Correction du TD n°2 : groupes et groupes cycliques

1 Échauffement sur les groupes

Exercice 1. Existence automatique d'inverses

1. Soit $(M, \star)$ un monoïde fini où tout élément est régulier. Démontrer que $(M, \star)$ est un groupe.
2. Soit $(G, \star)$ un groupe et H un sous-ensemble fini non vide de G stable par $\star$. Démontrer que H est un sous-groupe de G.
3. L'hypothèse de finitude est-elle nécessaire dans les deux questions précédentes ?
4. Soit $(M, \star)$ un monoïde tel que tout élément possède un inverse à gauche. Démontrer que $(M, \star)$ est un groupe.

Correction de l'exercice 1

Les deux premières questions reposent essentiellement sur le fait qu'une application injective d'un ensemble fini dans lui-même est bijective.

1. Soit $m \in M$. Puisque m est régulier à gauche, l'application
$$m \star - \, : M \to M, \quad x \mapsto m \star x$$
est injective. L'ensemble M étant fini, elle est donc bijective et il en découle qu'il existe un élément envoyé sur le neutre. Nous venons de prouver l'existence d'un inverse à droite m' de m. La régularité à droite de m fournit par un argument similaire l'existence d'un inverse à gauche m'' de m. Enfin, l'associativité permet d'écrire
$$m' = (m'' \star m) \star m' = m'' \star (m \star m') = m'$$
ce qui conclut quant à l'existence d'inverses.

Remarque : en combinant ceci à la question 4, nous aurions pu remplacer "régulier" par "régulier à droite" dans cette question.

2. Prenons un élément h de H. Puisque G est un groupe, l'application $h \star -$ de source G est injective, et c'est encore le cas de sa restriction à H. Puisque H est stable par $\star$, l'application $h \star -$ se restreint-corestreint en une application injective de H dans H. Elle est bijective puisque H est fini. Nous en tirons qu'il existe un élément $e_h \in H$ tel que $h \star e_h = h$. La régularité de h dans G en déduit que $e_h = e_G$; le neutre appartient donc à H. Il existe alors un élément $h' \in H$ tel que $h \star h' = e_G$. Toujours par régularité dans G, nous en déduisons que $h' = h^{-1}$; le sous-ensemble H est stable par prise d'inverse.
3. Le monoïde $(\mathbb{N}, +)$, ou le sous-ensemble $\mathbb{N}$ du groupe $\mathbb{Z}$ fournissent des contre-exemples pour des deux questions précédentes, si l'on ôtait l'hypothèse de finitude.
4. Soit $m \in M$. Nous posons successivement un inverse à gauche m_1 de m, puis un inverse à gauche m_2 de m_1. L'associativité de $\star$ permet d'écrire
$$m_2 = m_2 \star (m_1 \star m) = (m_2 \star m_1) \star m = m.$$
En particulier, l'élément m_1 est également un inverse à droite de m. Nous avons démontré que tout inverse à gauche était également inverse à droite. Il en découle que deux tels inverses doivent coïncider [1].

1. Attention, nous avions besoin qu'ils soient tous inverses à gauche et à droite pour conclure à l'unicité des inverses.

Exercice 2. Vrai/Faux, première édition

Pour chaque affirmation qui suit, démontrer sa véracité ou trouver un contre-exemple :

1. Le groupe $\mathbb{Z}$ est produit de deux groupes non triviaux.
2. Soit G un groupe. Si G a un nombre fini de sous-groupes, alors G est fini.

Correstion de l'exercice 2

1. **Faux.**
   L'intersection de deux sous-groupes non triviaux de $\mathbb{Z}$ est non trivial. Supposons que
   $$\mathbb{Z} \xrightarrow[\iota]{\sim} G \times H.$$
   Les sous-groupes $\iota^{-1}(G \times \{e\})$ et $\iota^{-1}(\{e\} \times H)$ sont d'intersection triviale. Il en découle que l'un des deux est trivial, i.e. que G ou H est trivial.
2. **Vrai.**
   Soit G un groupe avec un nombre fini de sous-groupes. Un élément d'ordre infini de G correspond à un sous-groupe isomorphe à $\mathbb{Z}$. Le groupe G admettrait alors une infinité de sous-groupes, correspondant aux $n\mathbb{Z}$ pour $n \geq 1$. Nous avons démontré que tout élément de G est d'ordre fini. Les sous-groupes $\langle g \rangle$ pour $g \in G$ sont donc finis, en nombre fini [2]. Puisque ces sous-groupes recouvrent G, le groupe G est fini.

