Corrigé du Partiel du cours d'Algèbre 1, ENS Ulm, Mercredi 9 Novembre 2021

Problème 1. *Soit $n \geq 3$ un entier. On se propose dans ce problème de montrer que les automorphismes du groupe S_n sont intérieurs, sauf dans le cas $n = 6$. Une suite de r transpositions $t_1, \ldots, t_r$ de S_n sera dite* alignée *si on a $t_i\, t_j = t_j\, t_i$ pour $|j - i| > 1$, et $t_i\, t_{i+1} \neq t_{i+1}\, t_i$ pour $1 \leq i < r$.*

(i) Soient t et t' deux transpositions distinctes dans S_n, de supports respectifs T et T'. Vérifier que l'on a $t\,t' \neq t'\,t$ si, et seulement si, $|T \cap T'| = 1$.

On a $T \neq T'$ car t et t' sont distinctes. Il y a deux cas. Soit $T \cap T' = \emptyset$, auquel cas $tt' = t't$ car deux permutations à supports disjoints commutent. Soit $|T \cap T'| = 1$, et donc $T = \{a, b\}$ et $T' = \{a, c\}$ avec a, b, c distincts. Dans ce cas, on a $tt' = (a\, b)(a\, c) = (a\, c\, b)$ et $t't = (a\, c)(a\, b) = (a\, b\, c)$, et donc tt' et $t't$ diffèrent sur a.

(ii) Donner un exemple d'une suite alignée de $n - 1$ transpositions engendrant S_n.

On pose $t_i = (i\ i + 1)$. Par le (i) c'est une suite alignée. Par le cours, elle engendre S_n.

(iii) On suppose que $t_1, \ldots, t_r$ est une suite alignée de r transpositions distinctes de S_n. Montrer qu'il existe $a_1, a_2, \ldots, a_{r+1}$ distincts dans $\{1, \ldots, n\}$ avec $t_i = (a_i\ a_{i+1})$ pour tout $i = 1, \ldots, r$.

Par récurrence sur r. Il n'y a rien à montrer pour $r = 1$, et pour $r = 2$ c'est le (i) car t_1 et t_2 ne commutent pas. On suppose $r \geq 3$. Soient $a_1, a_2, \ldots, a_r$ distincts avec $t_i = (a_i\ a_{i+1})$ pour tout $i = 1, \ldots, r - 1$. Par hypothèse et $r \geq 3$, t_r commute avec $t_1, \ldots, t_{r-2}$, et donc le support de t_r ne contient aucun des a_i avec $1 \leq i \leq r - 1$ par le (i). Toujours par hypothèse, t_r ne commute pas avec t_{r-1}, donc le support de t_r contient soit a_r, soit a_{r-1}, par le (i). Mais on a vu qu'il ne contient pas a_{r-1}. Le support de t_r est donc de la forme $\{a_r, x\}$ avec $x \neq a_i$ pour tout $i \leq r$. On pose $a_{r+1} = x$.

(iv) Soit f un automorphisme de S_n. On suppose qu'il existe une transposition t telle que $f(t)$ est une transposition. Montrer que pour toute transposition s, alors $f(s)$ est une transposition.

Soit s une transposition dans S_n. Comme les transpositions sont conjuguées dans S_n, il existe $\sigma \in \mathrm{S}_n$ avec $s = \sigma t \sigma^{-1}$. On en déduit $f(s) = f(\sigma) f(t) f(\sigma)^{-1}$. Comme $f(t)$ est une transposition, l'élément $f(s)$ qui lui est conjugué en est aussi une.

(v) (suite) Montrer que f est un automorphisme intérieur.

On pose $s_i = (i\ i + 1)$ pour $1 \leq i < n$. On a $s_i s_j = s_j s_i$ si, et seulement si, $|i - j| > 1$ par le (ii). Par le (vi), $t_i := f(s_i)$ est une transposition pour tout $1 \leq i < n$. Comme f est bijective, on a $t_i t_j = f(s_i s_j) = f(s_i s_j) = t_j t_i$ si, et seulement si, $|i - j| > 1$. Par le (iii), il existe n éléments distincts $a_1, a_2, \ldots, a_n$ de $\{1, \ldots, n\}$ avec $t_i = (a_i\, a_{i+1})$ pour $i = 1, \ldots, r$. Ainsi, l'application $\sigma : \{1, \ldots, n\} \to \{1, \ldots, n\}, i \mapsto a_i$, est dans S_n. Par la formule de conjugaison des cycles, on a $f(s_i) = \sigma s_i \sigma^{-1}$. Comme les s_i engendrent S_n, on constate $f = \mathrm{int}_\sigma$.

