

## Solution de l'exercice 1

### Question 1

Ici aucune difficulté particulière : il faut dérouler les définitions. L'ensemble  $Z(G)$  est par définition inclus dans le groupe  $(G, \cdot)$ . Montrons que  $Z(G)$  est un sous-groupe de  $G$ , c'est-à-dire montrons qu'il contient l'élément neutre, qu'il est stable par produit et passage à l'inverse.

1. On remarque que par définition de l'élément neutre, noté ici  $e$ , on a :

$$\forall g \in G, \quad ge = eg(= g).$$

Donc par définition de  $Z(G)$ , on a bien  $e \in Z(G)$ .

2. Soit  $(a, b) \in Z(G)^2$ , on a pour tout  $g \in G$ ,

$$\begin{aligned} (ab)g &= abg && \text{par associativité de la loi,} \\ &= agb && \text{car } b \in Z(G), \\ &= gab && \text{car } a \in Z(G). \end{aligned}$$

Ainsi, le produit  $ab \in Z(G)$ .

3. Soit  $a \in Z(G)$ . Pour tout  $g \in G$ , puisque  $a \in Z(G)$ , on a  $ag = ga$ . En multipliant à gauche et à droite par  $a^{-1}$ , on obtient  $ga^{-1} = a^{-1}g$ . Ceci étant vrai pour tout  $g \in G$ , on conclut que  $a^{-1} \in Z(G)$ .

Grâce à ces trois propriétés, on en déduit que  $Z(G)$  est bien un sous-groupe de  $G$ .

### Question 2

$H$  est un sous-groupe de  $G$  et par la question 1,  $Z(G)$  est aussi un sous-groupe de  $G$ . Donc par l'exercice 9 du TD 2, l'intersection de deux sous-groupes est toujours un sous-groupe et  $Z(G) \cap H$  est un sous-groupe de  $G$ . Pour plus de précision, voici la démonstration :

1.  $H$  est un sous-groupe de  $G$ , donc  $e \in H$ . De même  $e \in Z(G)$  donc on en déduit que  $e \in Z(G) \cap H$ .
2. Soit  $x$  et  $y$  deux éléments de  $Z(G) \cap H$ , alors  $(x, y) \in Z(G)^2$  et  $(x, y) \in H^2$ . Puisque  $Z(G)$  est un sous-groupe (question 1), on sait que  $xy^{-1} \in Z(G)$ . De même  $H$  étant un sous-groupe de  $G$ ,  $xy^{-1} \in H$ . Ainsi on voit que  $xy^{-1} \in Z(G) \cap H$ .

Par ces propriétés on conclut bien que  $Z(G) \cap H$  est un sous-groupe **de  $G$ !!!** Donc par définition d'un sous-groupe, c'est un groupe, qui est inclus dans  $G$ . Montrons que ce groupe  $Z(G) \cap H$  est inclus dans  $Z(H)$  : soit  $a \in Z(G) \cap H$  alors  $a \in H$  et  $a \in Z(G)$ . Puisque  $a \in Z(G)$ , on sait que  $a$  commute avec tous les éléments de  $G$  et donc a fortiori  $a$  commute avec tous les éléments de  $H$ .

*N.B. : un groupe est commutatif, un élément a plutôt tendance à commuter avec d'autres éléments.* Donc  $a \in \{x \in G, \forall h \in H, xh = hx\}$ . Puis comme  $a \in H$ , on conclut que  $a \in Z(H)$ . Finalement  $Z(G) \cap H$  est un groupe inclus dans  $Z(H)$  et donc est un sous-groupe de  $Z(H)$ .

### Question 3

Beaucoup d'erreurs sur cette question. Vous avez été nombreux à ne pas voir à quoi servait la surjectivité de  $\varphi$ . En deux étapes à nouveau : montrons que  $\varphi(Z(G))$  est un groupe (et même un sous-groupe de  $G'$ ). Puis montrons que  $\varphi(Z(G))$  est inclus dans  $Z(G')$ .

