv 0 \bmod p$, il est équivalent de demander $q(p+1)/2 + \frac{k}{p} \equiv 0 \bmod p$. Cette équation a une unique solution $\overline{q} \in \mathbb{Z}/p\mathbb{Z}$ car $(p+1)/2 \equiv -1/2$ est non nul modulo $p > 2$. On pose $h = \gamma^q$.

(iv) On remplace g par hg, qui a même classe dans G/H mais qui a la propriété que $\langle hg\rangle \simeq \mathbb{Z}/p\mathbb{Z}$ est un complément de H. Posant $K' = \langle hg\rangle$, le groupe G est produit semi-direct interne de K' par H. On a encore $\alpha(hg) = \alpha(h)\alpha(g) = 1 \cdot \alpha(g) = \alpha(g) = (x \mapsto x^{(1+p)})$. On conclut par un simple suivi des isomorphismes, comme dans la question (iii) de l'exercice précédent. Il est clair que le produit semi-direct en question est d'ordre p^3, non abélien, et contient un élément d'ordre p^2.

Exercice 6.6. Il y a exactement 2 groupes non abéliens d'ordre p^3 à isomorphisme près. En effet, pour $p = 2$ on a vu en cours qu'il n'y a que H_8 et D_8. Pour $p > 2$, il y en a un et un seul d'exposant p d'après l'exercice 6.4, à savoir le groupe d'Heisenberg fini $\mathrm{U}_3(\mathbb{Z}/p\mathbb{Z})$, ainsi qu'un et un seul d'exposant $> p$ d'après l'exercice 6.5, à savoir le produit semi-direct du (iv) de ce même exercice.

Il faut bien noter que l'on a utilisé $p = 2$ au (iii) de l'Exercice 6.4 ci-dessus. En effet, l'énoncé est inexact pour $p = 2$: le groupe H_8 est d'ordre 8, d'exposant 4, non abélien, mais n'est pas un produit semi-direct de $\mathbb{Z}/2\mathbb{Z}$ par $\mathbb{Z}/4\mathbb{Z}$ (les 3 sous-groupes d'ordre 4 n'ont pas de complément).

Exercice 6.7. Comme une action transitive est par définition sur un ensemble non vide, on a $|G| > 1$.

(i) Pour tout automorphisme α de G, et tout $g \in G$, alors $\alpha(g)$ et g ont même ordre. Par hypothèse, tous les éléments de $G \smallsetminus \{1\}$ ont donc même ordre. Mais l'un d'eux est d'ordre premier p, soit par Cauchy en considérant p premier divisant $|G|$, soit en prenant un élément non trivial arbitraire et en l'élevant à une puissance convenable.

(ii) On sait que tout élément de G est d'ordre 1 ou p par le (i). Par Cauchy, on en déduit que G est un p-groupe. Mais le centre $\mathrm{Z}(G)$ de G est non trivial d'après le cours. Comme $\mathrm{Z}(G)$ est clairement stable par tout automorphisme de G, l'hypothèse sur G montre donc $G = \mathrm{Z}(G)$: c'est un groupe abélien.

(iii) Ainsi, G est un p-groupe abélien élémentaire, et donc isomorphe à $(\mathbb{Z}/p\mathbb{Z})^n$ pour un certain $n \geqslant 1$. Réciproquement un tel groupe convient. En effet, pour tout corps k, le groupe $\mathrm{GL}_n(k)$ agit transitivement sur $k^n \smallsetminus \{0\}$, et on a $\mathrm{Aut}((\mathbb{Z}/p\mathbb{Z})^n) \supset \mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})$ (c'est même une égalité).

Exercice 6.8. (i) Si on a $p \neq 2$, alors n et $2n$ ont même valuation en p. Comme D_{2n} possède un sous-groupe cyclique C d'ordre n, les p-Sylow de C (il n'y en a en fait qu'un seul cas C est cyclique) sont des p-Sylow de D_{2n}, et sont donc cyclique.

(ii) Écrivons $2n = 2^k m$ avec m impair. Les 2-Sylow de S sont d'ordre 2^k. Mais D_{2n} contient un sous-groupe isomorphe à D_{2^k} par l'Exercice 4.41. Un tel sous-groupe est donc un 2-Sylow de D_{2n}, et on a donc $S \simeq \mathrm{D}_{2^k}$ par conjugaison des 2-Sylow.

Exercice 6.9. (i) Pour $n < p^2$ la valuation en p de $n!$ est $[n/p]$ (partie entière de n/p). Autrement dit, c'est le plus grand entier $0 \leqslant k$ tel que $kp \leqslant n$. Pour $1 \leqslant i \leqslant k$, notons c_i un p-cycle quelconque de S_n de support $\{(i-1)p + j \mid 1 \leqslant j \leqslant p\}$. Ce sont donc k p-cycles à supports disjoints. Ils engendrent donc un groupe abélien p-élémentaire 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.

(ii) Le groupe S_n s'identifie naturellement au sous-groupe H des $\sigma \in \mathrm{S}_{n+1}$ vérifiant $\sigma(n+1) = n+1$. On a $|\mathrm{S}_{n+1}| = (n+1)|\mathrm{S}_n|$. 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 isomorphie !) des p-Sylow de S_{n+1}.

Exercice 6.10. On rappelle que les p-Sylow d'un groupe fini G sont tous conjugués, donc isomorphes. On ne considère bien sûr que les premiers $p \leqslant n$ et on notera $\mathrm{Syl}_{p,n}$ un p-Sylow de S_n. D'après l'Exercice 6.9 assertions (i) et (ii), on a $\mathrm{Syl}_{p,n} \simeq \mathbb{Z}/p\mathbb{Z}$ pour $p \leqslant n < 2p$ (facile !), $\mathrm{Syl}_{p,n} \simeq (\mathbb{Z}/p\mathbb{Z})^2$ pour $2p \leqslant n < 3p$ et $p \neq 2$ (idem !), et $\mathrm{Syl}_{p,n} \simeq \mathrm{Syl}_{p,n+1}$ pour p ne divisant pas $n+1$. On raisonne au cas par cas.

Pour $n = 2$, on a clairement $\mathrm{Syl}_{2,2} = \mathrm{S}_2 \simeq \mathbb{Z}/2\mathbb{Z}$.

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

Pour $n = 4$, on a $\mathrm{Syl}_{3,4} \simeq \mathrm{Syl}_{3,3} \simeq \mathbb{Z}/3\mathbb{Z}$. On a $|\mathrm{S}_4| = 24 = 3 \cdot 8$, donc $|\mathrm{Syl}_{2,4}| = 8$. Mais comme D_4 est un sous-groupe d'ordre 8 de S_4 on a $\mathrm{Syl}_{2,4} \simeq \mathrm{D}_4$.

