Corrigé du Partiel du cours d'Algèbre 1, ENS Ulm, Mercredi 10 Novembre 2021

Problème 1. *On s'intéresse aux actions transitives de* S_4 *sur un ensemble à* 6 *éléments. On note* X *l'ensemble des parties à* 2 *éléments de* $\{1,2,3,4\}$*, et* Y *l'ensemble des* 4*-cycles dans* S_4*.*

(i) Montrer $|X| = |Y| = 6$*.*

On a $|X| = \binom{4}{2} = 6$*. Un* 4*-cycle dans* S_4 *s'écrit de manière unique sous la forme* $(1\,a\,b\,c)$ *avec* $\{a,b,c\} = \{2,3,4\}$*. Il en a donc* $|Y| = 3! = 6$*.*

(ii) Montrer que l'action naturelle de S_4 *sur* X *est transitive, et lister les éléments du stabilisateur de* $\{i,j\} \in X$*.*

L'action de $G = \mathrm{S}_4$ *sur* $\{1,2,3,4\}$ *est* 2*-transitive, donc celle sur* X *est transitive. Un élément* $\sigma \in \mathrm{S}_4$ *fixe* $x = \{i,j\}$ *ssi on a* $\sigma(\{i,j\}) = \{i,j\}$*. On note les deux autres élément de* $\{1,2,3,4\}$ *par* k *et* l*. On a donc manifestement* $G_x = \{1, (i\,j), (k\,l), (i\,j)(k\,l)\}$*. On peut aussi dire que l'inclusion* $\supset$ *est claire et que pour* $x \in X$ *on a* $|G_x| = |G|/|\mathrm{O}_x| = |G|/|X| = 24/6 = 4$*.*

(iii) Montrer que l'action par conjugaison de S_4 *sur* Y *est transitive, puis que le stabilisateur d'un* 4*-cycle* $c \in Y$ *est* $\langle c \rangle$*.*

On sait que le conjugué d'un k*-cycle est un* k*-cycle, et que deux* k*-cycles de* S_n *sont conjugués (par* k*-transitivité), donc l'action par conjugaison de* S_4 *sur* Y *est bien définie et transitive. Le raisonnement ci-dessus montre que pour* $c \in Y$ *on a* $|G_c| = 4$*. On conclut car on a* $ccc^{-1} = c$*, et donc* $\langle c \rangle \subset G_c$*.*

(iv) Montrer que ces actions de S_4 *sur* X *et* Y *sont fidèles.*

Vu la description des G_x *pour* $x \in X$*, il est clair qu'aucun élément non trivial de* S_4 *n'est dans* $G_{\{i,j\}}$ *pour toute partie à* 2 *éléments* $\{i,j\} \in X$*. Par exemple, pour* i,j,k *distincts on a* $G_{\{i,j\}} \cap G_{\{i,k\}} = \{1\}$*. De même, pour* $c = (i\,j\,k\,l) \in Y$ *on a* $G_c = \{1, (i\,j\,k\,l), (i\,k)(j\,l), (i\,l\,k\,l)\}$ *et donc* $G_c \cap G_{c'} = \{1\}$ *avec* $c' = (i\,j\,l\,k)$*.*

(v) Montrer qu'il existe une action transitive de S_3 *sur un ensemble à* 6 *éléments, et décrire ses stabilisateurs.*

L'action de $G = \mathrm{S}_3$ *sur* $Z = G$ *(lui-même) par translations à gauche convient (action de Cayley). Elle est bien transitive car pour* $g, g' \in G$*, on a* $g' = (g'g^{-1})g$*. Ses stabilisateurs sont triviaux car pour* $h \in G$*, on a* $gh = h$ *si, et seulement si,* $g = 1$*.*

(vi) (suite) En déduire une action transitive de S_4 *sur* Z*, dont les stabilisateurs sont tous égaux au sous-groupe* K_4 *de* S_4*.*

On a un morphisme surjectif $f : \mathrm{S}_4 \to \mathrm{S}_3$ *de noyau* K_4*. On en déduit que* $(g,z) \mapsto f(g)z, \mathrm{S}_4 \times Z \to Z$*, est une action transitive de* S_4 *sur l'ensemble à* 6 *éléments* S_3*. L'élément* $g \in \mathrm{S}_4$ *stabilise* $z \in Z$ *si, et seulement si,* $f(g) \in \mathrm{S}_3$ *stabilise* z*, et donc* $f(g) = 1$ *par la question précédente.*