On rappelle que le centralisateur d'un élément $\sigma \in \mathrm{S}_n$ est le sous-groupe $\mathrm{C}(\sigma) = \{\tau \in \mathrm{S}_n \mid \sigma\tau = \tau\sigma\}$.

(vi) *On suppose que $t \in \mathrm{S}_n$ est une transposition. Montrer* $\mathrm{C}(t) \simeq \mathrm{S}_2 \times \mathrm{S}_{n-2}$.

On suppose $t = (a\, b)$. Soit $\sigma \in \mathrm{S}_n$. On a $\sigma t \sigma^{-1} = (\sigma(a)\, \sigma(b))$. On en déduit que $\sigma t \sigma^{-1} = t$ si, et seulement si, $\sigma(\{a, b\}) = \{a, b\}$. Un tel σ préserve automatiquement le complémentaire I de $\{a, b\}$ dans $\{1, \ldots, n\}$. L'application $\mathrm{C}(t) \to \mathrm{S}_{\{a,b\}} \times \mathrm{S}_I, \sigma \mapsto (\sigma_{|\{a,b\}}, \sigma_I)$, est donc bijective. On conclut car c'est un morphisme de groupes et on a $\mathrm{S}_{\{a,b\}} \simeq \mathrm{S}_2$, ainsi que $\mathrm{S}_I \simeq \mathrm{S}_{n-2}$.

(vii) *Soit $s \in \mathrm{S}_n$ un élément d'ordre 2. Montrer qu'il existe un unique entier $1 \leq k \leq n/2$, tel que s est produit de k transpositions $s_1, \ldots, s_k$ à supports disjoints.*

L'ordre d'une permutation est le ppcm des longueurs des cycles de sa décomposition en cycles. Si ce ppcm est 2, c'est que tous ces cycles sont de longueur 2 (et qu'il y en a au moins 1).

(viii) *(suite) Soit $D = \langle s_1, \ldots, s_k \rangle$. Montrer que D est un sous-groupe de $\mathrm{C}(s)$ isomorphe à $(\mathbb{Z}/2\mathbb{Z})^k$.*

On a clairement $D \subset \mathrm{C}(s)$.Comme les s_i commutent et sont de carré 1, le groupe D est abélien 2-élémentaire. C'est donc un $\mathbb{Z}/2\mathbb{Z}$-espace vectoriel. Les t_i en constituent une base. En effet, ils sont générateurs par définition. Supposons que l'on a une relation $\prod_{i \in I} t_i = \mathrm{id}$ avec $I \subset \{1, \ldots, k\}$. Cela force $I = \emptyset$ car les t_i sont a supports disjoints.

(ix) *(suite) Montrer que D est distingué dans $\mathrm{C}(s)$.*

Pour $\sigma \in \mathrm{C}(s)$ on a $s = \sigma s \sigma^{-1} = (\sigma s_1 \sigma^{-1})(\sigma s_2 \sigma^{-1}) \cdots (\sigma s_n \sigma^{-1})$ et les $\sigma s_i \sigma^{-1}$ sont des transpositions à supports disjoints (images des supports des s_i par σ, par le cours). Par unicité de la décomposition en cycles, les ensembles des s_i et des $\sigma s_i \sigma^{-1}$ coïncident. On a donc $\sigma D \sigma^{-1} = \langle \sigma s_1 \sigma^{-1}, \ldots, \sigma s_k \sigma^{-1} \rangle = D$.

(x) *(suite) On suppose $n = 4$ et $k = 2$. Montrer $|\mathrm{C}(s)| > 4$.*

On a $s \in \mathrm{K}_4$. Comme K_4 est abélien, on a donc $\mathrm{K}_4 \subset \mathrm{C}(s)$. On conclut car $s_1 \in \mathrm{C}(s) \smallsetminus \mathrm{K}_4$.