2 Morphismes de groupes

Exercice 5. Autour de HK

Soient G un groupe, et H, K deux sous-groupes de G. Pour toute la suite, nous considérons l'application
$$f : H \times K \to G, \quad (h,k) \mapsto hk.$$

1. Démontrer que f est injective si, et seulement si, on a $H \cap K = \{e\}$.
2. Démontrer que $HK = \mathrm{Im}(f)$ est un sous-groupe de G si, et seulement si, on a $HK = KH$.
3. Démontrer que f est un morphisme de groupes si, et seulement si, on a
   $$\forall (h,k) \in H \times K, \ \ hk = kh.$$
4. En déduire une condition nécessaire et suffisante portant sur H et K pour que f soit un isomorphisme de groupes.

Correction de l'exercice 5

1. Si $H \cap K = \{e\}$, supposons que $f(h,k) = f(h',k')$. Cela se réécrit :
   $$hk = h'k'$$
   puis
   $$h'^{-1}h = k'k^{-1}.$$

2. Mais à ce stade, rien ne garantit qu'il n'y ai pas des redondances infinies.

Cet élément appartient alors à $H \cap K$, d'où

$$h'^{-1}h = k'k^{-1} = e$$

ce qui se réécrit

$$h = h' \text{ et } k = k'$$

et démontre l'injectivité [3].

Si en revanche $g \in H \cap K$, nous avons alors $f(g, e) = f(e, g)$ ce qui contredit l'injectivité.

2. L'ensemble des inverses d'un groupe est le groupe lui-même. Supposons que HK est un groupe. Nous obtenons la suite d'égalité suivante :

$$HK = (HK)^{-1} = K^{-1}H^{-1} = KH.$$

Réciproquement, supposons que $KH = HK$. Alors, pour tous couples $(h, k), (h', k') \in H \times K$, nous pouvons trouver $(k_1, h_1) \in K \times H$ tels que $kh' = h_1k_1$. Ceci permet d'écrire

$$(hk)(h'k') = h(kh')k' = h(h_1k_1)k' = (hh_1)(k_1k')$$

et de démontrer que HK est stable par produits. Il contient le neutre car $e = f(e, e)$. Enfin, pour tout couple $(h, k) \in H \times K$, l'hypothèse permet d'écrire $hk = k_2h_2$ avec $(k_2, h_2) \in K \times H$ puis

$$(hk)^{-1} = (k_2h_2)^{-1} = h_2^{-1}k_2^{-1} \in HK.$$

3. Si f est un morphisme de groupes, alors

$$\begin{aligned} kh &= f(e, k)f(h, e) \\ &= f((e, k)(h, e)) \\ &= f(h, k) \\ &= hk \end{aligned}$$

où nous avons utilisé l'hypothèse pour passer à la deuxième ligne.

Réciproquement, supposons la formule vérifiée. Pour tous couples $(h, k), (h', k') \in H \times K$, nous pouvons écrire

$$\begin{aligned} f((h, k)(h', k')) &= f((hh', kk')) \\ &= hh'kk' \\ &= (hk)(h'k') \\ &= f(h, k)f(h', k') \end{aligned}$$

où nous avons utilisé l'hypothèse pour passer à la troisième ligne.

4. L'application f est un isomorphisme de groupes si et seulement si c'est un morphisme de groupes injectif et surjectif. Les deux premières conditions se réécrivent au regard des questions 1 et 3. La surjectivité signifie exactement que $HK = G$. Ainsi, l'application f est un isomorphisme de groupes si et seulement si

$$H \cap K = \{e\},\ HK = G \text{ et } \forall (h, k) \in H \times K,\ hk = kh.$$

3. Attention, l'application f n'est pas un morphisme de groupes en général. Il ne suffit donc pas de regarder la préimage du neutre.

Exercice 11. Ordre de certaines puissances p-ièmes

Soient G un groupe, H l'un de ses sous-groupes et p un nombre premier. On pose $a \in G \backslash H$ tel que $a^p \in H$. Montrer que $\mathrm{ord}(a) = p\,\mathrm{ord}(a^p)$.

Correction de l'exercice 11

Si a est d'ordre infini, alors aucun $(a^p)^n$ ne peut être trivial donc a^p aussi. Si a est d'ordre fini, alors $(a^p)^{\mathrm{ord}(a)} = e$ donc a^p est d'ordre fini et nous avons que

$$\mathrm{ord}(a^p) = \frac{\mathrm{ord}(a)}{\mathrm{pgcd}(\mathrm{ord}, p)}.$$

Si le PGCD vaut 1, les éléments a et a^p ont même ordre. L'inclusion des sous-groupes $\langle a^p \rangle \subseteq \langle a \rangle$ ainsi que l'égalité de leur cardinaux entraîne que $\langle a \rangle = \langle a^p \rangle \subset H$. Ceci est impossible. Ainsi, $\mathrm{pgcd}(\mathrm{ord}(a), p) = p$ et l'on obtient l'identité souhaitée.