(vii) *Rappeler pourquoi tout groupe d'ordre* 4 *est isomorphe à* $\mathbb{Z}/4\mathbb{Z}$ *ou à* $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Si G *est d'ordre* 4 *alors soit* G *a un élément d'ordre* 4, *et donc* $G \simeq \mathbb{Z}/4\mathbb{Z}$, *soit tout élément de* G *est d'ordre* 1 *ou* 2 *(Lagrange). Mais* $g^2 = 1$ *pour tout* $g \in G$ *implique* G *abélien car alors* $[g,h] = ghgh = (gh)^2 = 1$ *pour tout* g, h. *Dans ce cas,* G *est un groupe abélien* 2*-élémentaire, et donc* $\simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

(viii) *Déterminer le commutant dans* S_4 *(ou « centralisateur ») de la transposition* $(i\,j)$.

Un élément $\sigma \in \mathrm{S}_4$ *commute avec la transposition* $(i\,j)$ *si et seulement si on a* $(\sigma(i)\,\sigma(i)) = \sigma(i\,j)\sigma^{-1} = (i\,j)$, *ou ce qui revient au même, si et seulement si* $\sigma(\{i,j\}) = \{i,j\}$. *Le commutant cherché est donc* $G_{\{i,j\}}$.

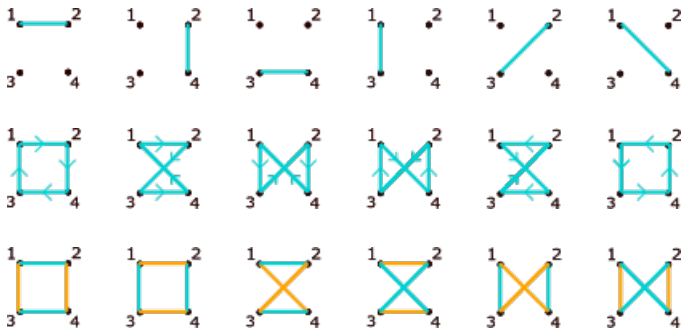
(ix) *Soit* $H \subset \mathrm{S}_4$ *un sous-groupe d'ordre* 4. *Montrer que soit* H *est le stabilisateur d'un point de* X, *soit* H *est le stabilisateur d'un point de* Y, *soit* H *est le sous-groupe* K_4 *de* S_4.

Si H *est cyclique d'ordre* 4, *il est engendré par un élément d'ordre* 4 *dans* S_4. *Vu les types possibles d'éléments* (4, $3+1$, $2+2$, $2+1+1$, $1+1+1+1$), *les éléments d'ordre* 4 *de* S_4 *sont les* 4*-cycles. On a donc* $H = G_c$ *pour un* $c \in Y$ *d'après la question (ii). Sinon on a* $H \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. *Si* H *ne contient aucune transposition, on a nécessairement* $H = \mathrm{K}_4 = \{1, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}$. *Si* H *contient* $(i\,j)$, *on a* H *inclus dans le commutant de* $(i\,j)$ *(car* H *est commutatif), puis* $H = G_{(i\,j)}$ *par la question précédente.*

(x) *En déduire qu'à isomorphisme près, il existe exactement* 3 *actions transitives de* S_4 *sur des ensembles à* 6 *éléments.*

Une action transitive de $G = \mathrm{S}_4$ *sur un ensemble à* 6 *éléments a ses stabilisateurs qui sont des sous-groupes d'ordre* $|G|/6 = 4$. *De plus, par un résultat du cours, deux actions transitives de* G *sont isomorphes si, et seulement si, elles possèdent un stabilisateur en commun. La question précédente, ainsi que (ii), (iii) et (vi), montrent donc que tout action de* G *sur un ensemble à* 6 *éléments est isomorphe à* X, Y *ou* Z. *Ces actions sont non isomorphes entre elles car les stabilisateurs de* X, Y *et* Z *sont tous différents : ceux de* Y *contiennent un* 4*-cycle, ceux de* X *une transposition, et ceux non triviaux de* Z *uniquement des double-transpositions.*

(xi) *Faire correspondre ces trois actions aux dessins ci-dessous.*



La première ligne représente les parties à 2 *éléments de* $\{1,2,3,4\}$ *: c'est* X. *La seconde représente les* 4*-cycles de* S_4, *c'est* Y. *La troisième ligne définit manifestement une action transitive de* S_4 *telle que les doubles transpositions agissent trivialement, c'est donc l'action de noyau* K_4.

