

## Éléments de correction du partiel du 16 décembre 2019

**Exercice 1** Montrer qu'un groupe d'ordre 200 n'est pas simple.

**Solution 1** Soit  $G$  un groupe d'ordre 200. Notons que  $200 = 2^3 \times 5^2$ . D'après les Théorèmes de SYLOW le nombre de 5-SYLOW de  $G$  est congru à 1 modulo 5 et divise  $2^3 = 8$  donc vaut 1. L'unique 5-SYLOW de  $G$  est donc nécessairement distingué dans  $G$ ; en particulier  $G$  n'est pas simple.

**Exercice 2** Soit  $n \in \mathbb{N}^*$ . Montrer qu'il existe un morphisme injectif de  $\mathcal{S}_n$  dans  $\mathcal{A}_{n+2}$ .

**Solution 2** Considérons l'application  $\psi: \mathcal{S}_n \rightarrow \mathcal{A}_{n+2}$  définie par

$$\begin{cases} \psi(\sigma) = \sigma & \text{si } \sigma \text{ est une permutation paire} \\ \psi(\sigma) = \sigma \circ (n+1 \ n+2) & \text{si } \sigma \text{ est une permutation impaire} \end{cases}$$

L'application  $\psi$  est injective par unicité de la décomposition en cycles à supports disjoints. On peut vérifier que  $\psi$  est un morphisme de groupes.

**Exercice 3** Soit  $G$  un groupe de type fini.

Un sous-groupe  $H$  de  $G$  est-il nécessairement de type fini? Justifiez votre réponse.

**Solution 3** Soit  $G$  est un groupe de type fini;  $G$  peut contenir un sous-groupe  $H$  qui n'est pas de type fini.

Considérons le sous-groupe  $G$  de  $GL(2, \mathbb{Q})$  engendré par les matrices

$$A = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \quad \text{et} \quad B = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Soit  $H$  le sous-groupe de  $G$  formé des matrices de  $G$  avec des 1 sur la diagonale. Raisonnons par l'absurde : supposons que  $H$  soit de type fini. Alors il existe un entier  $N \geq 1$  tel que  $H$  soit contenu dans le sous-groupe de  $GL(2, \mathbb{Q})$  formé des matrices de la forme

$$\begin{pmatrix} 1 & \frac{a}{N} \\ 0 & 1 \end{pmatrix}$$

Or  $A^{-N} B A^N = \begin{pmatrix} 1 & \frac{1}{2^N} \\ 0 & 1 \end{pmatrix}$  : contradiction ( $2^N > N$ ). Ainsi  $H$  n'est pas de type fini alors que  $G$  l'est.

Considérons par exemple le groupe libre  $G$  sur deux générateurs  $a$  et  $b$ . Soit  $H$  le sous-groupe engendré par tous les éléments de la forme  $ab^n$  avec  $n \in \mathbb{N}$ . Raisonnons par l'absurde : supposons que  $H$  soit de type fini. Alors il existe un entier  $N$  tel que dans tout mot de  $H$  le nombre de  $b$  consécutifs soit toujours strictement inférieur à  $N$ . Or  $ab^N$  appartient à  $H$  : contradiction. Le sous-groupe  $H$  de  $G$  n'est donc pas de type fini.

**Exercice 4** Soit  $G$  un groupe abélien d'ordre  $pq$  où  $p$  et  $q$  sont deux nombres premiers distincts. Montrer que  $G$  est cyclique.

**Solution 4** Le théorème de structure appliqué à  $G$  assure que  $G$  est isomorphe à ou bien  $\mathbb{Z}/pq\mathbb{Z}$ , ou bien  $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$ . Cependant le Lemme chinois assure que  $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$  est isomorphe à  $\mathbb{Z}/pq\mathbb{Z}$ . Ainsi  $G$  est isomorphe à  $\mathbb{Z}/pq\mathbb{Z}$  et est cyclique.

Autre rédaction possible Notons multiplicativement la loi du groupe  $G$ . Comme  $p$  et  $q$  sont premiers, les éléments de  $G$  distincts de  $e$  sont d'ordre ou bien  $p$ , ou bien  $q$ , ou bien  $pq$  (théorème de LAGRANGE).