(xi) *On suppose que $\mathbb{Z}/2\mathbb{Z} \times \mathrm{S}_m$ a un sous-groupe distingué isomorphe à $(\mathbb{Z}/2\mathbb{Z})^k$ avec $k \geq 2$ et $m \geq 3$. Montrer $m = 4$. On pourra considérer la projection naturelle $\mathbb{Z}/2\mathbb{Z} \times \mathrm{S}_m \to \mathrm{S}_m$.*

Regardons le morphisme surjectif $f : \mathbb{Z}/2\mathbb{Z} \times \mathrm{S}_m \to \mathrm{S}_m$. Soit H un sous-groupe distingué de $\mathbb{Z}/2\mathbb{Z} \times \mathrm{S}_m$ isomorphe à $(\mathbb{Z}/2\mathbb{Z})^k$. Comme f est surjectif, le sous-groupe $H' = f(H)$ est distingué dans S_m. Par le cours, c'est donc $\{1\}$, A_n, S_n, ou le sous-groupe K_4 dans le cas particulier $m = 4$. Mais on a $H \cap \ker f \subset \mathbb{Z}/2\mathbb{Z} \times \{0\}$, et donc $|H \cap \ker f| = 1$ ou 2. On en déduit que $H' \simeq H/(H \cap \ker f)$ est d'ordre 2^k ou 2^{k-1}, et donc $H' \neq \{1\}$. Pour $m \geq 3$, cela exclut S_m et A_m (leurs ordres sont multiples de 3). La seule possibilité est donc $m = 4$ et $H' = \mathrm{K}_4$.

(xii) *En déduire que pour $n \neq 6$, tout automorphisme de S_n est intérieur.*

Soit f un automorphisme de S_n. Soit t une transposition. Comme f est un isomorphisme, l'élément $s = f(t) \in \mathrm{S}_n$ est d'ordre 2. Par le (vii), s est un produit de k transpositions à supports disjoints par le (vii). On va montrer que pour $n \neq 6$ on a nécessairement $k = 1$, ce qui concluera par le (iv) et (v).

Noter que f induit aussi un isomorphisme $\mathrm{C}(t) \xrightarrow{\sim} \mathrm{C}(s)$, car pour $\tau \in \mathrm{S}_n$ on a $\tau t = t \tau \iff f(\tau)s = sf(\tau)$. Par le (vii), on a $\mathrm{C}(t) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathrm{S}_{n-2}$, et on sait aussi que $\mathrm{C}(t) \simeq \mathrm{C}(s)$ possède un sous-groupe distingué isomorphe à $(\mathbb{Z}/2\mathbb{Z})^k$. Supposant $k \geq 2$, le (xi) montre $m = n - 2 = 2$ ou $m = n - 2 = 4$. On peut donc supposer $n = 4$ et $k = 2$. Mais dans ce cas on a $|\mathrm{C}(t)| = 4$ et $|\mathrm{C}(s)| > 4$ par le (x) : une contradiction.

Dans les trois questions suivantes on étudie le cas $n = 6$.

(xii) *Montrer qu'il existe un sous-groupe H de S_6 qui est isomorphe à S_5, et dont l'action naturelle sur $\{1, 2, \ldots, 6\}$ est transitive.*

On rappelle que l'action de S_5 sur les 6 pentagones mystiques est transitive. Numérotant arbitrairement ces 6 pentagones, on en déduit un morphisme de groupes $f : \mathrm{S}_5 \to \mathrm{S}_6$ dont l'image H agit transitivement sur $\{1, \ldots, 6\}$. D'après le cours on sait qu'une action transitive de S_n sur $m > 2$ éléments avec $n > 4$ est fidèle (car les sous-groupes distingués d'un tel S_n sont $1, \mathrm{A}_n$ et S_n). On en déduit que f induit un isomorphisme $\mathrm{S}_5 \simeq H$.

(xiii) *(suite) En considérant l'action par translations de S_6 sur l'ensemble S_6/H, montrer qu'il existe un isomorphisme $f : \mathrm{S}_6 \to \mathrm{S}_6$ tel que $f(H) \subset \{\sigma \in \mathrm{S}_6 \mid \sigma(1) = 1\}$.*

(proche d'un argument vu en TD) Soient $G = \mathrm{S}_6$ et $X = G/H$ (ensemble des classes à gauche). On a $|H| = 5!$ et donc $|X| = |G|/|H| = 6!/5! = 6$. Le groupe G agit transitivement par translations sur l'ensemble X. D'après le cours, on sait qu'une action transitive de S_n sur $m > 2$ éléments avec $n > 4$ est fidèle. Le groupe $G = \mathrm{S}_6$ agit donc fidèlement sur X. Le sous-groupe $H \subset G$ fixe le point $H \in X$. Numérotons les éléments de X en attribuant à $H \in X$ le numéro 1, et arbitrairement les 5 autres. Le morphisme associé à l'action induit alors un morphisme injectif $f : \mathrm{S}_6 \to \mathrm{S}_6$ avec $f(H) \subset \{\sigma \in \mathrm{S}_6 \,|\, \sigma(1) = 1\}$. Mais f est bijectif, car injectif d'un semble fini dans lui-même : c'est un automorphisme de S_6.