1. Soit  $e'$  l'élément neutre de  $G'$ . Puisque  $\varphi$  est un morphisme, on sait que  $e' = \varphi(e)$ . Or puisque par la question 1,  $Z(G)$  est un sous-groupe de  $G$ , on sait que  $e \in Z(G)$ . Donc  $e'$  est bien l'image par  $\varphi$  d'un élément de  $Z(G)$ , id est  $e' \in \varphi(Z(G))$ .
2. Soit  $a'$  et  $b'$  deux éléments de  $\varphi(Z(G))$ . Par définition de  $\varphi(Z(G))$ , il existe  $a$  et  $b$  dans  $Z(G)$  tels que

$$a' = \varphi(a) \quad \text{et} \quad b' = \varphi(b).$$

Maintenant par les propriétés de morphisme,

$$a'(b')^{-1} = \varphi(a)\varphi(b)^{-1} = \varphi(a)\varphi(b^{-1}) = \varphi(ab^{-1}).$$

De plus,  $Z(G)$  étant un sous-groupe de  $G$  (question 1), on sait que  $ab^{-1} \in Z(G)$ . Ainsi  $a'(b')^{-1}$  est l'image par  $\varphi$  d'un élément de  $Z(G)$  et donc  $a'(b')^{-1} \in \varphi(Z(G))$ .

Par ces propriétés, on en déduit que  $\varphi(Z(G))$  est un sous-groupe de  $G$  et est donc un groupe.

3. Or, montrons que  $\varphi(Z(G))$  est inclus dans  $Z(G')$ . Soit  $a' \in \varphi(Z(G))$ , il existe  $a \in Z(G)$  tel que  $a' = \varphi(a)$ . Pour montrer que  $a' \in Z(G')$  il faut montrer qu'il commute avec tous éléments  $g'$  de  $G'$  en utilisant le fait que  $a \in Z(G)$ , c'est-à-dire en utilisant le fait que  $a$  commute avec tous les éléments de  $G$ . Prenons un élément  $g'$  quelconque de  $G'$  et montrons qu'il commute avec  $a'$ . Puisque  $\varphi$  est surjective (et j'insiste, c'est l'unique passage où cela nous sert), on sait que tout élément de  $G'$  admet un antécédent (au moins) dans  $G$ . Donc il existe  $g \in G$  tel que

$$g' = \varphi(g).$$

Maintenant, on écrit que, par la propriété de morphisme,

$$a'g' = \varphi(a)\varphi(g) = \varphi(ag).$$

Puisque  $a \in Z(G)$ ,

$$a'g' = \varphi(ga) = \varphi(g)\varphi(a) = g'a'.$$

Et finalement  $a' \in Z(G')$ .

Ainsi  $\varphi(Z(G))$  est un groupe inclus dans  $Z(G')$  et est donc un sous-groupe de  $Z(G')$ .

### Solution de l'exercice 2

Considérons pour commencer le système

$$(S_1) \quad \begin{cases} n \equiv 1 \pmod{3} \\ n \equiv 4 \pmod{5} \end{cases}$$

Puisque 3 et 5 sont premiers entre eux, le théorème chinois nous garantit l'existence ET L'UNIQUE d'une solution modulo  $3 \times 5 = 15$ . Cherchons cette solution. Puisque 3 et 5 sont premiers entre eux, par l'identité de Bezout, on sait qu'il existe  $(u, v) \in \mathbb{Z}$  tel que

$$3u + 5v = 1.$$

Par l'algorithme d'Euclide,

$$\begin{aligned}5 &= 3 + 2 \\3 &= 2 + 1.\end{aligned}$$

En remontant cet algorithme,

$$\begin{aligned}1 &= 3 - 2 \\&= 3 - (5 - 3) = 3 * 2 - 5.\end{aligned}$$

Une valeur possible pour le couple  $(u, v)$  est  $(2, -1)$ . Considérons l'entier  $n_0 = 3u * 4 + 5v * 1 = 3 * 2 * 4 - 5 = 19$ . On vérifie facilement que  $n_0$  est une solution de  $(S_1)$ . Donc par l'unicité assurée par le théorème chinois, le système  $(S_1)$  est équivalent à

$$(S_1) \Leftrightarrow n \equiv 19 \equiv 4 \pmod{15}.$$

Ainsi le système

$$(S) \quad \begin{cases} n \equiv 1 \pmod{3} \\ n \equiv 4 \pmod{5} \\ n \equiv 5 \pmod{7} \end{cases}$$

est équivalent à

$$(S) \quad \begin{cases} n \equiv 4 \pmod{15} \\ n \equiv 5 \pmod{7}. \end{cases}$$