Montrons que si  $G$  admet un élément  $x$  d'ordre  $p$  et un élément  $y$  d'ordre  $q$  alors  $xy$  est d'ordre  $pq$ . Nous avons

- ◊  $xy \neq e$ ; en effet raisonnons par l'absurde, *i.e.* supposons que  $xy = e$ . Alors  $y = x^{-1}$  a même ordre que  $x$ ;
- ◊  $(xy)^p \neq e$ ; en effet  $(xy)^p = x^p y^p$  (car  $G$  est abélien). Comme  $x^p = e$  nous avons  $(xy)^p = y^p$ . Puisque  $q$  ne divise pas  $p$  nous avons  $y^p \neq e$  d'où  $(xy)^p \neq e$ .
- ◊  $(xy)^q \neq e$ ; en effet  $(xy)^q = x^q y^q$  (car  $G$  est abélien). Comme  $y^q = e$  nous avons  $(xy)^q = x^q$ . Puisque  $p$  ne divise pas  $q$  nous avons  $x^q \neq e$  d'où  $(xy)^q \neq e$ .

Il s'en suit que  $xy$  est d'ordre  $pq$ .

Si  $G$  n'est pas cyclique, *i.e.* si  $G$  ne possède pas d'élément d'ordre  $pq$ , alors tous les éléments non triviaux de  $G$  sont tous d'ordre  $p$  ou tous d'ordre  $q$ . Supposons par exemple que tous les éléments non triviaux de  $G$  sont d'ordre  $p$ . Soit  $x$  d'ordre  $p$  et soit  $H$  le sous-groupe engendré par  $x$ . Considérons le groupe quotient  $G/H$  d'ordre  $q$ . Puisque  $q$  est premier  $G/H$  est cyclique. Soit  $z \in G$  tel que  $\bar{z}$  engendre  $G/H$ ;  $\bar{z}$  est donc d'ordre  $q$ . Mais nous avons aussi  $\bar{z}^p = \bar{z}^p = \bar{1}$ . Comme  $\bar{z}$  est d'ordre  $q$ , nous en déduisons que  $q$  divise  $p$  ce qui est absurde. Il en résulte que  $G$  est cyclique.

### Exercice 5

- (1) Soit  $H$  un sous-groupe distingué de  $\mathcal{S}_4$  qui contient un 4-cycle. Montrer que  $H = \mathcal{S}_4$ .
- (2) Soient  $P_1$  et  $P_2$  deux sous-groupes d'ordre 8 de  $\mathcal{S}_4$ . Supposons que  $P_1 \cap P_2$  contienne un 4-cycle. Montrer que  $P_1 = P_2$  (indication : on montre que le normalisateur de  $P_1 \cap P_2$  dans  $\mathcal{S}_4$  contient  $P_1 \cup P_2$ , on considère le sous-groupe engendré par  $P_1 \cup P_2$  et on utilise 1.)
- (3) D'après ce qui précède un 4-cycle est dans un unique sous-groupe d'ordre 8 de  $\mathcal{S}_4$ . En déduire le nombre de sous-groupes d'ordre 8 de  $\mathcal{S}_4$  en comptant le nombre de 4-cycles.