(xiv) *(suite) Montrer que f n'est pas intérieur.*

Notons Γ_i le stabilisateur dans S_6 de l'élément i de $\{1, \ldots, 6\}$ pour l'action naturelle. On a $f(H) \subset \Gamma_1$ par le (xiii). Supposons $f = \mathrm{int}_\tau$ avec $\tau \in \mathrm{S}_6$. On en déduit $\tau H \tau^{-1} \subset \Gamma_1$ puis $H \subset \tau^{-1}\Gamma_1\tau = \Gamma_j$ avec $j := \tau^{-1}(1)$ (principe de conjugaison). Ainsi, H fixe l'élément $j \in \{1, \ldots, 6\}$ pour l'action naturelle, et n'agit donc pas transitivement sur ce dernier.

On note $\mathrm{Int}\,\mathrm{S}_n \subset \mathrm{Aut}\,\mathrm{S}_n$ le sous-ensemble des automorphismes intérieurs. Pour $k = 1, 2, 3$ on notera aussi T_k le sous-ensemble de S_6 constitué des produits de k transpositions à supports disjoints.

(xv) *Montrer que $\mathrm{Int}\,\mathrm{S}_n$ est un sous-groupe distingué de $\mathrm{Aut}\,\mathrm{S}_n$, et qu'il est isomorphe à S_n.*

Considérons l'application $f : \mathrm{S}_n \to \mathrm{Aut}\,\mathrm{S}_n$, $\sigma \mapsto \mathrm{int}_\sigma$. On a $\mathrm{int}_\sigma \circ \mathrm{int}_{\sigma'} = \mathrm{int}_{\sigma\sigma'}$ pour tout $\sigma, \sigma' \in \mathrm{S}_n$: l'application f est un morphisme de groupes. Son image $\mathrm{Int}\,\mathrm{S}_n$ est donc un sous-groupe de $\mathrm{Aut}\,\mathrm{S}_n$. La formule $g \circ \mathrm{int}_\sigma \circ g^{-1} = \mathrm{int}_{g(\sigma)}$ pour $\sigma \in \mathrm{S}_n$ et $g \in \mathrm{Aut}\mathrm{S}_n$ montre qu'il est distingué. Il ne reste qu'à vérifier que l'on a $\ker f = \{1\}$, c'est à dire que le centre de S_n est trivial. (Jusqu'ici, l'argument a déjà été vu en TD). Soit σ dans le centre de S_n. On a $\sigma(i\,j)\sigma^{-1} = (\sigma(i)\,\sigma(j)) = (i\,j)$ pour tout $i < j$, et donc σ préserve tous les couples $\{i, j\}$ avec $i \neq j$. Comme $n > 2$ cela montre $\sigma = 1$.

(xvi) *Déterminer $|T_k|$ pour $k = 1, 2, 3$.*

Par unicité de la décomposition en cycles on a

$$|T_1| = \binom{6}{2} = 15, \quad |T_2| = \frac{1}{2!} \cdot \binom{6}{2} \cdot \binom{4}{2} = 45 \text{ et } |T_3| = \frac{1}{3!} \cdot \binom{6}{2} \cdot \binom{4}{2} \cdot \binom{2}{2} = 15.$$

(xvii) *En déduire que pour* $f \in \mathrm{Aut}\,\mathrm{S}_6$ *non intérieur on a* $f(T_2) = T_2$, $f(T_1) = T_3$ *et* $f(T_3) = T_1$.

Pour k fixé, les éléments de T_k sont conjugués d'après le cours. On en déduit que pour tout i, il existe j tel que $f(T_i) \subset T_j$. Comme f est injective, on a forcément $f(T_2) = T_2$ par le (xvi), puis soit $f(T_1) = T_1$ et $f(T_3) = T_3$, soit $f(T_1) = T_3$ et $f(T_3) = T_1$. Dans le premier cas, f est intérieur par le (iv)-(v).