(xii) *(Bonus) Identifions* S_4 *au sous-groupe de* S_5 *fixant l'élément* 5. *Est-ce que la restriction à* S_4 *de l'action exotique de* S_5 *est transitive ? Si oui, l'identifier à l'une des* 3 *actions ci-dessus.*

Soit H *le stabilisateur dans* S_4 *du pentagone* P *contenant le* 5*-cycle* $(1\,2\,3\,4\,5)$ *(sans poisson dans l'illustration du cours). C'est l'ensemble des* $\sigma \in \mathrm{S}_4$ *tels que* $(\sigma(1)\,\sigma(2)\,\sigma(3)\,\sigma(4)\,5)$ *est l'un des quatre* 5*-cycles de* $\langle(1\,2\,3\,4\,5)\rangle$. *Le cycle* $(1\,2\,3\,4\,5)$ *correspond à* $\sigma = \mathrm{id}$, *le cycle* $(4\,3\,2\,1\,5)$ *à* $\sigma = (1\,4)(3\,2)$, *le cycle* $(3\,1\,4\,2\,5)$ *à* $\sigma = (1\,3\,4\,2)$, *et le cycle* $(2\,4\,1\,3\,5)$ *à* $\sigma = (1\,2\,4\,3)$. *En particulier,* H *est d'ordre* 4, *donc l'orbite du pentagone* P *a* $6 = 24/4$ *éléments : l'action est transitive. On a reconnu que* H *est le stabilisateur du* 4*-cycle* $(1\,2\,4\,3)$ *dans* Y. *C'est donc l'action du milieu.*

Problème 2. (Non simplicité d'un groupe non abélien minimal) *Soit* G *un groupe fini non abélien dont tous les sous-groupes stricts sont abéliens. On se propose de montrer que* G *n'est pas simple.*

On suppose par l'absurde que G *est simple. On note* $\mathcal{M}$ *l'ensemble des sous-groupes maximaux de* G.

(i) *Soient* A *et* B *deux sous-groupes stricts de* G, *montrer que* $\mathrm{N}_G(A \cap B)$ *contient* A *et* B.

Le groupe $A \cap B$ *est inclus dans* A, *qui est abélien car* A *est strict, donc on a* $A \cap B \lhd A$, *i.e.* $A \subset \mathrm{N}_G(A \cap B)$. *Par symétrie on a aussi* $B \subset \mathrm{N}_G(A \cap B)$.

(ii) *En déduire que pour* $A, B \in \mathcal{M}$ *avec* $A \neq B$, *on a* $A \cap B = \{1\}$.

Le sous-groupe engendré par A *et* B *est* $\neq A$, *sinon* $B \subset A$ *puis* $B = A$ *par maximalité de* B. *Il est donc alors égal à* G *par maximalité de* A. *On a donc* $\mathrm{N}_G(A \cap B) = G$ *par le (i), i.e.* $A \cap B$ *est distingué dans* G. *Comme* $A \cap B \subset A \neq G$, *on a* $A \cap B = \{1\}$ *car* G *est simple.*

(iii) *Montrer que* $(g, A) \mapsto gAg^{-1}$ *définit une action de* G *sur* $\mathcal{M}$.

L'application int_g *est un automorphisme du groupe* G, *elle envoit donc sous-groupe maximal sur sous-groupe maximal. La vérification que c'est une action est immédiate.*

(iv) *Montrer que l'orbite de* $A \in \mathcal{M}$ *est de cardinal* $|G|/|A|$.