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

Pour $n = 6$, on a $\mathrm{Syl}_{5,6} \simeq \mathrm{Syl}_{5,5} \simeq \mathbb{Z}/5\mathbb{Z}$ et $\mathrm{Syl}_{3,6} \simeq (\mathbb{Z}/3\mathbb{Z})^2$. On a aussi $|\mathrm{S}_6| = 620 = 2^4 \cdot 3^2 \cdot 5$, donc $|\mathrm{Syl}_{2,6}| = 16$, et il reste donc à trouver un sous-groupe d'ordre 16 de S_6. Mais $\mathrm{S}_4 \times \mathrm{S}_2$ s'identifie au sous-groupe de S_6 préservant $\{5, 6\}$, et contient $\mathrm{D}_8 \times \mathrm{S}_2$ d'ordre 16. On a donc $\mathrm{Syl}_{2,6} \simeq \mathrm{D}_8 \times \mathbb{Z}/2\mathbb{Z}$.

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

On considère enfin le cas $n = 8$. Pour $p = 3, 5, 7$ on a $\mathrm{Syl}_{p,8} \simeq \mathrm{Syl}_{p,7}$, déjà déterminé. On a $|\mathrm{S}_8| = 2^7 \cdot 3^2 \cdot 5 \cdot 7$ et donc $|\mathrm{Syl}_{2,8}| = 2^7$. Le sous-groupe de S_8 préservant $\{1, 2, 3, 4\}$ (et donc $\{5, 6, 7, 8\}$) est naturellement isomorphe à $\mathrm{S}_4 \times \mathrm{S}_4$. On obtient donc un sous-groupe d'ordre 2^6 de S_8 en considérant $\mathrm{D}_8 \times \mathrm{D}_8$. Concrètement, on peut prendre par exemple

$$D = \langle (1\,2\,3\,4), (5\,6\,7\,8), (1\,4)(2\,3), (5\,8)(6\,7) \rangle \simeq \mathrm{D}_8 \times \mathrm{D}_8.$$

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

$$\tau = (1\,5)(2\,6)(3\,7)(4\,8).$$

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

$$\mathrm{Syl}_{2,8} \simeq S \simeq (\mathrm{D}_8 \times \mathrm{D}_8) \rtimes_\alpha \mathbb{Z}/2\mathbb{Z}$$

où $\alpha : \mathbb{Z}/2\mathbb{Z} \to \mathrm{Aut}(\mathrm{D}_8 \times \mathrm{D}_8)$ est le morphisme envoyant $\overline{1}$ sur l'automorphisme $(x, y) \mapsto (y, x)$ de $\mathrm{D}_8 \times \mathrm{D}_8$.

Exercice 6.11. Les p-Sylow de S_{p^2} sont d'ordre p^m avec $m = \mathrm{v}_p(\mathrm{S}_{p^2}) = p + 1$. Pour $i = 0, \ldots, p-1$, on considère le p-cycle

$$\mathrm{c}_i = (ip+1 \;\; ip+2 \;\; \ldots \;\; ip+p) \;\in\; \mathrm{S}_{p^2}.$$

Ces p permutations sont des p-cycles sont à supports disjoints. En particulier, elles commutent deux à deux, et par unicité de la décomposition en cycles, engendrent un sous-groupe $H_1 = \langle \mathrm{c}_1, \ldots, \mathrm{c}_p \rangle$ 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 $\tau \in \mathrm{S}_{p^2}$ défini par $\tau(i) \equiv i + p \bmod p^2$ pour tout i. C'est un produit de p cycles de longueur p à supports disjoints, vérifiant $\tau \mathrm{c}_i \tau^{-1} = \mathrm{c}_{i+1}$, 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, et on conclut manifestement par suivi des isomorphismes.

Exercice 6.12. On pose $G = \mathrm{GL}_2(\mathbb{Z}/q\mathbb{Z})$. Observer que l'on a $\gcd(q-1,q+1) = 2$ si 1 pour $q = 2$, et $\gcd(q-1,q+1) = 2$ pour $q > 2$. En particulier, pour $p > 2$ on a exclusivement $p \mid q-1$ ou $p \mid q+1$, de sorte que l'on a $\mathrm{v}_p(|G|) = 2\alpha$ pour $p \mid q-1$ et $\mathrm{v}_p(|G|) = \beta$ pour $p \mid q+1$.

(i) Le sous-groupe des matrices diagonales est isomorphes à $(\mathbb{Z}/q\mathbb{Z})^\times \times (\mathbb{Z}/q\mathbb{Z})^\times$. De plus le groupe $(\mathbb{Z}/q\mathbb{Z})^\times$ est cyclique d'ordre $q-1$ d'après Gauss. Il contient donc un sous-groupe cyclique d'ordre p^α. Ainsi, G contient un sous-groupe diagonal isomorphe à $\mathbb{Z}/p^\alpha\mathbb{Z} \times \mathbb{Z}/p^\alpha\mathbb{Z}$. Par le premier paragraphe ci-dessus, c'est un p-Sylow, et il est donc isomorphe (même conjugué) à S.

(ii) On a vu à l'exercice **??** que G contient un sous-groupe cyclique C d'ordre q^2-1, dont la valuation en p est $\beta = \mathrm{v}_p(|G|)$. Ainsi, le sous-groupe cyclique d'ordre p^β de C est un p-Sylow de G, et donc isomorphe à S.

(iii) On suppose $p = 2$. On a donc $\alpha, \beta \geqslant 1$, $q > 2$, et $\gcd(q-1,q+1) = 2$, de sorte que l'on a soit $\alpha = 1$, soit $\beta = 1$. Supposons d'abord $\beta = 1$. D'après l'Exercice 5.44, le normalisateur dans G du sous-groupe $T \simeq (\mathbb{Z}/q\mathbb{Z})^\times \times (\mathbb{Z}/q\mathbb{Z})^\times$ des matrices diagonales est le groupe $N = T\langle w\rangle$ avec $w = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$. Il est isomorphe à $N' = (\mathbb{Z}/q\mathbb{Z})^\times \times (\mathbb{Z}/q\mathbb{Z})^\times \rtimes_\varphi \mathbb{Z}/2\mathbb{Z}$ avec $\varphi_{\overline{1}}(x,y) = (y,x)$. On constate $\mathrm{v}_2(|N|) = 2\alpha+1 = \mathrm{v}_2(|G|)$ de sorte que les 2-Sylow de N sont des 2-Sylow de G, et donc isomorphes à S. Mais si D désigne l'unique 2-Sylow de $(\mathbb{Z}/q\mathbb{Z})^\times$ (cyclique d'ordre 2^α), alors $D \times D$ est l'unique 2-Sylow de $(\mathbb{Z}/q\mathbb{Z})^\times \times (\mathbb{Z}/q\mathbb{Z})^\times$, et il est stable par $(x,y) \mapsto (y,x)$, de sorte que $(D \times D) \rtimes_\varphi \mathbb{Z}/2\mathbb{Z}$ est un 2-Sylow de $N' \simeq N$, et donc isomorphe à S.