### Solution 5

- (1) Les sous-groupes distingués de  $\mathcal{S}_4$  sont  $\text{id}$ ,  $\{\text{id}, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$ ,  $\mathcal{A}_4$  et  $\mathcal{S}_4$ . Le seul de ces sous-groupes qui contient un 4-cycle est  $\mathcal{S}_4$ .
- (2) Soient  $P_1$  et  $P_2$  deux sous-groupes d'ordre 8 de  $\mathcal{S}_4$ . Si  $P_1 \neq P_2$ , alors  $P_1 \cap P_2$  contient un 4-cycle et est donc d'ordre 4. Par conséquent  $P_1 \cap P_2$  est d'indice 2 dans  $P_1$  donc distingué dans  $P_1$ . De même  $P_1 \cap P_2$  est d'indice 2 dans  $P_2$  donc distingué dans  $P_2$ . Par suite le normalisateur  $N$  de  $P_1 \cap P_2$  dans  $\mathcal{S}_4$  contient  $P_1 \cup P_2$ . Ainsi  $N$  est un sous-groupe de  $P_1 \cap P_2$  d'ordre un diviseur de 24 qui est un multiple de 8 et  $> 8$ . Il en résulte que  $|N| = 24$  et donc que  $N = \mathcal{S}_4$ . Ainsi  $P_1 \cap P_2 \triangleleft \mathcal{S}_4$  et  $P_1 \cap P_2 = \mathcal{S}_4$  : absurde.
- (3) Déterminons le nombre de 4-cycles de  $\mathcal{S}_4$ . Un 4-cycle s'écrit de manière unique  $(1\ i\ j\ k)$  où  $i, j$  et  $k$  sont trois entiers distincts parmi  $\{2, 3, 4\}$ . Il y a donc  $3 \times 2 \times 1 = 6$  4-cycles dans  $\mathcal{S}_4$ . Soit  $n_2$  le nombre de sous-groupes d'ordre 8. Ils sont tous isomorphes car ce sont les 2-SYLOW qui sont tous conjugués. Soit  $k$  le nombre de 4-cycles dans un 2-SYLOW. Nous avons donc  $n_2 k = 6$  car un 4-cycle engendre un 2-groupe forcément contenu dans un 2-SYLOW. De plus  $k \geq 2$  car si  $c$  est un 4-cycle dans un sous-groupe  $P$  d'ordre 8, alors  $c^{-1}$  appartient à  $P$ . Si  $n_2$  vaut 1 l'unique 2-SYLOW contient un 4-cycle et est distingué dans  $\mathcal{S}_4$  donc est  $\mathcal{S}_4$  : contradiction. Par suite  $n_2 = 3$  et  $k = 2$ .

**Exercice 6** Soit  $G$  un groupe d'ordre 15.

- (1) Combien  $G$  possède-t-il d'éléments d'ordre 3 ?
- (2) Combien  $G$  possède-t-il d'éléments d'ordre 5 ?
- (3) Démontrer que  $G$  est isomorphe à  $\mathbb{Z}/15\mathbb{Z}$ .

**Solution 6**

- (1) Soit  $n_3$  le nombre de 3-SYLOW de  $G$ . D'après les théorèmes de SYLOW,  $n_3 \equiv 1 \pmod{3}$  et  $n_3|5$ , *i.e.*  $n_3 = 1$ . Soit  $H$  l'unique 3-SYLOW de  $G$ . Tout élément d'ordre 3 engendre un sous-groupe d'ordre 3. Il y a donc exactement deux éléments d'ordre 3 : si  $H = \{\text{id}, g, h\}$ , alors ces éléments sont  $g$  et  $h$ .
- (2) De la même façon, on montre que  $G$  possède quatre éléments d'ordre 5. Soit  $n_5$  le nombre de 5-SYLOW de  $G$ . Les théorèmes de SYLOW assurent que  $n_5 \equiv 1 \pmod{5}$  et  $n_5|3$  soit que  $n_5 = 1$ . Mais tout élément d'ordre 5 engendre un sous-groupe d'ordre 5. Il y a donc exactement quatre éléments d'ordre 5.
- (3) L'ordre d'un élément de  $G$  est un diviseur de 15, donc est égal à 1, 3, 5 ou 15. Comme il y a un élément d'ordre 1, deux éléments d'ordre 3 et quatre éléments d'ordre 5, il y a huit éléments d'ordre 15. Ainsi  $G$  possède un élément d'ordre son cardinal ;  $G$  est donc le groupe cyclique engendré par cet élément, *i.e.*  $G$  est isomorphe à  $\mathbb{Z}/15\mathbb{Z}$ .

**Exercice 7** Soient  $p$  un nombre premier et  $n$  un entier naturel avec  $p > n$ . Considérons un groupe  $G$  d'ordre  $pn$  et  $H$  un sous-groupe de  $G$  d'ordre  $p$ . Montrer que  $H$  est un sous-groupe distingué de  $G$ .

Indication : compter les  $p$ -SYLOW de  $G$ .