(xviii) *Montrer* $\mathrm{Aut}\,\mathrm{S}_6/\mathrm{Int}\,\mathrm{S}_6 \simeq \mathbb{Z}/2\mathbb{Z}$.

Si f et g sont deux automorphismes de S_6 non intérieurs, on a $f \circ g(T_1) = f(g(T_1)) = f(T_3) = T_1$ d'après le (xvi), et donc $f \circ g$ est intérieur. Comme f^{-1} est aussi non intérieur, on en déduit $g \in f\,\mathrm{Int}\,\mathrm{S}_6$.

Problème 2. *Soit p un nombre premier impair. On se propose de classifier, à isomorphisme près, les groupes d'ordre $4p$. On commence par quelques questions préliminaires.*

(i) *Déterminer, à isomorphisme près, les groupes abéliens d'ordre $4p$.*

Soient $a_1, \ldots, a_n$ les facteurs invariants d'un tel groupe. On a $1 < a_1 \,|\, a_2 \,|\, \cdots \,|\, a_n$ et $4p = a_1 \ldots a_n$. Comme $4p$ est sans facteur cube, on a $n \leq 2$, et comme p^2 ne divise pas $4p$ car p est impair, on a que p ne divise pas a_1. Les seules possibilités sont donc $n = 1$ et $a_1 = 4p$, ou $n = 2$ et $(a_1, a_2) = (2, 2p)$. Par le cours, il y a donc exactement deux groupes abéliens d'ordre p à isomorphisme près, à savoir $\mathbb{Z}/4p\mathbb{Z}$ et $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2p\mathbb{Z}$.

(ii) *Montrer que tout groupe d'ordre 4 est isomorphe à $\mathbb{Z}/4\mathbb{Z}$ ou à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.*

Soit Q d'ordre 4 non cyclique. On a $x^2 = 1$, et donc $x^{-1} = x$, pour tout $x \in Q$. On sait qu'un tel Q est abélien car on a $xy = x^{-1}y^{-1} = (yx)^{-1} = yx$. Il est donc abélien élémentaire, isomorphe à $(\mathbb{Z}/2\mathbb{Z})^2$.

(iii) *Soient G un groupe d'ordre mn avec $(m, n) = 1$ et N un sous-groupe distingué de G d'ordre n. Montrer que N est l'unique sous-groupe de G d'ordre n On pourra considérer la projection canonique $G \to G/N$.*

Soit N' un sous-groupe de G d'ordre n. Regardons la projection canonique $\pi : G \to G/N$. Pour $x \in N'$ on a $x^n = 1$ par Lagrange, et donc $\pi(x)^n = 1$. Mais on a aussi $m = |G/N|$ et donc $\pi(x)^m = 1$ par Largrange. Ainsi, l'ordre de $\pi(x)$ divise n et m : c'est donc 1, puis $\pi(x) = 1$. On a montré $\pi(N') = 1$, et donc $N' \subset N$, puis $N' = N$.

(iv) *Montrer que tout groupe d'ordre $2p$ contient un unique sous-groupe d'ordre p.*

Un groupe G d'ordre $2p$ contient un sous-groupe P d'ordre p par Cauchy. Il est d'indice 2 donc distingué. On a p impair, donc P est l'unique sous-groupe d'ordre p de G par le (iii).

Dans les questions (v) à (viii) qui suivent, on suppose que G est un groupe d'ordre $4p$ ne possèdant pas de sous-groupe distingué d'ordre p. On veut montrer $p = 3$ et $G \simeq \mathrm{A}_4$. Pour cela, on fixe $x \in G$ d'ordre p (il en existe par Cauchy) et on note $C \subset G$ la classe de conjugaison de x.

(v) *Montrer* $|C| \neq 1$ *et* $|C| \,|\, 4$.

On a $x \in C$ *et donc* $|C| = 1$ *si et seulement si,* $\sigma x \sigma^{-1} = x$ *pour tout* $\sigma \in G$. *Cela implique* $\langle x \rangle \triangleleft G$ *(et même que* x *est central). La formule orbite stabilisateur pour l'action de conjugaison de* G *sur* C *montre* $4p = |G| = |C||G_x|$ *où* $G_x = \{g \in G \mid gx = xg\}$ *est le centralisateur de* x *dans* G. *C'est un sous-groupe de* G *contenant* $\langle x \rangle$. *On a donc* $p \mid |G_x|$ *puis* $|C| \,|\, 4$.