Supposons maintenant $\alpha = 1$, et donc $\mathrm{v}_2(|G|) = 2\alpha+\beta = 2+\beta$. On a vu à l'exercice **??** que G possède un sous-groupe H isomorphe à D_{2n} avec $n := q^2-1 = (q-1)(q+1)$. Mais on a alors $\mathrm{v}_2(|H|) = \mathrm{v}_2(2n) = 1+\alpha+\beta = 2+\beta = \mathrm{v}_2(|G|)$. Ainsi, tout 2-Sylow de D_{2n} est un 2-Sylow de G, et donc isomorphe à S. On conclut par l'Exercice 6.8 (ii).

Exercice 6.13. (i) 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 $\binom{p^\alpha n}{p^\alpha} \equiv n \bmod p$, et on conclut car on a $n \not\equiv 0 \bmod p$.

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

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

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

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

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 $|\mathscr{E}| \not\equiv 0 \bmod p$ au (i). On en déduit par équation aux classes qu'il existe une G-orbite dans $\mathscr{E}$ de cardinal premier à p, et donc un $X \in \mathscr{E}$ avec $\mathrm{v}_p(|G_X|) = \mathrm{v}_p(|G|) = \alpha$ (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 6.15. (i) Seule l'inclusion $\subset$ est non triviale. Soient $H = \mathrm{N}_G(P)$ et $g \in G$ avec $gHg^{-1} = H$. On a $P \subset H \subset G$. 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 $h^{-1}g \in \mathrm{N}_G(P) = H$, et donc $g \in H$. (On a répété l'argument de Frattini, que l'on aurait d'ailleurs pu appliquer directement au groupe $\mathrm{N}_G(H)$ et à son sous-groupe distingué H).

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

Exercice 6.16. (i) Par Cauchy, G possède un sous-groupe cyclique H d'ordre q. Comme H est d'indice p, le plus petit diviseur premier de $|G|$, le Lemme de Ore (Exercice 4.22) montre que H est distingué dans G. Cela montre le (i). Donnons une seconde démonstration utilisant les théorèmes de Sylow. On a $\mathrm{n}_q(G) \,|\, p$ et $\mathrm{n}_q(G) \equiv 1 \bmod q$. On a $p \not\equiv 1 \bmod q$ car $p < q$, donc $\mathrm{n}_q(P) = 1$ et G possède un unique q-Sylow. Il est donc distingué, et cyclique d'ordre q car $\mathrm{v}_q(|G|) = 1$.

(ii) Soit K un sous-groupe d'ordre p de G (il en existe par Cauchy ou Sylow). Pour des raisons de cardinalité (Exercice 2.9), on a $G = HK$ avec $H \cap K = \{1\}$. Ainsi, G est produit semi-direct interne de K par H. Considérons le morphisme de groupes habituel dans cette situation $\alpha : K \to \mathrm{Aut}(H)$, $k \mapsto (h \mapsto khk^{-1})$. Comme H est cyclique d'ordre q on sait que l'on a $\mathrm{Aut}(H) \simeq (\mathbb{Z}/q\mathbb{Z})^\times$, et en particulier $|\mathrm{Aut}(H)| = q - 1$ car q est premier. Sous l'hypothèse $q \not\equiv 1 \bmod p$, les cardinaux $|K|$ et $|\mathrm{Aut}(H)|$ sont premiers entre eux, et donc le morphisme α est trivial (i.e. $khk^{-1} = h$ pour tout $h \in H$ et tout $k \in K$). Le produit semi-direct est donc direct, et on a un isomorphisme

$$G \simeq H \times K \simeq \mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \simeq \mathbb{Z}/pq\mathbb{Z}$$

(le dernier isomorphisme étant l'isomorphisme chinois).

(iii) On suppose désormais $q \equiv 1 \bmod p$. Le groupe $(\mathbb{Z}/q\mathbb{Z})^\times$ étant d'ordre $q-1$ (Gauss), il admet un élément ζ d'ordre p que l'on fixe. Mieux, comme $(\mathbb{Z}/q\mathbb{Z})^\times$ est cyclique, il admet un unique sous-groupe d'ordre p, à savoir $\langle\zeta\rangle$ (ou encore les p racines du polŷnome $X^p - 1$ dans $(\mathbb{Z}/q\mathbb{Z})[X]$). Regardons encore $\alpha : K \to \mathrm{Aut}(H)$ comme ci-dessus. Si α est trivial, le raisonnement précédent s'applique et montre $G \simeq \mathbb{Z}/pq\mathbb{Z}$. Supposons α non trivial, et donc injectif car $|K|$ est premier. Dans ce cas, $\alpha(K)$ est un sous-groupe d'ordre p de $\mathrm{Aut}(H)$: c'est donc $\langle\zeta\rangle$ par la remarque précédente. Ainsi, $x := \alpha^{-1}(\zeta)$ est un générateur de K vérifiant $xhx^{-1} = h^\zeta$ pour tout $h \in H$. Identifions K à $\mathbb{Z}/p\mathbb{Z}$ en envoyant x sur $\overline{1}$, et H à $\mathbb{Z}/q\mathbb{Z}$ arbitrairement. Par suivi des isomorphismes, on a montré $G \simeq G_\zeta$. Comme G_ζ est non commutatif, on a en outre G_ζ non isomorphe à $\mathbb{Z}/pq\mathbb{Z}$.

Exercice 6.17. (i) 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 $\mathrm{n}_p(G)(p-1)$ éléments d'ordre p dans G.

(ii) Soit S l'ensemble des éléments de G qui ne sont pas d'ordre p. Par le (i), on a $|G| = |S| + \mathrm{n}_p(G)(p-1)$ 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 $\mathrm{n}_q(G) = 1$.

(iii) Si G est simple, on a $\mathrm{n}_p(G) > 1$ et $\mathrm{n}_q(G) > 1$. Par Sylow, on a donc $\mathrm{n}_q(G) = p$ et $\mathrm{n}_p(G) = q$ ou q^2. Mais $\mathrm{n}_p(G) = q^2$ implique $\mathrm{n}_q(G) = 1$ par le (ii), une contradiction. On a donc $\mathrm{n}_q(G) = p$. Mais on a aussi les congruences $\mathrm{n}_q(G) \equiv 1 \bmod q$ et $\mathrm{n}_p(G) \equiv 1 \bmod p$, et donc $p \equiv 1 \bmod q$ et $q \equiv 1 \bmod p$. C'est absurde, car ces congruences impliquent $p > q$ et $q > p$.

(iv) Par Sylow, on a $\mathrm{n}_p(G) \,|\, qr$ et $\mathrm{n}_p(G) \equiv 1 \bmod p$. Par le (i) on sait que G contient $(p-1)\mathrm{n}_p(G)$ 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

$$(p-1)\mathrm{n}_p(G) + (q-1)\mathrm{n}_q(G) + (r-1)\mathrm{n}_r(G) < |G| = pqr. \tag{83}$$

On suppose par l'absurde $\mathrm{n}_p(G), \mathrm{n}_q(G)$ et $\mathrm{n}_r(G)$ tous > 1. Par la congruence de Sylow, ils sont alors $\geqslant 1+p, 1+q$ et $1+r$ respectivement. Quitte à renommer p, q, et r on peut supposer $p > q > r$. On en déduit que $\mathrm{n}_p(G) \in \{q, r, qr\}$ ne peut pas être q ou r : c'est donc qr. L'inégalité (83) montre alors $(q-1)\mathrm{n}_q(G) + (r-1)\mathrm{n}_r(G) < qr$ puis $q^2 - qr + r^2 < 2$. Mais on a $4(q^2 - qr + r^2) = (2q-r)^2 + 3r^2$, et $(2q-r)^2 + 3r^2 < 8$ force $r < 2$: absurde.