Par la formule orbite-stabilisateur, il suffit de montrer que le stabilisateur de A *est* A. *Mais par définition c'est* $\mathrm{N}_G(A)$, *et on a* $A \subset \mathrm{N}_G(A)$. *Comme* A *est maximal, on a soit* $A = \mathrm{N}_G(A)$, *soit* $\mathrm{N}_G(A) = G$ *i.e.* $A \lhd G$. *Dans ce second cas, on a* $A = \{1\}$ *car* G *est simple. Mais* $\{1\}$ *n'est pas maximal, car pour* $x \in G \neq \{1\}$ *on a* $\{1\} \subsetneq x \subsetneq G$ *(la seconde inclusion est stricte car* G *n'est pas abélien). (Il faut faire attention à ce que* $\mathbb{Z}/p\mathbb{Z}$ *est simple et abélien !).*

(v) *Pour* $A \in \mathcal{M}$, *on pose* $\mathcal{C}(A) = \bigcup_{g \in G} gAg^{-1}$. *Montrer* $|\mathcal{C}(A)| = 1 + \frac{|G|}{|A|}(|A| - 1)$.

Par le (iv), dans cette réunion il y a $|G|/|A|$ *conjugués distincts de* A. *Ces conjugués sont isomorphes entre eux, donc ont même cardinal* $|A|$. *Les intersections 2 à 2 sont triviales d'après le (ii). Comptant l'élément neutre à part, et pour chacun de ces conjugués les* $|A| - 1$ *éléments non triviaux, on obtient la formule de l'énoncé.*

(vi) *(suite) En déduire* $1 + \frac{|G|}{2} \leq |\mathcal{C}(A)| < |G|$.

Pour $n = |G|$ *et* $a = |A|$ *on a* $1 + \frac{n}{a}(a - 1) = n + 1 - n/a$ *avec* $a | n$ *et* $n > a$, *d'où* $n/a \geq 2$ *et* $|\mathcal{C}(A)| < n$. *On a déjà vu que* $\{1\}$ *n'est pas maximal plus haut. On en déduit* $a \geq 2$, *puis* $\frac{n}{a}(a - 1) = n(1 - 1/a) \geq \frac{n}{2}$.

(vii) *Montrer que pour $A, B \in \mathcal{M}$, avec B non inclus dans $\mathcal{C}(A)$, on a $\mathcal{C}(A) \cap \mathcal{C}(B) = \{1\}$.*

Si B n'est pas inclus dans $\mathcal{C}(A)$, on a en particulier $B \neq gAg^{-1}$ pour tout $g \in G$, puis $hBh^{-1} \neq gAg^{-1}$ pour tout $h, g \in G$, ce qui implique $hBh^{-1} \cap gAg^{-1} = \{1\}$ par le (ii). Le résultat s'en déduit.

(viii) *Conclure.*

On sait que $\mathcal{M}$ est non vide (on a $G \neq \{1\}$, donc on peut considérer un sous-groupe maximal contenant 1). Soit $A \in \mathcal{M}$. On a $\mathcal{C}(A) \neq G$ par le (vi). Soit $g \notin \mathcal{C}(A)$. On a $\langle g \rangle \neq G$ car G n'est pas abélien. Ainsi, $\langle g \rangle$ s'inclut dans un sous-groupe maximal B, et on a $g \in B \smallsetminus \mathcal{C}(A)$. On a donc $|\mathcal{C}(A) \cup \mathcal{C}(B)| - 1 = |\mathcal{C}(A)| - 1 + |\mathcal{C}(B)| - 1$ par le (vii), mais cette quantité est $\geq |G| > |G| - 1$ par le (vi) : une contradiction.

Problème 3. *Soit $n \geq 1$ un entier. On se propose de démontrer l'équivalence entre les deux propriétés suivantes :* (a) *tout groupe d'ordre n est cyclique,* (b) *n est premier à son indicatrice d'Euler $\varphi(n)$.*

(i) *Montrer que l'on a $(n, \varphi(n)) = 1$ si, et seulement si, n est un produit de nombres premiers distincts $p_1, \ldots, p_r$ avec $p_i \nmid p_j - 1$ pour $i \neq j$.*

C'est la formule $\varphi(\prod_i p_i^{m_i}) = \prod_i p_i^{m_i - 1}(p_i - 1)$.