(vi) *Montrer que* G *ne possède pas de sous-groupe d'ordre* $2p$.

Soit H *un sous-groupe distingué de* G *d'ordre* $2p$. *Alors* H *est d'indice* 2 *dans* G, *donc distingué dans* G. *Mais* H *est d'ordre* $2p$, *donc possède un unique sous-groupe d'ordre* p, *disons* P, *par le (iv). Pour* $g \in G$, *on a donc* $gPg^{-1} \subset gHg^{-1} = H$, *et donc* $gPg^{-1} = P$ *par l'unicité susmentionnée, car on a* $|gPg^{-1}| = |P|$ *(image de* P *par une bijection).*

(vii) *En déduire* $|C| = 4$ *et que l'action de* G *par conjugaison sur* C *est fidèle.*

Revenans à la preuve du (ii), on a $|G_x| \neq 2p$ *par le (vi), et on a vu* $p \,|\, |G_x|$, *on a donc soit* $|G_x| = p$ *et* $|C| = 4$, *soit* $|G_x| = 4p$ *et* $|C| = 1$. *Ce dernier cas est exclus par le (v). On a donc* $|C| = 4$, *et le noyau de l'action* K *de* G *sur* C *vérifie* $K \subset G_x$ *et* $K \triangleleft G$. *On a donc* $|K| \mid |G_x| = p$ *(Lagrange), puis* $K = 1$ *car* G *n'a pas de sous-groupe distingué d'ordre* p.

(viii) *Conclure.*

Par le (vii), on a un morphisme injectif $G \to \mathrm{S}_4$. *On a donc* $4p = |G| \,|\, |\mathrm{S}_4| = 24$. *On en déduit* $p = 3$, $|G| = 12$. *Un sous-groupe d'indice* 2 *de* S_4 *est forcément distingué, et égal à* A_4 *par le cours (ou plus généralement car le seul sous-groupe d'indice* 2 *de* S_n *est* A_n, *par un argument vu en TD).*

On suppose désormais que G *est un groupe* <u>*non abélien*</u> *d'ordre* $4p$, *et que* P *est un sous-groupe distingué d'ordre* p *de* G. *On fixe aussi un sous-groupe* Q *de* G *d'ordre* 4. *Il en existe par le premier théorème de Sylow vu en cours.*

(ix) *Montrer que* Q *est un complément de* P *et que* $Q \to \mathrm{Aut}(P), q \mapsto (\mathrm{int}_q)_{|P}$, *est un morphisme de groupes bien défini et non trivial.*

Le sous-groupe $P \cap Q$ *est trivial car son ordre divise* $4 = |Q|$ *et* $p = |P|$ *(Lagrange). On a* $|P||Q| = 4p = |G|$. *On en déduit que* P *et* Q *sont complément l'un de l'autre. Le morphisme de l'énoncé est bien défini car* P *est distingué dans* G. *Si ce morphisme est trivial, on a* $pq = qp$ *pour tout* $p \in P$ *et* $q \in Q$. *Mais* P *est abélien (car cyclique) et* Q *est aussi abélien par le (ii). Comme* $G = PQ$ *on aurait alors* G *abélien : absurde.*

(x) *Soit* V *un groupe abélien* 2-*élémentaire d'ordre* 4, C *un groupe cyclique, et* $f : V \to C$ *un morphisme de groupes. Montrer qu'il existe une base* v, w *de* $V^\sharp$ *avec* $f(v) = 1$.

Comme C *est cyclique, il a au plus un élément d'ordre* 2. *Comme on a* $v^2 = 1$ *pour tout* $v \in V$, *et donc* $f(v)^2 = 1$, *on en déduit* $|f(V)| \leq 2$. *On en déduit que* $\ker f$ *est non trivial. On choisit* v *non nul dans* $\ker f$, *et on la complète en une base du* $\mathbb{Z}/2\mathbb{Z}$-*espace vectoriel* v, w *de* W *pour répondre à la question.*

(xi) *On suppose $Q \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Montrer que l'on a $G \simeq \mathbb{Z}/2\mathbb{Z} \times H$ pour un certain groupe H, puis que l'on a un isomorphisme $H \simeq \mathrm{D}_{2p}$.*

On applique la question précédente à $V = Q$ au morphisme $f : Q \to \mathrm{Aut}(P)$. C'est possible car on sait que l'on a $\mathrm{Aut}(P) \simeq (\mathbb{Z}/p\mathbb{Z})^\times$ et que ce dernier est cyclique par Gauss. Ainsi, il existe une base v, w de $Q^\sharp$ telle que $vxv^{-1} = x$ pour tout $x \in P$. Comme v et w commutent, le (ix) montre que v est dans le centre de G.