Exercice 6.18. (i) On peut supposer G non trivial. Si G est un p-groupe, on sait que son centre est non trivial. S'il est simple, il est donc abélien et isomorphe à $\mathbb{Z}/p\mathbb{Z}$. Si on a $|G| = pq$, $|G| = p^2q$ ou $|G| = pqr$ avec p, q, r premiers distincts, on a vu aux Exercices 6.16 et 6.17 que G possède un sous-groupe de Sylow adéquat qui est distingué. En particulier, G n'est pas simple.

(ii) On raisonne par récurrence sur $|G|$ (évident pour $|G| = 1$). Si G est cyclique d'ordre premier, il est résoluble. Sinon, il n'est pas simple par le (i), et donc possède un sous-groupe distingué $H \subset G$ avec $H \neq 1, G$. Mais on a $|H||G/H| = |G|$ donc $|H|$ et $|G/H|$ sont $< |G|$ et encore produits d'au plus 3 nombres premiers, et donc résolubles par hypothèse de récurrence. On en déduit que G est résoluble par le cours.

Exercice 6.19. Pour le (i), voir le corrigé de la question (i) du Problème 1 de l'Examen 2022-2023. Pour le (ii), on rappelle que $\mathrm{n}_p(G)$ est l'indice de $\mathrm{N}_G(P)$ dans G. On a donc soit $\mathrm{n}_p(G) = 1$, soit $|G| \mid \mathrm{n}_p(G)!$ par le (i). Mais si $\mathrm{n}_p(G) = 1$, l'unique p-Sylow de G est distingué, donc égal à G, et G est un p-groupe simple, donc cyclique d'ordre p.

Exercice 6.20. (i) Écrivons $|G| = \prod_{i=1}^r p_i^{\alpha_i}$ avec les p_i premiers distincts et croissants. D'après l'Exercice 6.18, on a $\sum_{i=1}^r \alpha_i \geqslant 4$. On sait aussi que G n'est pas un p-groupe, donc on a $r > 1$. On a enfin $|G| \leqslant 60$ et $3^4 > 60$, puis $p_1 = 2$. On a $2 \cdot 3^3 = 54$ qui convient, et $2 \cdot 3^2 \cdot 5 > 60$, donc supposant $|G| \neq 54$ on a $\alpha_1 \geqslant 2$. Ainsi, $|G|/4$ est $\leqslant 15$ et produit d'au moins deux nombres premiers, dont au moins un impair. Les seules possibilités pour $|G|/4$ sont donc $6, 9, 10, 12, 14$ et 15.

(ii) Si on a $|G| = 24$, alors on a $\mathrm{n}_2(G) > 1$ car G est simple, puis $\mathrm{n}_2(G) = 3$, ce qui est absurde car $24 > 3!$ (Exercice 6.19). De même, on exclut $|G| = 36$ car $\mathrm{n}_3(G) = 1$ ou 4 sont impossibles ($36 > 4!$), et $|G| = 48$ car $\mathrm{n}_2(G) = 1$ ou 3 sont impossibles. Pour $|G| = 40$ c'est plus simple car on a $\mathrm{n}_5(G) = 1$, ainsi que pour $|G| = 54 = 2 \cdot 3^3$ car on a $\mathrm{n}_3(G) = 1$.

(iii) D'après le cours, il ne reste qu'à éliminer $|G| = 56$. Supposons donc $|G| = 56 = 2^3 \cdot 7$. On a $\mathrm{n}_7(G) \mid 8$ et $\mathrm{n}_7(G) \equiv 1 \bmod 7$, donc $\mathrm{n}_7(G) = 8$. Mais cela implique $\mathrm{n}_2(G) = 1$ par le (ii) de l'Exercice 6.17 : une contradiction.

Exercice 6.21. Soient G d'ordre 12, D un 2-Sylow de G et T un 3-Sylow de G. On a $G \simeq \mathbb{Z}/3\mathbb{Z}$ et $|D| = 4$. On sait qu'un groupe d'ordre 4 est abélien (car d'ordre p^2 !) et donc que l'on a $D \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ ou $D \simeq \mathbb{Z}/4\mathbb{Z}$. Par l'Exercice 6.17, soit D, soit T est distingué dans G. Par l'Exercice 2.9, D et T sont compléments l'un de l'autre, et donc on a soit $D \lhd G$ et $G \simeq D \rtimes T$, soit $T \lhd G$ et $G \simeq T \rtimes D$ (produits semi-directs internes). On suppose en outre G non abélien : comme T et D sont abéliens, cela implique que G n'est pas produit direct de T et D.

Supposons d'abord D distingué dans G, et regardons le morphisme $\alpha : T \to \mathrm{Aut}(D), t \mapsto \alpha_t$, avec $\alpha_t(d) = tdt^{-1}$ pour $d \in D$. Comme G n'est pas produit direct, α est non trivial, *i.e.* $\alpha(T)$ est un sous-groupe d'ordre 3 de $\mathrm{Aut}(D)$. Cela montre que D n'est pas cyclique d'ordre 4, sans quoi on aurait $\mathrm{Aut}(D) \simeq (\mathbb{Z}/4\mathbb{Z})^\times \simeq \mathbb{Z}/2\mathbb{Z}$. On a donc $D \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, et $\alpha(T)$ est un sous-groupe d'ordre 3 de $\mathrm{Aut}(D) \simeq \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) \simeq \mathrm{S}_3$. Mais à conjugaison près, il y a un unique élément d'ordre 3 dans $\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$ (ou dans S_3 !), à savoir $u = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$

et son inverse (qui est aussi sa transposée !). On peut donc trouver une $\mathbb{Z}/2\mathbb{Z}$-base e, f du 2-groupe abélien élémentaire D, et un générateur g de T, tels que $\mathrm{Mat}_{e,f}\,\alpha_g = u$. Ainsi, considérons l'isomorphisme $b : \mathbb{Z}/3\mathbb{Z} \xrightarrow{\sim} T$ envoyant 1 sur g, et l'isomorphisme $a : (\mathbb{Z}/2\mathbb{Z})^2 \xrightarrow{\sim} D$ envoyant $(1,0)$ sur e et $(0,1)$ sur f. Par suivi des isomorphismes, on a

$$G \simeq (\mathbb{Z}/2\mathbb{Z})^2 \rtimes_{\alpha'} \mathbb{Z}/3\mathbb{Z}$$

avec $\alpha'_{\overline{1}} = u$. En particulier, il y a au plus un tel groupe G. Mais le groupe $G = \mathrm{A}_4$ convient (on a $D = \mathrm{K}_4$). On a donc $G \simeq \mathrm{A}_4$.