**Solution 7** D'après les hypothèses,  $\text{pgcd}(p, n) = 1$ , donc  $H$  est un  $p$ -SYLOW de  $G$ . Notons  $n_p$  le nombre de  $p$ -SYLOW de  $G$ . Alors par les théorèmes de SYLOW,  $n_p \equiv 1 \pmod{p}$  et  $n_p|n$ . Si  $n_p \neq 1$ , alors  $n_p \geq p + 1$ , ce qui contredit que  $n_p$  divise  $n$  puisque  $n < p$ . Ainsi,  $n_p = 1$  et  $H$  est l'unique  $p$ -SYLOW de  $G$  donc est distingué dans  $G$ .

**Exercice 8** Déterminer à isomorphisme près tous les groupes d'ordre 33.

**Solution 8** Soit  $G$  un groupe d'ordre 33.

Les éléments de  $G$  sont d'ordre 1, 3, 11 ou 33. Une application directe des théorèmes de SYLOW montre que  $G$  contient un unique 3-SYLOW et un unique 11-SYLOW. En effet soit  $n_p$  le nombre de  $p$ -SYLOW de  $G$  ; d'une part  $n_3 \equiv 1 \pmod{3}$  et  $n_3|11$ , d'autre part  $n_{11} \equiv 1 \pmod{11}$  et  $n_{11}|3$ , *i.e.*  $n_{11} = 1$ . Les éléments d'ordre 3 et 11 sont contenus dans ces deux groupes. On a au plus  $1 + (3 - 1) + (11 - 1) = 1 + 2 + 10 = 13$  éléments d'ordre 1, 3 ou 11. Il existe donc un élément d'ordre 33 dans  $G$  qui est donc cyclique isomorphe à  $\mathbb{Z}/33\mathbb{Z}$ .

**Exercice 9**

- (1) Soit  $G$  un groupe fini de cardinal  $p^m$  avec  $p$  premier et  $m \in \mathbb{N}^*$  qui opère sur un ensemble fini non vide  $E$ . Posons

$$E^G = \{x \in E \mid \forall g \in G, g \cdot x = x\}.$$

Montrer que  $|E^G| = |E| \pmod{p}$ .

- (2) Soit  $H$  un groupe fini d'ordre  $n$ . Soit  $p$  un diviseur premier de  $n$ . Montrer que  $H$  contient un élément d'ordre  $p$  (lemme de CAUCHY). Indication : faire agir  $\mathbb{Z}/p\mathbb{Z}$  sur l'ensemble  $E$  des  $(x_1, x_2, \dots, x_p)$  de  $\mathbb{H}^p$  tels que  $x_1 x_2 \dots x_p = e$ .

- (3) Soit  $H$  un groupe fini d'ordre  $n$ . Soit  $m \in \mathbb{N}^*$  tel que pour tout  $x \in H$  on ait  $x^m = e$ . Montrer que  $n$  divise une puissance de  $m$ .

### Solution 9

- (1) Si  $x$  appartient à  $E$ , nous notons  $\mathcal{O}(x)$  l'orbite de  $x$  sous l'action de  $G$ . Les éléments de  $E^G$  sont exactement les éléments  $x$  de  $E$  tels que  $\mathcal{O}(x) = \{x\}$ . Notons  $\omega_1, \omega_2, \dots, \omega_r$  les orbites de  $E$  de cardinal strictement supérieur à 1. Si  $x_i$  est un élément de  $\omega_i$ , alors  $|\omega_i| = [G : \text{Stab}_G(x_i)]$ , c'est donc une puissance de  $p$ . Il résulte de l'équation aux classes que

$$|E| = |E^G| + \sum_{i=1}^r |\omega_i| \equiv |E^G| \pmod{p}$$

- (2) Soit  $(x_1, x_2, \dots, x_p)$  un élément de  $E$ . Nous avons  $x_1 x_2 \dots x_p = e$ . En multipliant à gauche par  $x_1^{-1}$  et à droite par  $x_1$  nous obtenons  $x_2 x_3 \dots x_p x_1 = e$ , i.e.  $(x_2, x_3, \dots, x_p, x_1)$  appartient à  $E$ . Notons  $c$  le cycle  $(1 \ 2 \ \dots \ p)$  de  $\mathcal{S}_p$ . Il s'agit d'un élément d'ordre  $p$  qui engendre un sous-groupe cyclique  $K$  isomorphe à  $\mathbb{Z}/p\mathbb{Z}$ . Nous définissons une opération de  $K$  sur l'ensemble  $H^p$  par

$$c \cdot (x_1, x_2, \dots, x_p) = (x_{c(1)}, x_{c(2)}, \dots, x_{c(p)}) = (x_2, x_3, \dots, x_p, x_1).$$