Posons $D = \langle v \rangle \simeq \mathbb{Z}/2\mathbb{Z}$ et $H = P\langle w \rangle$. Comme P est distingué dans G, H est un sous-groupe de G. Par le (ix), on a $|H| = 2p$ et $D \cap H = \{1\}$. On a vu que l'on a $dh = hd$ pour tout $d \in D$ et $h \in H$. Ainsi, G est produit direct interne de D et H. On a donc $G \simeq D \times H$. Le groupe H est d'ordre $2p$, et non abélien sinon G serait abélien. On sait par le cours que cela entraîne $H \simeq \mathrm{D}_{2p}$.

On suppose finalement $Q \simeq \mathbb{Z}/4\mathbb{Z}$, et dans les questions (xii) à (xiv) on suppose en outre $p \equiv 3 \bmod 4$.

(xii) *Montrer qu'il existe un unique morphisme non trivial $\alpha : \mathbb{Z}/4\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/p\mathbb{Z})$.*

Soit g un générateur de $\mathbb{Z}/4\mathbb{Z}$. Se donner un morphisme $\mathbb{Z}/4\mathbb{Z} \to \mathrm{Aut}\,\mathbb{Z}/p\mathbb{Z}$ est la même chose que se donner l'image du générateur g, qui peut être n'importe quel élément $a \in \mathrm{Aut}\,\mathbb{Z}/p\mathbb{Z}$ vérifiant $a^4 = 1$ (propriété universelle du groupe quotient $\mathbb{Z}/4\mathbb{Z}$). On sait que tout automorphisme de $\mathbb{Z}/p\mathbb{Z}$ est de la forme $\varphi_k : x \mapsto kx$, avec $k \in (\mathbb{Z}/p\mathbb{Z})^\times$. On a $\varphi_k^4 = \varphi_{k^4} = 1$ si, et seulement si, $k^4 = 1$ dans $(\mathbb{Z}/p\mathbb{Z})^\times$. Mais $(\mathbb{Z}/p\mathbb{Z})^\times$ n'a pas d'élément d'ordre 4, car sinon on aurait $4 \mid p-1$ par Lagrange. On a donc $k^4 = 1$ si, et seulement si, $k^2 = 1$, ou ce qui revient au même, $k = \pm 1$. L'unique morphisme non trivial $\mathbb{Z}/4\mathbb{Z} \to \mathrm{Aut}\,\mathbb{Z}/p\mathbb{Z}$ est donc celui envoyant g sur φ_{-1} (i.e. $x \mapsto -x$).

(xiii) *Montrer $G \simeq \mathbb{Z}/p\mathbb{Z} \rtimes_\alpha \mathbb{Z}/4\mathbb{Z}$.*

On sait que G est produit semi-direct interne de P par Q par le (ix), pour un morphisme non trivial $Q \to \mathrm{Aut} P$. On a donc $G \simeq \mathbb{Z}/p\mathbb{Z} \rtimes_\beta \mathbb{Z}/4\mathbb{Z}$ avec $\beta : \mathbb{Z}/4\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/p\mathbb{Z})$, et sans suivre précisément les isomorphismes choisis $P \simeq \mathbb{Z}/p\mathbb{Z}$ et $Q \simeq \mathbb{Z}/4\mathbb{Z}$ on sait que β est non trivial. On a donc $\beta = \alpha$ par le (xiii).

(xiv) *En déduire que tout groupe non abélien d'ordre $4p$ est isomorphe à un, et un seul, des groupes suivants : $\mathbb{Z}/2\mathbb{Z} \times \mathrm{D}_{2p}$, $\mathbb{Z}/p\mathbb{Z} \rtimes_\alpha \mathbb{Z}/4\mathbb{Z}$ ou A_4 (cas $p = 3$).*

Soit G un groupe non abélien d'ordre $4p$. On a montré que si G n'a pas de sous-groupe distingué d'ordre p, alors on a $p = 3$ et $G \simeq \mathrm{A}_4$ au (viii). Réciproquement, A_4 est bien d'ordre 12 et sans sous-groupe d'ordre 3 distingué.