Supposons maintenant T distingué dans G, et regardons le morphisme $\alpha : D \to \mathrm{Aut}(T), d \mapsto \alpha_d$, avec $\alpha_d(t) = dtd^{-1}$ pour $t \in T$. Comme G n'est pas produit direct, α est non trivial, *i.e.* $\alpha(D)$ est un sous-groupe non trivial de $\mathrm{Aut}(T) \simeq (\mathbb{Z}/3\mathbb{Z})^\times \simeq \mathbb{Z}/2\mathbb{Z}$. Autrement dit, il existe $x \in D$ vérifiant $\alpha_x(t) = t^{-1}$ pour tout $t \in T$ (l'unique automorphisme d'ordre 2 d'un groupe d'ordre 3). Comme $d \mapsto \alpha_d$ est un morphisme de groupes, x n'est pas un carré dans D. Cela montre que si on a $D \simeq \mathbb{Z}/4\mathbb{Z}$ alors x engendre D. Dans ce cas, un suivi des isomorphismes montre

$$G \simeq \mathbb{Z}/3\mathbb{Z} \rtimes_{\alpha'} \mathbb{Z}/4\mathbb{Z}, \;\; \alpha'_{\overline{1}}(t) = -t.$$

Le groupe G est donc uniquement déterminé à isomorphisme près, et il y a donc au plus un groupe non abélien d'ordre 12 ayant un 3-Sylow distingué et un 2-Sylow cyclique. Le groupe $\widetilde{\mathrm{D}_6}$ a cette propriété. En effet, il se surjecte sur $\mathrm{D}_6 \simeq \mathrm{S}_3$, de sorte qu'il est non abélien, et il a un unique élément d'ordre 2, de sorte que ses 2-Sylow sont cycliques, et aussi non distingués car ceux de son quotient S_3 sont non distingués.

Dans le cas restant, T est distingué dans G et on a $D \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Soit $y \in D$ tel que $\alpha_y = 1$. On a y d'ordre 2, $y \neq x$, et donc $\{x, y\}$ est une $\mathbb{Z}/2\mathbb{Z}$-base de $D^\sharp \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. On constate que $\langle y \rangle$ est dans le centre de G, et que $\langle x \rangle T$ en est un complément, de sorte que l'on a un produit direct interne $G \simeq \mathbb{Z}/2\mathbb{Z} \times H$ avec $H = \langle x \rangle T$ non abélien d'ordre 6, donc isomorphe à S_3.

Le groupe D_{12} admet un sous-groupe cyclique et distingué d'ordre 6, donc aussi un sous-groupe cyclique distingué d'ordre 3 (rotations d'ordre $\mid 3$), et son 2-Sylow est $\simeq \mathrm{D}_4 \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ (Exercice 6.8, c'est aussi le sous-groupe engendré par deux réflexions orthogonales d'un pentagone régulier). Il est donc isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathrm{S}_3$.

Exercice 6.22. (i) Soit G non abélien d'ordre pq^2. On rappelle que tous les q-Sylow de G sont conjugués, donc isomorphes. Comme ils sont d'ordre q^2, ils sont soit $\simeq \mathbb{Z}/q^2\mathbb{Z}$, soit $\simeq (\mathbb{Z}/q\mathbb{Z})^2$. Enfin, si l'un d'eux est distingué, ils le sont tous, car en fait il n'y en a qu'un. Soient P un p-Sylow de G et Q un q-Sylow de G. On a vu à l'Exercice 6.17 (iii) que soit P, soit Q est distingué dans G. Pour justifier le (i), il ne reste donc qu'à montrer que ces deux cas sont exclusifs. En effet, on a $G = PQ$ et $P \cap Q = \{1\}$ par l'Exercice 2.9. Si P et Q étaient distingués on aurait un produit direct $G = P \times Q$ par l'Exercice 2.11, et G serait abélien car P et Q le sont.

(ii) On écrit encore $G = PQ$ comme ci-dessus et on suppose P distingué. On a donc un produit semi-direct interne de Q par $P \simeq \mathbb{Z}/p\mathbb{Z}$. Pour qu'un tel produit semi-direct soit non abélien, il faut que le morphisme naturel $Q \to \mathrm{Aut}(P) \simeq (\mathbb{Z}/p\mathbb{Z})^\times$ soit non trivial, et donc que q divise $p-1$. Si c'est le cas, fixons un élément $\zeta \in (\mathbb{Z}/p\mathbb{Z})^\times$ d'ordre q. Notons G_n le produit semi-direct $\mathbb{Z}/p\mathbb{Z} \rtimes_\alpha \mathbb{Z}/q^n\mathbb{Z}$ défini par $\alpha : \mathbb{Z}/q^n\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/p\mathbb{Z})$ envoyant $\overline{1}$ sur $x \mapsto \zeta x$. En raisonnant comme dans l'Exercice 6.21, on voit que l'on a soit $G \simeq \mathrm{G}_2$ (cas Q cyclique), soit $G \simeq \mathbb{Z}/q\mathbb{Z} \times G_1$ (cas Q non cyclique). Réciproquement, G_2 et $\mathbb{Z}/q\mathbb{Z} \times G_1$ sont bien d'ordre pq^2, non abéliens, et non isomorphes, le premier ayant un q-Sylow cyclique, et l'autre isomorphe à $(\mathbb{Z}/q\mathbb{Z})^2$.

(iii) On écrit encore $G = PQ$ comme ci-dessus et on suppose maintenant $Q \simeq \mathbb{Z}/q^2\mathbb{Z}$ distingué, de sorte que G est produit semi-direct interne de $P \simeq \mathbb{Z}/p\mathbb{Z}$ par $Q \simeq \mathbb{Z}/q^2\mathbb{Z}$.

Pour qu'un tel produit semi-direct soit non abélien, il faut que le morphisme naturel $P \to \mathrm{Aut}(Q)$ soit non trivial. On sait que $\mathrm{Aut}(\mathbb{Z}/q^2\mathbb{Z}) \simeq (\mathbb{Z}/q^2\mathbb{Z})^\times$ est d'ordre $\varphi(q^2) = q(q-1)$. Ainsi, il existe un morphisme non trivial $\mathbb{Z}/p\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/q^2\mathbb{Z})$ si, et seulement si p divise $q-1$. Supposons donc $q \equiv 1 \bmod p$. On sait que $(\mathbb{Z}/q^2\mathbb{Z})^\times$ est cyclique (Corollaire 5.9 Chap. 2) et donc possède un unique sous-groupe d'ordre p. Fixons $\zeta \in (\mathbb{Z}/q^2\mathbb{Z})^\times$ d'ordre p. Un générateur convenable de P agit donc comme $g \mapsto g^\zeta$ par conjugaison sur Q. Ainsi, par suivi des isomorphismes on a $G \simeq \mathbb{Z}/q^2\mathbb{Z} \rtimes_\alpha \mathbb{Z}/p\mathbb{Z}$ avec $\alpha_{\overline{1}}(x) = \zeta x$, comme unique possibilité pour G. Réciproquement, ce groupe convient, et on a donc $\mathrm{b}(p,q) = 1$.