On propose aussi une preuve plus conceptuelle. Rappelons que l'ordre de a a été défini a partir du noyau du morphisme

$$\varphi_a : \mathbb{Z} \to G, \;\; n \mapsto a^n.$$

Puisque $e \in H$, le noyau de φ_a est contenu dans $\varphi_a^{-1}(H)$. Les hypothèses donnent des informations sur le sous-groupe $\varphi_a^{-1}(H)$ de $\mathbb{Z}$. Puisque $a \notin H$, ce sous-groupe ne contient pas 1 et puisque $a^p \in H$, ce sous-groupe contient p. Il s'agit donc de $p\mathbb{Z}$.

Le diagramme suivant est commutatif :

$$\begin{array}{ccc} \mathbb{Z} & \xrightarrow{\varphi_a} & G \\ {\scriptstyle p\times -}\downarrow & \nearrow_{\varphi_{a^p}} & \\ \mathbb{Z} & & \end{array}$$

et puisque $\mathrm{Ker}(\varphi_a) \subseteq p\mathbb{Z}$, l'inclusion $p\mathrm{Ker}(\varphi_{a^g}) \subseteq \mathrm{Ker}(\varphi_a)$ est une égalité. L'identité sur les ordres s'en déduit.

Exercice 12. Endomorphismes de certains produits

1. Soit G et G' deux groupes finis d'ordres premiers entre eux. Exhiber un isomorphisme de monoïdes

$$\mathrm{End}(G) \times \mathrm{End}(G') \cong \mathrm{End}(G \times G')$$

qui se restreint-corestreint en un isomorphisme si l'on remplace "endomorphisme" par "automorphisme".

Remarque : vous pouvez généraliser à une famille $(G_i)_{i\in I}$ de groupes d'exposants finis et deux à deux premiers entre eux et obtenir un isomorphisme

$$\prod_{i\in I} \mathrm{End}(G_i) \cong \mathrm{End}\left(\prod_{i\in I} G_i\right)$$

qui se restreint-corestreint pareillement.

2. Trouver un contre-exemple lorsque les ordres ne sont pas premiers entre eux.

Correction de l'exercice 12

1. Nous construisons d'abord l'application suivante :

$$\mathrm{End}(G) \times \mathrm{End}(G') \to \mathrm{End}(G \times G'), \quad (\varphi, \psi) \mapsto [(g, g') \mapsto (\varphi(g), \psi(g'))]$$

dont nous vérifions qu'elle est bien définie et fournit un morphisme de monoïdes injectif [4].

Il reste à démontrer sa surjectivité. Prenons un endomorphisme f de $G \times G'$. Si f est image de (φ, ψ), alors nous devrions avoir $f(G \times \{e\}) \subset G \times \{e\}$ et l'analogue pour $\{e\} \times G'$. Démontrons d'abord ces inclusions. Nous définissons le morphisme de groupes composé

$$\tilde{f} : G' \hookrightarrow G \times G' \xrightarrow{f} G \times G' \xrightarrow{p_1} G$$

où la première flèche est l'inclusion canonique et la dernière la projection sur le premier facteur. Soit $g' \in G'$. L'ordre de son image divise l'ordre de g' donc $|G'|$. Puisqu'elle appartient à G, son ordre doit également diviser $|G|$ ce qui implique que son ordre est 1. Ainsi, notre composée est triviale. À présent, il est possible d'écrire pour tout $(g, g') \in G \times G'$:

$$\begin{aligned}(p_1 \circ f)(g, g') &= f(g, e) f(e, g') \\ &= f(g, e)\tilde{f}(g') \\ &= (p_1 \circ f)(g, e)\end{aligned}$$

Nous définissons alors par $\varphi = (p_1 \circ f)(-, e)$ un endomorphisme de G. Symétriquement, nous définissons par $\psi = (p_2 \circ f)(e, -)$ un endomorphisme de G'. Il se trouve que

$$\begin{aligned}f(g, g') &= ((p_1 \circ f)(g, g'), (p_2 \circ f)(g, g')) \\ &= ((p_1 \circ f)(g, e), (p_2 \circ f)(e, g')) \\ &= (\varphi(g), \psi(g'))\end{aligned}$$

où l'égalité de la première ligne est tautologique, le passage à le première ligne provient du calcul précédent, et celui à la dernière de la définition de φ et ψ.