(ii) *On suppose $p^2 \mid n$ avec p premier. Montrer qu'il existe un groupe non cyclique d'ordre n.*

Si on a $n = p^2 m$, le groupe $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$, d'ordre n, n'est pas cyclique, car il contient $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \times \{0\} \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ qui n'est pas cyclique (son min est 2).

(iii) *Soient p et q premiers avec $p \mid q - 1$. Montrer qu'il existe un morphisme non trivial $\mathbb{Z}/p\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$.*

On a $\mathrm{Aut}(\mathbb{Z}/q\mathbb{Z}) \simeq (\mathbb{Z}/q\mathbb{Z})^\times$, qui est d'ordre $q - 1$. Par Gauss ou Cauchy, $\mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$ admet donc un élément d'ordre p, disons τ. Le morphisme $\mathbb{Z}/p\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/q\mathbb{Z}), \overline{k} \mapsto \tau^k$, est alors bien défini et non trivial.

(iv) *(suite) En déduire qu'il existe un groupe non abélien d'ordre pq.*

Soit $\varphi : \mathbb{Z}/p\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$ un morphisme non trivial, i.e. $\tau = \varphi(\overline{1})$ est un automorphisme non trivial de $\mathbb{Z}/q\mathbb{Z}$. On pose $G = \mathbb{Z}/q\mathbb{Z} \rtimes_\varphi \mathbb{Z}/p\mathbb{Z}$. Soit $x \in \mathbb{Z}/q\mathbb{Z}$ tel que $\tau(x) \neq x$. Alors les éléments $a = (x, 0)$ et $b = (0, \overline{1})$ ne commutent pas : on a $ab = (x, \overline{1})$ et $ba = (\tau(x), \overline{1})$. (Plus généralement, $A \rtimes_\psi B$ est abélien si, et seulement si, A et B sont abéliens et ψ est trivial.)

(v) *(suite) En déduire que pour tout $r \geq 1$, il existe un groupe non abélien d'ordre pqr.*

Si G est non abélien d'ordre m, alors $G \times \mathbb{Z}/r\mathbb{Z}$ est non abélien d'ordre mr (il contient le groupe $G \times \{0\}$ qui est isomorphe à G).

(vi) *Démontrer* (a) $\implies$ (b).

Supposons que tout groupe d'ordre n est cyclique. Le (ii) montre que n est sans facteur carré. Le (iv) montre que si $pq | n$ alors p ne divise pas $q - 1$. Le (i) conclut $(n, \varphi(n)) = 1$.

(vii) *Montrer qu'un groupe abélien d'ordre $p_1p_2\cdots p_r$, avec les p_i premiers distincts, est cyclique.*

Par Cauchy il existe x_i dans G d'ordre p_i. Les p_i sont deux à deux premiers entre eux. Le groupe G est commutatif. Par un lemme du cours (Cauchy encore !) le produit des x_i est d'ordre $p_1p_2\dots p_r$, donc G est cyclique.

(viii) *Soit f un morphisme entre deux groupes finis de cardinaux premiers entre eux. Montrer que f est le morphisme trivial.*

Soit $f : G \to G'$ avec $a = |G|$ premier à $b = |G'|$. On a $\mathrm{Im}\, f$ sous-groupe de G', donc $|\mathrm{Im}\, f|$ divise b. On a $|\mathrm{Im}\, f||\ker f| = |G|$ donc $|\mathrm{Im}\, f|$ divise a. On a $(a, b) = 1$ donc $|\mathrm{Im}\, f| = 1$, i.e. f est trivial.

On va montrer (b) $\implies$ (a) par récurrence sur n. On suppose donc $(n, \varphi(n)) = 1$, et que tout groupe d'ordre $d < n$, avec $(d, \varphi(d)) = 1$, est cyclique. Soit G un groupe fini d'ordre n.

(ix) *Montrer que soit G n'est pas simple, soit il est abélien (utiliser le résultat du Problème 2).*

Par Lagrange, un sous-groupe strict H de G est d'ordre $d < n$ avec $d|n$. Mais par le (i) un tel d vérifie $(d, \varphi(d)) = 1$. Donc H est cyclique par hypothèse de récurrence, donc abélien. Par le Problème 2, G n'est donc pas simple, ou il est abélien.