(iv) On suppose maintenant Q distingué et $Q \simeq (\mathbb{Z}/q\mathbb{Z})^2$. Comme Q est abélien distingué, le morphisme $f : G \to \mathrm{Aut}(Q), g \mapsto (q \mapsto gqg^{-1})$, est trivial sur Q, et donc a pour image le sous-groupe $f(G) = f(P) \simeq \mathbb{Z}/p\mathbb{Z}$ de $\mathrm{Aut}(Q)$. Le choix d'une base de $Q^\sharp$ identifie $f(G)$ à un sous-groupe H de $\mathrm{GL}_2(\mathbb{Z}/q\mathbb{Z})$, et changer de base de Q revient à conjuguer H par un élément de $\mathrm{GL}_2(\mathbb{Z}/q\mathbb{Z})$, de sorte que le groupe G définit une unique classe de conjugaison de sous-groupes d'ordre p de H. Enfin, par suivi des isomorphismes, G s'identifie au produit semi-direct naturel

$$G_H := (\mathbb{Z}/q\mathbb{Z})^2 \rtimes_\alpha H,$$

avec $\alpha_h(x) = h(x)$ pour $h \in H$ et $x \in (\mathbb{Z}/q\mathbb{Z})^2$. Réciproquement, si $H \subset \mathrm{GL}_2(\mathbb{Z}/q\mathbb{Z})$ est un sous-groupe quelconque d'ordre p. Le groupe G_H ci-dessus est d'ordre pq^2, ayant $\{0\} \times (\mathbb{Z}/q\mathbb{Z})^2$ pour unique q-Sylow, et tel que le sous-groupe d'ordre p de $\mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})^2$ naturellement associé, et via l'identification naturelle $\mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})^2 = \mathrm{GL}_2(\mathbb{Z}/q\mathbb{Z})$, est H par construction. Cela conclut.

(v) Supposons d'abord $q = 2$, et donc $p > 2$. On a $\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) \simeq \mathrm{S}_3$. On en déduit $\mathrm{c}(3,2) = 1$ (il y a même un unique sous-groupe d'ordre 3) et $\mathrm{c}(p,2) = 0$ pour $p > 3$. Supposons maintenant $p = 2$, et donc $q > 2$. Un élément d'ordre 2 dans $\mathrm{GL}_2(\mathbb{Z}/q\mathbb{Z})$ est annulé par $X^2 - 1 = (X-1)(X+1) \in \mathbb{Z}/q\mathbb{Z}[X]$ qui est scindé à racines distinctes (car $-1 \neq 1$!). Il est donc conjugé à $\mathrm{diag}(1,-1)$ ou à $\mathrm{diag}(-1,-1)$ (exclusivement), et on a $\mathrm{c}(2,q) = 2$.

(vi) Par le (iii), Cauchy et Lagrange on a

$$\mathrm{c}(p,q) \neq 0 \iff p \,|\, |\mathrm{GL}_2(\mathbb{Z}/q\mathbb{Z})| = q(q-1)(q+1) \iff q \equiv \pm 1 \bmod p.$$

Noter que comme on a $p > 2$, on ne peut pas avoir à la fois p divisant $q+1$ et $q-1$.

Supposons d'abord $p \,|\, q-1$. On a dit que $(\mathbb{Z}/q\mathbb{Z})^\times$ a un sous-groupe d'ordre p, et donc $X^p - 1$ est scindé à racines distinctes dans $\mathbb{Z}/q\mathbb{Z}[X]$. Ainsi, un sous-groupe H d'ordre p est engendré par un élément h diagonalisable. Fixons $\zeta \in (\mathbb{Z}/q\mathbb{Z})^\times$ d'ordre p, et pour $i \in \mathbb{Z}/q\mathbb{Z}$, posons $h_i = \mathrm{diag}(\zeta, \zeta^i)$ et $H_i = \langle h_i \rangle$. On vient de montrer que H est conjugué à l'un des H_i. Reste à voir à quelle condition on a H_i conjugué à H_j. Le groupe H_0 est le seul à avoir un générateur possédant la valeur propre 1, et donc H_i n'est pas conjugué à H_0 pour $i \neq 0$. De plus, dans H_i avec $i \neq 0$, les seuls éléments possédant la valeur propre ζ sont h_i et $\mathrm{diag}(\zeta^j, \zeta)$ où j est l'inverse de i dans $(\mathbb{Z}/p\mathbb{Z})^\times$. Pour i, j non nuls, on a donc H_i conjugué à H_j si, et seulement si, $ij = 1$. On conclut car le nombre d'orbites de $x \mapsto x^{-1}$ sur $(\mathbb{Z}/q\mathbb{Z})^\times$ est $1 + 1 + \frac{p-3}{2} = \frac{p+1}{2}$ car $p > 2$ (on a $q > 2$ et les points fixes sont 1 et -1).

Supposons enfin $p \,|\, q+1$. D'après l'Exercice 6.12, et utilisant $p > 2$, on sait que les p-Sylow de $\mathrm{GL}_2(\mathbb{Z}/q\mathbb{Z})$ sont cycliques. En particulier, chaque p-Sylow de $\mathrm{GL}_2(\mathbb{Z}/q\mathbb{Z})$ possède un et un seul sous-groupe d'ordre p. Mais on sait aussi que tout sous-groupe d'ordre p est inclus dans un p-Sylow, de sorte que par conjugaison des p-Sylow, deux sous-groupes d'ordre p quelconque de $\mathrm{GL}_2(\mathbb{Z}/q\mathbb{Z})$ sont conjugués, [1] et on a $\mathrm{c}(p,q) = 1$.

1. Un autre point de vue, plus naturel avec le recul mais prématuré à ce stade du cursus, consisterait à utiliser que $\mathrm{M}_2(\mathbb{Z}/q\mathbb{Z})$ contient une unique classe de $\mathrm{GL}_2(\mathbb{Z}/q\mathbb{Z})$-conjugaison de sous-corps de cardinal q^2, et d'utiliser que le groupe mutliplicatif d'un tel corps est cyclique par Gauss

Exercice 6.23. (i) Si x, y et z sont d'ordres respectifs p, q et r (Cauchy), alors xyz est d'ordre pqr si G est abélien.

(ii) Le nombre de r-Sylow d'un tel groupe est $\equiv 1 \bmod r$ et divise p ou $q < r$, c'est donc 1.

(iii) D'après l'Exercice 6.17 (iv), G possède un sous-groupe de Sylow S distingué. Par le théorème de Schur-Zassenhaus, S possède un complément K. Si on a $|S| = r$, c'est gagné. Supposons $|S| = p$ ou q, et donc $|K| = pr$ ou qr. Par le (ii), K admet un r-Sylow distingué R. Considérons morphisme de conjugaison $\varphi : R \to \mathrm{Aut}(S)$, $g \mapsto (s \mapsto gsg^{-1})$. On a $\mathrm{Aut}(S) \simeq (\mathbb{Z}/|S|\mathbb{Z})^\times$, d'ordre $|S| - 1 > r$. Ainsi, φ est trivial, et donc S commute à R. Ainsi, le normalisateur de R dans G contient S et K, ainsi donc que $G = SK$, et K est distingué dans G.