La remarque ci-dessus montre que  $E$  est stable par cette opération. Appliquons alors le résultat de la question précédente à l'opération induite sur  $E$ . Nous avons  $|E| \equiv |E^K| \pmod{p}$ . Le cardinal de  $E$  est  $n^{p-1}$  (en effet on peut choisir  $x_1, x_2, \dots, x_{p-1}$  quelconques,  $x_p$  est alors déterminé de manière unique). Comme  $p$  divise  $n$ ,  $|E^K|$  est nul modulo  $p$ . Or les éléments de  $E^K$  sont justement les  $p$ -uplets  $(x, x, \dots, x)$  avec  $x^p = e$ . Notons que  $E^K$  contient le  $p$ -uplet  $(e, e, \dots, e)$ ; en particulier  $E^K$  est non vide et par suite  $E^K$  a un cardinal supérieur à  $p$ . Il y a donc au moins  $(p-1)$  éléments d'ordre  $p$  dans  $H$ .

- (3) Il suffit de montrer que tous les facteurs premiers de  $n$  sont des facteurs premiers de  $m$ . Soit  $p$  un premier divisant  $n$ . Le lemme de CAUCHY garantit l'existence d'un élément  $x \in H$  d'ordre  $p$ . Or par hypothèse  $x^m = e$  donc  $p$  divise  $m$ .

### Exercice 10

Soit  $G$  un groupe d'ordre 2009.

- (1) Montrer que  $G \simeq P \times Q$  où  $P$  est un groupe d'ordre 41 et  $Q$  est un groupe d'ordre 49. En déduire que chaque groupe d'ordre 2009 est abélien.
- (2) Classifier à isomorphisme près tous les groupes d'ordre 2009.
- (3) Soient  $P$  est un groupe d'ordre 41 et  $Q$  est un groupe d'ordre 49. Montrer que  $\text{Aut}(G) \simeq \text{Aut}(P) \times \text{Aut}(Q)$ .
- (4) Montrer que
  - a) si  $Q$  est cyclique, alors  $\text{Aut}(Q)$  est cyclique aussi. Quel est l'ordre de  $\text{Aut}(Q)$  quand  $Q$  est cyclique ?
  - b) si  $Q$  n'est pas cyclique, alors  $\text{Aut}(Q)$  est isomorphe à  $\text{GL}(2, \mathbb{F}_7)$  où  $\mathbb{F}_7$  est le corps à 7 éléments. Quel est l'ordre de  $\text{GL}(2, \mathbb{F}_7)$  ?

### Solution 10

- (1) Notons que  $|G| = 2009 = 7^2 \times 41$ . D'après le premier théorème de SYLOW le groupe  $G$  possède un 41-SYLOW  $P$  d'ordre 41 et un 7-SYLOW  $Q$  d'ordre 49. Notons  $n_p$  le nombre de  $p$ -SYLOW de  $G$ . D'après le troisième théorème de SYLOW
- ◇  $n_{41}$  est congru à 1 modulo 41 et divise 49 donc est égal à 1 ;
  - ◇  $n_7$  est congru à 1 modulo 7 et divise 41 donc est égal à 1.

Nous en déduisons que  $P \triangleleft G$  et  $Q \triangleleft G$ .

Nous constatons aussi que  $P \cap Q = \{e\}$ , que  $G = PQ$  et que les deux sous-groupes dans le produit sont distingués dans  $G$ . Tout ceci revient à dire  $G \simeq P \times Q$ .

Reste à montrer que  $G$  est abélien. Notons que  $P$  et  $Q$  sont abéliens puisque  $P$  est d'ordre premier et que  $Q$  est d'ordre premier au carré. Par ailleurs les éléments de  $P$  commutent avec ceux de  $Q$ . Ainsi  $G$  est abélien.