On a aussi montré que si G a un sous-groupe distingué P d'ordre p, alors ce sous-groupe est unique par le (iii), que tout 2-Sylow Q de G est un complément de P par (ix), et qu'en particulier un tel Q est isomorphe à G/P. On a vu au (ii) qu'on a soit $Q \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, auquel cas on a $G \simeq \mathbb{Z}/2\mathbb{Z} \times \mathrm{D}_{2p}$ par le (xi), soit $Q \simeq \mathbb{Z}/4\mathbb{Z}$, auquel cas on a $G \simeq \mathbb{Z}/p\mathbb{Z} \rtimes_\alpha \mathbb{Z}/4\mathbb{Z}$ par le (xiii). On conclut car il est clair que $\mathbb{Z}/2\mathbb{Z} \times \mathrm{D}_{2p}$ possède $0 \times C$ pour sous-groupe distingué d'ordre p et pour complément $\mathbb{Z}/2\mathbb{Z} \times \langle \tau \rangle \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, et que $\mathbb{Z}/p\mathbb{Z} \rtimes_\alpha \mathbb{Z}/4\mathbb{Z}$ possède $\mathbb{Z}/p\mathbb{Z} \times \{0\}$ pour sous-groupe distingué d'ordre p et pour complément $\{0\} \times \mathbb{Z}4\mathbb{Z} \simeq \mathbb{Z}/4\mathbb{Z}$.

(xv) *On suppose enfin $p \equiv 1 \bmod 4$. Comment la classification du (xiv) est-elle modifiée ?*

Pour $p \equiv 1 \bmod 4$, il existe exactement 4 élément $k \in (\mathbb{Z}/p\mathbb{Z})^\times$ tels que $k^4 = 1$, à savoir ± 1, et $\pm i$ avec $i^2 = -1$. L'argument du (xii) montre qu'il existe alors deux autres morphismes non *triviaux* $\beta_1, \beta_2 : \mathbb{Z}/4\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/p\mathbb{Z})$*, l'un envoyant le générateur* g *sur* φ_i*, et l'autre* g *sur* $\varphi_{-i} = \varphi_i^{-1}$*. L'argument du (iii) montre qu'une possibilité supplémentaire est que l'un des deux générateurs* g *de* Q *satisfait* $ghg^{-1} = h^i$ *pour tout* $h \in P$ *(l'autre générateur* g^{-1} *satisfaisant alors* $g^{-1}hg = h^{-i}$*). Par suivi des isomorphismes, on en déduit* $G \simeq \mathbb{Z}/p\mathbb{Z} \rtimes_{\beta_1} \mathbb{Z}/4\mathbb{Z} \simeq \mathbb{Z}/p\mathbb{Z} \rtimes_{\beta_2} \mathbb{Z}/4\mathbb{Z}$*. C'est l'unique groupe à ajouter à la liste. Il admet un (unique) sous-groupe distingué* P *d'ordre* p *avec un groupe* $\simeq \mathbb{Z}/4\mathbb{Z}$ *pour complément, mais il n'est pas isomorphe à* $G' = \mathbb{Z}/p\mathbb{Z} \rtimes_\alpha \mathbb{Z}/4\mathbb{Z}$*. En effet, l'image de* $G \to \mathrm{Aut}(P)$ *contient un élément d'ordre 4, et pas celle de* $G' \to \mathrm{Aut}(P)$*.*

(xvi) (Bonus) Lequel des groupes ci-dessus est isomorphe à D_{4p} *?*

Soient $G = \mathrm{D}_{4p}$*,* $c = (1\,2\,\ldots\,2p)$ *et* $\tau = (1\ 2p)(2\ 2p-1)\cdots(p\ p+1)$*. On sait que le sous-groupe* $C = \langle c \rangle$ *de* G *est distingué d'ordre* $2p$ *et* $\tau c = c^{-1}\tau$*. L'unique sous-groupe d'ordre* p *de* C*, engendré par* c^2*, est aussi distingué dans* G*. Mais* C *contient l'élément* c^p *qui est d'ordre 2. On a donc* $\tau c^p = c^{-p}\tau = c^p\tau$*. Ainsi,* τ *et* c^p *engendrent un sous-groupe de* G *isomorphe à* $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$*. D'après le (xi) on a donc* $\mathrm{D}_{4p} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathrm{D}_{2p}$*.*