(iv) Par le (iii), si G est non abélien d'ordre pq, G est produit semi-direct interne de K par R avec $|R| = r$ et $|K| = pq$. Par l'Exercice 6.16, on sait que l'on a soit $K \simeq \mathbb{Z}/pq\mathbb{Z}$, soit $p \,|\, q-1$ et $K \simeq \mathbb{Z}/q\mathbb{Z} \rtimes \mathbb{Z}/p\mathbb{Z}$, un produit semi-direct supposé *non trivial*, mais qu'il est inutile de préciser davantage, car il n'en existe qu'un à isomorphisme près par cet exercice.

Supposons d'abord $K \simeq \mathbb{Z}/q\mathbb{Z} \rtimes \mathbb{Z}/p\mathbb{Z}$. On a donc $K = QP$ avec Q son q-Sylow distingué et P un p-Sylow. Un morphisme $f : K \to (\mathbb{Z}/r\mathbb{Z})^\times$ est nécessairement trivial sur Q. En effet, f ne peut pas être injectif sinon K serait abélien, et $\ker f = P$ entraînerait P distingué dans K puis $K \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$ par l'Exercice 2.11. On a donc $q \,|\, \ker f$, puis $Q \subset \ker f$, *i.e.* f se factorise par $K/Q \simeq \mathbb{Z}/p\mathbb{Z}$. On a donc soit $f(K) = 1$ et $G = \mathbb{Z}/r\mathbb{Z} \times H$ (produit direct), soit $f(K)$ est l'unique sous-groupe d'ordre p de $\mathrm{Aut}(\mathbb{Z}/r\mathbb{Z}) \simeq (\mathbb{Z}/r\mathbb{Z})^\times$. Ce dernier cas est possible si, et seulement si, on a $p \,|\, r-1$. Il conduit à un produit semi-direct unique à isomorphisme près que l'on note $\mathbb{Z}/r\mathbb{Z} \rtimes (\mathbb{Z}/q\mathbb{Z} \rtimes \mathbb{Z}/p\mathbb{Z})$. En effet, pour justifier l'unicité fixons $\zeta \in (\mathbb{Z}/r\mathbb{Z})^\times$ d'ordre p. Il existe $x \in P$ tel que $f(x) = \zeta$. On identifie P à $\mathbb{Z}/p\mathbb{Z}$ en faisant correspondre x et $\overline{1}$. Par suivi des isomorphismes, on a identifié G à $\mathbb{Z}/r\mathbb{Z} \rtimes_\alpha (\mathbb{Z}/q\mathbb{Z} \rtimes \mathbb{Z}/p\mathbb{Z})$ où α est l'unique morphisme $\mathbb{Z}/q\mathbb{Z} \rtimes \mathbb{Z}/p\mathbb{Z} \to (\mathbb{Z}/r\mathbb{Z})^\times$ trivial sur $\mathbb{Z}/q\mathbb{Z} \times \{0\}$ et envoyant $(0, \overline{1})$ sur ζ.

Supposons maintenant $H \simeq \mathbb{Z}/pq\mathbb{Z}$. On a donc $H = Q \times P$ (produit direct) avec Q, P les uniques q et p-Sylow de G. Pour $n \,|\, pq$ et $n \,|\, r-1$, il existe à isomorphisme près un unique produit semi-direct $\mathbb{Z}/r\mathbb{Z} \rtimes_n \mathbb{Z}/pq\mathbb{Z}$ tel que le morphisme correspondant $\mathbb{Z}/pq\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/r\mathbb{Z})$ a pour image l'unique sous-groupe cyclique d'ordre n de $\mathrm{Aut}(\mathbb{Z}/r\mathbb{Z}) \simeq (\mathbb{Z}/r\mathbb{Z})^\times$. Ces assertions d'unicité découlent d'un simple suivi d'isomorphismes sans doute maitrisé par le lecteur s'il s'est aventuré jusque là !

Exercice 6.24. Dans la table on constate que l'on a $\mathrm{N}(n) = 1$ si, et seulement si, $n = pq$ avec p et q premiers et $p \,|\, q-1$. Tous ces cas sont donc expliqués par l'Exercice 6.16.

Dans tous les cas $\mathrm{N}(n) = 2, 3$ ou 5 on a $n = pqr$ avec p, q, r premiers. On a vu en effet qu'il y a exactement deux groupes non abéliens d'ordre p^3 pour p premier (Exercice 6.6) donc le cas $p = q = r$ donne bien $\mathrm{N}(n) = 2$. Les cas $n = pq^2$ avec $q \neq p$ sont aussi tous expliqués par l'Exercice 6.22. Les deux cas avec p, q, r distincts sont $30 = 2 \cdot 3 \cdot 5$ et $42 = 2 \cdot 3 \cdot 7$. Mais on a $\mathrm{N}(30) = 3$ par l'Exercice 6.16 car on a $2 \,|\, 3-1$, $2 \,|\, 5-1$ et $3 \nmid 5-1$. De plus, on a aussi $\mathrm{N}(42) = 5$ car on a $2 \,|\, 3-1$, $2 \,|\, 5-1$ et $3 \mid 7-1$

Exercice 6.25. (i) Pour $g \in G$ et $x \in X$ fixés, on a par définitions

$$g\,\widehat{x} \;=\; \widehat{gx}\,h'_{g,x} \;=\; \widetilde{gx}\,h_{gx}\,h'_{g,x} = g\,\widetilde{x}\,h_{g,x}^{-1}\,h_{gx}\,h'_{g,x} \;=\; g\,\widehat{x}\,h_x^{-1}\,h_{g,x}^{-1}\,h_{gx}\,h'_{g,x}.$$

(d'ordre $q^2 - 1$). L'idée est qu'à isomorphisme près, il n'y a qu'un corps fini de cardinal q^2, disons $\mathbb{F}_{q^2}$, et qu'une structure de $\mathbb{F}_{q^2}$-espace vectoriel sur le groupe abélien $(\mathbb{Z}/q\mathbb{Z})^2$.

On en déduit $1 = h_x^{-1}\, h_{g,x}^{-1}\, h_{gx}\, h'_{g,x}$, qui est la formule de l'énoncé. Pour le (ii) fixons $g \in G$. Dans le groupe abélien H_{ab} on a par le (i)

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

car $x \mapsto gx$ étant une bijection de X on a $\prod_{x\in X} h_{gx} \equiv \prod_{x\in X} h_x$. Ainsi, $\mathrm{Ver}(g)$ ne dépend pas du choix de $x \mapsto \widetilde{x}$. Pour le (iii) on a

$$gg'\,\widehat{x} \;=\; \widehat{gg'x}\, h_{gg',x} \;\text{ et }\; gg'\,\widehat{x} \;=\; g\,\widehat{g'x}\, h_{g',x} \;=\; \widehat{gg'x}\, h_{g,g'x},$$

puis la relation de l'énoncé. Pour le (iv) fixons $g, g' \in G$. Comme H_{ab} est abélien on a

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

par le (iii). On a aussi $\prod_{x\in X} h_{g,g'x} = \prod_{x\in X} h_{g,x} = \mathrm{Ver}(g)$ par la bijection $X \to X, x \mapsto g'x$.