- (2) D'après 1. tous les groupes d'ordre 2009 sont abéliens, il suffit donc pour répondre à cette question d'appliquer le théorème de structure pour les groupes abéliens de type fini. Ce théorème montre qu'il y a deux groupe non isomorphes d'ordre 2009

$$\mathbb{Z}/49\mathbb{Z} \times \mathbb{Z}/41\mathbb{Z} \quad \text{et} \quad \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/41\mathbb{Z}$$

soit encore

$$\mathbb{Z}/2009\mathbb{Z} \quad \text{et} \quad \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/287\mathbb{Z}$$

- (3) **Remarque.** Si  $\varphi$  est un automorphisme de  $G$ , alors  $\varphi(P) = P$  et  $\varphi(Q) = Q$ . En effet comme dans tout groupe et pour tout  $p$  premier l'image par un morphisme d'un  $p$ -élément est un  $p$ -élément et que  $P$  et  $Q$  sont les seuls 41-SYLOW et 7-SYLOW de  $G$  respectivement,  $\varphi(P) \subset P$  et  $\varphi(Q) \subset Q$ . Comme  $\varphi$  est une bijection ces deux inclusions sont en fait des égalités.

Il découle de la Remarque précédente que la restriction de tout automorphisme  $\varphi \in \text{Aut}(G)$  au sous-groupe  $P$  (resp.  $Q$ ) est un automorphisme qu'on appellera  $\varphi_P$  (resp.  $\varphi_Q$ ) de  $P$  (resp.  $Q$ ). Les automorphismes de  $\varphi_P$  et  $\varphi_Q$  ainsi définis sont uniquement définis puisqu'ils sont les restrictions d'un même automorphisme aux sous-groupes  $P$  et  $Q$  respectivement.

Considérons l'application

$$\Phi: \text{Aut}(G) \rightarrow \text{Aut}(P) \times \text{Aut}(Q), \quad \varphi \mapsto (\varphi_P, \varphi_Q)$$

Remarquons que  $\Phi(\text{id}) = (\text{id}, \text{id})$ . Soient  $\varphi$  et  $\phi$  deux éléments de  $\text{Aut}(G)$ . Alors d'une part

$$\begin{aligned} (\varphi \circ \phi)_P(P) &= (\varphi \circ \phi)(P) \\ &= \varphi(\phi(P)) \\ &= \varphi_P(\phi_P(P)) \\ &= (\varphi_P \circ \phi_P)(P) \end{aligned}$$

et d'autre part

$$\begin{aligned} (\varphi \circ \phi)_Q(Q) &= (\varphi \circ \phi)(Q) \\ &= \varphi(\phi(Q)) \\ &= \varphi_Q(\phi_Q(Q)) \\ &= (\varphi_Q \circ \phi_Q)(Q) \end{aligned}$$

Autrement dit  $\Phi$  est un morphisme de groupes.

Montrons maintenant que  $\Phi$  est un isomorphisme.

Commençons par montrer que  $\Phi$  est injective. Un automorphisme  $\varphi$  de  $\text{Aut}(G)$  appartient à  $\ker \Phi$  si et seulement si  $\varphi_P = \text{id}_P$  et  $\varphi_Q = \text{id}_Q$ . Or tout élément de  $G$  s'écrit sous la forme  $xy$  avec  $x \in P$  et  $y \in Q$ . Ainsi

$$\varphi(xy) = \varphi(x)\varphi(y) = \varphi_P(x)\varphi_Q(y) = \text{id}_P(x)\text{id}_Q(y) = xy.$$

Montrons que  $\Phi$  est surjective. Soient  $\varphi_1$  dans  $\text{Aut}(P)$  et  $\varphi_2$  dans  $\text{Aut}(Q)$ . Considérons l'application

$$\varphi: G \rightarrow G, \quad xy \mapsto \varphi_1(x)\varphi_2(y)$$

avec  $x \in P$  et  $y \in Q$ . L'application  $\sigma$  est définie sans ambiguïté puisque  $G$  étant la somme directe de  $P$  et de  $Q$  chacun de ses éléments s'écrit de manière unique comme produit d'un élément de  $P$  et d'un autre de  $Q$ . Montrons que  $\varphi$  est un automorphisme de  $G$  dont l'image sous l'action de  $\Phi$  est  $(\varphi_1, \varphi_2)$ .