(x) *Soit H un sous-groupe distingué strict de G. En considérant un morphisme $G \to \mathrm{Aut}(H)$ approprié, montrer $H \subset \mathrm{Z}(G)$.*

On sait que $G \to \mathrm{Aut}(G), g \mapsto \mathrm{int}_g$, est un morphisme de groupes. Comme H est distingué dans G, il est stable par int_g pour tout $g \in G$. On en déduit que $f : G \to \mathrm{Aut}(H), g \mapsto (\mathrm{int}_g)_{|H}$, est un morphisme de groupes. Mais on a vu ci-dessus $H \simeq \mathbb{Z}/d\mathbb{Z}$ avec $d|n$ et $d < n$ car H est strict. On a donc $\mathrm{Aut}(H) \simeq \mathrm{Aut}(\mathbb{Z}/d\mathbb{Z})(\simeq \mathbb{Z}/d\mathbb{Z})^\times$. Ainsi, G est de cardinal n et $|\mathrm{Aut}(H)$ de cardinal $\varphi(d)$, qui est premier à n par le (i). Donc le morphisme f est trivial par le (viii). Cela veut dire que $\mathrm{int}_g(h) = ghg^{-1} = h$ pour tout $g \in G$ et $h \in H$: on a $H \subset \mathrm{Z}(G)$.

(xi) *En déduire que $G/\mathrm{Z}(G)$ est cyclique.*

C'est évident si G est abélien. Sinon G n'est pas simple, et donc $\mathrm{Z}(G)$ non trivial par la question précédente. Ainsi, le groupe $G/\mathrm{Z}(G)$ est d'ordre $d|n$ avec $d < n$. Un tel d vérifie $(d, \varphi(d)) = 1$ par le (i) : le groupe $G/\mathrm{Z}(G)$ est donc cyclique par hypothèse de récurrence.

(xii) *Démontrer* (b) $\implies$ (a).

Par un exercice vu en TD on sait que $G/\mathrm{Z}(G)$ monogène implique G abélien. Mais par le (vii), G est alors cyclique, ce qu'il fallait démontrer.

(xiii) (Application) *Montrer qu'un groupe d'ordre* 255 *est cyclique.*

On a $255 = 5 \cdot 51 = 3 \cdot 5 \cdot 17$ et $\varphi(255) = 2 \cdot 4 \cdot 16$ premier à 255.

(xiv) (Devinette) *Quels sont les entiers n tels que tout groupe d'ordre n est abélien ?*

Ce sont les entiers de la forme $n = \prod_i p_i^{\alpha_i}$ avec $\alpha_i \leq 2$ pour tout i, et p_i ne divise pas $p_j^{\alpha_i} - 1$ pour $i \neq j$.

La démonstration n'était pas demandée ! Montrons simplement que si tout groupe d'ordre n est abélien alors n est de la forme ci-dessus (l'autre sens, plus difficile, sera vu plus tard). Soit p un nombre premier. Le sous-groupe des unipotents supérieurs de $\mathrm{GL}_3(\mathbb{Z}/p\mathbb{Z})$ est non commutatif d'ordre p^3. Ainsi, si p^3 divise n il existe un groupe non abélien d'ordre

n (considérer le produit direct avec un groupe cyclique d'ordre n/p^3). Soient p, q premiers distincts avec $pq|n$. On a déjà vu que pour $p \mid q-1$, il existe un groupe non abélien d'ordre n. Supposons donc que p^2q divise n. Si $q \mid p^2-1$ il existe un groupe non abélien d'ordre p^2q (et donc un groupe non abélien d'ordre n). En effet, on a $\mathrm{Aut}((\mathbb{Z}/p\mathbb{Z})^2) \simeq \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ d'ordre $(p^2-1)(p^2-p) = p(p^2-1)(p-1)$, donc on peut trouver un morphisme non trivial $\varphi : \mathbb{Z}/q\mathbb{Z} \to \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$, et le groupe $(\mathbb{Z}/p\mathbb{Z})^2 \rtimes_\varphi \mathbb{Z}/q\mathbb{Z}$ fait l'affaire.