Exercice 6.26. (i) 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 $\mathbb{Z}/S \sim \Omega_i$ (formule orbite-stabilisateur). Ainsi, S_i est non nul, et donc de la forme $d_i\mathbb{Z}$ où d_i est le plus petit entier $n \geqslant 1$ avec $g^n g_i H = g_i H$, soit encore $g_i^{-1} g^n g_i \in H$, puis $d_i = |\mathbb{Z}/S| = |\Omega_i| = n_i$. De plus, les n_i éléments de Ω_i sont les $g^n g_i H$ avec $1 \leqslant n \leqslant n_i$. On choisit enfin pour représentants de X les éléments $x_{n,i} := g^n g_i$ avec $1 \leqslant n \leqslant n_i$. On peut calculer $\mathrm{Ver}(g)$ à l'aide de ce système de représentants par l'Exercice 6.25 (ii). On a $gx_{n,i} = x_{n+1,i}$ pour $n < n_i$, *autrement dit le* $h_{g,x_{n,i}}$ *vaut* 1, et

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

et donc $h_{g,x_{n_i,i}} = g_i^{-1} g^n g_i \in H$. On a donc bien $\mathrm{Ver}(g) \equiv \prod_i g_i^{-1} g^{n_i} g_i$. Pour le (ii), on a $g_i^{-1} g^{n_i} g_i \equiv g^{n_i}$ dans G_{ab}, et donc

$$\mathrm{Res}(\mathrm{Ver}(g)) \equiv \prod_i g^{n_i} = g^{\sum_i \Omega_i} = g^{|G/H|}.$$

Dans le cas G abélien on a $G = G_{\mathrm{ab}}$ et $H = H_{\mathrm{ab}}$ et on conclut par le (ii).

Exercice 6.27. (i) D'après le cours, on a $\mathrm{D}(\mathrm{S}_n) = \mathrm{A}_n$, et donc $(\mathrm{S}_n)_{\mathrm{ab}} \simeq \mathbb{Z}/2\mathbb{Z}$. On peut aussi raisonner directement de la manière suivante. On sait que S_n est engendré par les transpositions. Ainsi, son quotient $(\mathrm{S}_n)_{\mathrm{ab}}$ a la même propriété. Mais comme deux transpositions sont conjuguées dans S_n, elles ont même image dans $(\mathrm{S}_n)_{\mathrm{ab}}$. On en déduit que $(\mathrm{S}_n)_{\mathrm{ab}}$ est engendré par la classe de $(1\,2)$, et donc qu'il est donc soit trivial, soit $\simeq \mathbb{Z}/2\mathbb{Z}$. Il n'est pas trivial car la signature se factorise en un morphisme surjectif $(\mathrm{S}_n)_{\mathrm{ab}} \to \{\pm 1\}$.

(ii) Le morphisme $\mathrm{Res} : (\mathrm{S}_n)_{\mathrm{ab}} \to (\mathrm{S}_{n+1})_{\mathrm{ab}}$ envoie évidemment la classe de $(1\,2)$ sur celle de $(1\,2)$. D'après le (i), c'est donc un isomorphisme $\mathbb{Z}/2\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}/2\mathbb{Z}$.

(iii) Comme $\mathrm{Res} : (\mathrm{S}_n)_{\mathrm{ab}} \to (\mathrm{S}_{n+1})_{\mathrm{ab}}$ est un isomorphisme, il suffit de voir que $\mathrm{Res} \circ \mathrm{Ver} : (\mathrm{S}_{n+1})_{\mathrm{ab}} \to (\mathrm{S}_{n+1})_{\mathrm{ab}}$ est un isomorphisme pour n pair, nul pour n impair. Mais par l'Exercice 6.26 (ii), c'est l'endomorphisme $g \mapsto g^{n+1}$ d'un groupe d'ordre 2. Cela conclut.

Exercice 6.28. (i) 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 l'Exercice 6.15 (ii), g^n et $h\, g^n\, h^{-1}$ sont donc conjugués dans $\mathrm{N}_G(P)$. Ainsi, il existe $k \in \mathrm{N}_G(P)$ vérifiant $kg^nk^{-1} = h\, g^n\, h^{-1}$. Comme $g^n \in P$ est dans le centre de $\mathrm{N}_G(P)$ par l'hypothèse de l'exercice, on a $kg^nk^{-1} = g^n$, ce qui conclut.

Le (ii) est une conséquence directe du (i) de l'Exercice 6.26. Montrons le (iii). Posons $\varphi = \mathrm{Ver}_{|P} : P \to P$. On a $\varphi(g) = g^{|G/P|}$ par le (ii). C'est un morphisme de groupes

(simplement car P abélien), qui est injectif par Lagrange car $|G/P|$ est premier à $|P|$, et donc bijectif. Soit $N = \ker \mathrm{Ver}$, c'est un sous-groupe distingué de G. Les remarques juste faites 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 $\mathrm{Ver}(g) = \mathrm{Ver}(p)$ pour un certain $p \in P$ par surjectivité de φ, puis $gp^{-1} \in N$ et $g \in NP$. (On aurait aussi pu dire que φ^{-1} est une section de groupes de Ver).

Exercice 6.29. (i) Soit N le normalisateur de P dans G. Considérons le morphisme $\varphi : N \to \mathrm{Aut}(P), n \mapsto (\mathrm{int}_n)_{|P}$. Il est trivial sur P car P est abélien, et il se factorise donc en un morphisme $\overline{\varphi} : N/P \to \mathrm{Aut}(P), nP \mapsto (\mathrm{int}_n)_{|P}$. On a $P \simeq \mathbb{Z}/p^m\mathbb{Z}$ pour un certain $m \geqslant 1$, et donc $\mathrm{Aut}(P) \simeq (\mathbb{Z}/p^m\mathbb{Z})^\times$ 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 $|\mathrm{Aut}(P)|$, de sorte que tout morphisme $N/P \to \mathrm{Aut}(P)$ est trivial par Lagrange. Ainsi, $\overline{\varphi}$, puis φ, est trivial. Mais cela veut dire que P est dans le centre de N. Par Burnside (Exercice 6.28), P a un complément distingué dans G.

(ii) On a cette fois-ci $\mathrm{Aut}(P) \simeq \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ de cardinal $p(p-1)^2(p+1)$. 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 $\ell \leqslant p+1$, et donc $\ell = p+1$, $p = 2$ et $\ell = 3$.

(iii) 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 $G \simeq \mathbb{Z}/p\mathbb{Z}$). 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 le (i), on est donc dans ce second cas. Par le (ii), on a $p = 2$ et $3 \,|\, |G|$, puis $2^2 \cdot 3 = 12$ divise $|G|$.