De la même façon, puisque 15 et 7 sont premiers entre eux, par le théorème des restes chinois, on sait qu'il existe une unique solution au système  $(S)$  modulo  $15 * 7 = 105$ . Puisque 15 et 7 sont premiers entre eux, par l'identité de Bezout, on sait qu'il existe  $(u', v') \in \mathbb{Z}$  tel que

$$15u' + 7v' = 1.$$

Par l'algorithme d'Euclide,

$$15 = 7 * 2 + 1.$$

En remontant cet algorithme (ou plutôt en inversant cette égalité),

$$1 = 15 - 7 * 2.$$

Ainsi, une valeur possible pour le couple  $(u', v')$  est  $(1, -2)$ . Considérons l'entier  $n_1 = 15u' * 5 + 7v' * 4 = 15 * 1 * 5 - 7 * 2 * 4 = 19$ . On vérifie facilement que  $n_1$  est une solution de  $(S)$ . Donc par l'unicité assurée par le théorème chinois, le système  $(S)$  est équivalent à

$$(S) \Leftrightarrow n \equiv 19 \pmod{105}.$$

Ce qui conclut l'exercice.

## Solution de l'exercice 3

### Question 1

Puisque  $p$  et  $q$  sont premiers entre eux (car premiers et distincts),  $\varphi(pq) = \varphi(p)\varphi(q)$ . Puisque  $p$  est premier,  $\varphi(p) = p - 1$ , puis de même  $\varphi(q) = q - 1$  et on en déduit que  $\varphi(n) = (p - 1)(q - 1)$ . Maintenant puisque  $t \equiv 1 \pmod{\varphi(n)}$  on sait qu'il existe  $k \in \mathbb{Z}$  tel que

$$t = k\varphi(n) + 1 = k(p - 1)(q - 1) + 1.$$

Soit  $x \in \mathbb{Z}$ , montrons que

$$\begin{cases} x^t \equiv x [p] \\ x^t \equiv x [q] \end{cases}$$

Premier cas, si  $x = 0 [p]$  alors on a naturellement que  $x^t = 0 = x [p]$ .

Second cas, si  $x \neq 0 [p]$ , par le théorème d'Euler (ou ici le petit théorème de Fermat puisque  $p$  est premier),

$$\begin{aligned} x^{\varphi(p)} &= x^{p-1} = 1 [p] \\ \Rightarrow x^{k\varphi(p)} &= (x^{p-1})^{k(q-1)} = 1^{k(q-1)} = 1 [p] \\ \Rightarrow x^t &= 1 * x = x [p]. \end{aligned}$$

Exactement de la même façon, puisque  $q$  est premier, on a  $x^t = x [q]$ . On a donc montré

$$\begin{cases} x^t \equiv x [p] \\ x^t \equiv x [q] \end{cases}$$

Puis, comme  $p$  et  $q$  sont premiers entre eux, par le théorème des restes chinois, l'application canonique de  $\mathbb{Z}/pq\mathbb{Z}$  dans  $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$  est un isomorphisme. Comme  $x$  et  $x^t$  ont même image par cet isomorphisme (d'après le système écrit juste au-dessus), on en déduit (par injectivité) que nécessairement,

$$x^t = x [n].$$

## Question 2

Puisque  $u$  est premier avec  $\varphi(n)$ , on sait qu'il est inversible dans  $\mathbb{Z}/\varphi(n)\mathbb{Z}$ . Notons  $v$  son inverse. Par définition :

$$uv \equiv 1 [\varphi(n)].$$

Puisque  $n = pq$ ,  $p$  et  $q$  premiers distincts et en posant  $t = uv$ , on se trouve exactement dans la situation de la question 1. Donc d'après le résultat de la question 1, on sait que pour tout  $x \in \mathbb{Z}/n\mathbb{Z}$ ,

$$x^{uv} = x [n].$$

Ainsi pour tout  $x \in \mathbb{Z}/n\mathbb{Z}$ ,

$$\psi_u \circ \psi_v(x) = (x^v)^u = x^{uv} = x \quad \text{et} \quad \psi_v \circ \psi_u(x) = (x^u)^v = x^{uv} = x.$$

Finalement,  $\psi_u \circ \psi_v = \psi_v \circ \psi_u = Id_{\mathbb{Z}/n\mathbb{Z}}$ , ces applications sont réciproques l'une de l'autre et sont donc bijectives.