Le fait que  $\varphi_1$  et  $\varphi_2$  soient des morphismes de groupes entraîne que  $\varphi$  est un morphisme de groupes. Il en est de même pour la surjectivité de  $\varphi$ . Supposons que  $\varphi(xy) = 1$  pour  $x \in P$  et  $y \in Q$ . La définition de  $\varphi$  implique que  $\varphi_1(x)\varphi_2(y) = 1$ . Or  $\varphi_1(x)$  appartient à  $P$ ,  $\varphi_2(y)$  appartient à  $Q$  et  $P \cap Q = \{e\}$  donc  $\varphi_1(x) = \varphi_2(y) = 1$ . Puisque  $\varphi_1$  est un automorphisme de  $P$  et  $\varphi_2$  un automorphisme de  $Q$  nous obtenons  $x = y = 1$ . Comme  $G = PQ$  tout élément de  $\ker \varphi$  s'écrit comme produit d'un  $x \in P$  et d'un  $y \in Q$ . Ainsi  $\ker \varphi = \{e\}$ .

Finalement  $\varphi$  est un automorphisme de  $G$ . Il s'ensuit de la définition de  $\varphi$  que  $\varphi_P = \varphi_1$  et  $\varphi_Q = \varphi_2$ . Par conséquent  $\Phi(\varphi) = (\varphi_1, \varphi_2)$ . Ainsi  $\Phi$  est surjective.

- (4) a) Si  $Q$  est cyclique, il est isomorphe à  $(\mathbb{Z}/49\mathbb{Z}, +)$ . Alors  $|\text{Aut}(Q)| = \varphi(49) = 7 \times 6 = 42$  où  $\varphi$  est la fonction indicatrice d'EULER. Comme  $42 = 2 \times 3 \times 7$  le théorème chinois assure que  $\text{Aut}(Q)$  est cyclique d'ordre 42.
- b) Supposons maintenant que  $Q$  soit non cyclique. Alors  $Q \simeq (\mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}, +)$ . Ce dernier groupe peut aussi être considéré comme l'espace vectoriel de dimension 2 sur le corps  $\mathbb{F}_7$  avec la base canonique  $e_1 = (1, 0)$  et  $e_2 = (0, 1)$ . La loi externe induite par  $\mathbb{F}_7$  est décrite par les identités

$$\lambda e_1 = \underbrace{(1, 0) + (1, 0) + \dots + (1, 0)}_{\lambda \text{ fois}} \quad \lambda e_2 = \underbrace{(0, 1) + (0, 1) + \dots + (0, 1)}_{\lambda \text{ fois}}$$

avec  $\lambda \in \mathbb{F}_7$ , identités qui sont ensuite étendues au groupe tout entier par linéarité. Cette action est définie sans ambiguïté.

Soit  $\varphi \in \text{Aut}(Q)$ , alors

$$\begin{aligned} \varphi(\lambda e_1) &= \varphi(\underbrace{(1, 0) + (1, 0) + \dots + (1, 0)}_{\lambda \text{ fois}}) \\ &= \underbrace{\varphi(1, 0) + \varphi(1, 0) + \dots + \varphi(1, 0)}_{\lambda \text{ fois}} \\ &= \lambda \varphi((1, 0)) \\ &= \lambda \varphi(e_1) \end{aligned}$$

et

$$\begin{aligned} \varphi(\lambda e_2) &= \varphi(\underbrace{(0, 1) + (0, 1) + \dots + (0, 1)}_{\lambda \text{ fois}}) \\ &= \underbrace{\varphi(0, 1) + \varphi(0, 1) + \dots + \varphi(0, 1)}_{\lambda \text{ fois}} \\ &= \lambda \varphi((0, 1)) \\ &= \lambda \varphi(e_2) \end{aligned}$$

Ainsi  $\varphi$  est une application linéaire. Étant bijectif  $\varphi \in \text{GL}(2, \mathbb{F}_7)$ . Par suite  $\text{Aut}(Q) \subset \text{GL}(2, \mathbb{F}_7)$ . L'autre inclusion est claire car chaque bijection linéaire de  $\mathbb{F}_7 \times \mathbb{F}_7$  est aussi un automorphisme du groupe  $\mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$ . Finalement  $|\text{GL}(2, \mathbb{F}_7)| = (7^2 - 1)(7^2 - 7)$ .