Nous appelons dans la suite $\varphi \times \psi$ l'image de (φ, ψ). Pour démontrer la restriction-corestriction, vérifier les deux identités

$$\mathrm{Im}(\varphi \times \psi) = \mathrm{Im}(\varphi) \times \mathrm{Im}(\psi)$$

$$\mathrm{Ker}(\varphi \times \psi) = \mathrm{Ker}(\varphi) \times \mathrm{Ker}(\psi).$$

2. Pour trouver un contre-exemple, considérer que $G = G' = \mathbb{Z}/2\mathbb{Z}$. Le groupe d'automorphismes de $\mathbb{Z}/2\mathbb{Z}$ est trivial. En revanche, celui de $(\mathbb{Z}/2\mathbb{Z})^2$ ne l'est pas puisqu'il contient l'inversion des coordonnées $(x, y) \mapsto (y, x)$.

Correction de la remarque : la remarque est plus subtile que le cas d'un produit de deux groupes. En effet, il n'est pas possible de décomposer tout élément de $\prod_I G_i$ comme produit fini d'éléments avec une seule coordonnée non triviale. Pour conclure, nous considérons pour $j \in I$ la composée

$$\tilde{f} : \prod_{i \neq j} G_i \to \prod_I G_i \xrightarrow{f} \prod_I G_i \xrightarrow{p_j} G_j.$$

Soit n_j l'exposant de G_j. Puisqu'il est premier à tous les exposants de G_i, la puissance n_j-ième est une bijection de $\prod_{i \neq j} G_i$. Soit u dans ce dernier produit, que nous écrivons v^{n_j}. Nous avons

$$\tilde{f}(u) = \tilde{f}(v)^{n_j} = e$$

car G_j est d'exposant n_j. Le reste est identique.

4. N'hésitez pas à demander si vous souhaitez que je rédige les détails.

Exercice 17. Le groupe $(\mathbb{Z}/n\mathbb{Z})^\times$

Le but de cet exercice est de déterminer, pour tout entier n, la structure du groupe des inversibles $(\mathbb{Z}/n\mathbb{Z})^\times$. Nous commençons par essayer de dévisser le problème.

1. Soient A, B deux anneaux dont on notera $+$ et $\times$ les lois. On appelle morphisme d'anneaux une application de A dans B qui est un morphisme de groupes additifs et de monoïdes multiplicatifs. Ceci équivaut aux trois formules

$$\forall a, a' \in A,\ \ f(a+a') = f(a) + f(a'),\ \ f(aa') = f(a)f(a') \text{ et } f(1) = 1.$$

   Démontrer l'égalité suivante entre les sous-ensembles de $A \times B$:

$$(A \times B)^\times = A^\times \times B^\times.$$

2. Remarquer que l'isomorphisme du théorème des restes choinois est un morphisme d'anneaux. En déduire que pour $\text{pgcd}(n, m) = 1$, le groupe $(\mathbb{Z}/nm\mathbb{Z})^\times$ est isomorphe à $(\mathbb{Z}/n\mathbb{Z})^\times \times (\mathbb{Z}/m\mathbb{Z})^\times$.
3. Retrouver ce résultat en utilisant l'exercice 12.

La question précédente permet de se ramener au cas $n = p^k$. Nous allons démontrer que pour tout nombre premier impair p, nous avons

$$\left(\mathbb{Z}/p^k\mathbb{Z}\right)^\times \cong \mathbb{Z}/p^{k-1}(p-1)\mathbb{Z}$$

puis que

$$\forall k \geq 2,\ \ \left(\mathbb{Z}/2^k\mathbb{Z}\right)^\times \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{k-2}\mathbb{Z}.$$

4. Démontrer que $(\mathbb{Z}/p^k\mathbb{Z})^\times$ contient un élément d'ordre $p-1$.
5. Démontrer pour tout entier $r \geq 1$,

$$\forall (a, b) \in \mathbb{Z}^2,\ \ a \equiv b \mod p^r \implies a^p \equiv b^p \mod p^{r+1}.$$

   En déduire pour tout premier p l'ordre de $\overline{1+p}$ dans $(\mathbb{Z}/p^k\mathbb{Z})^\times$.
6. Conclure si $p \neq 2$.
7. Traiter le cas $p = 2$.
8. En guise d'application, déterminer les entiers naturels $n \geq 1$ tels que $(\mathbb{Z}/n\mathbb{Z})^\times$ est cyclique.

Correction de l'exercice 17

1. Nous écrivons la suite d'équivalence formelle qui démontre cette égalité de sous-ensembles de $A \times B$:

$$\begin{aligned}(a,b) \in (A\times B)^\times &\Leftrightarrow \exists (a',b') \in (A\times B),\ \ (a,b)(a',b') = (1,1)\\ &\Leftrightarrow \exists (a',b') \in (A\times B),\ \ aa' = 1 \text{ et } bb' = 1\\ &\Leftrightarrow (\exists a' \in A,\ aa' = 1) \text{ et } (\exists b' \in B,\ bb' = 1)\\ &\Leftrightarrow (a,b) \in A^\times \times B^\times\end{aligned}$$

2. L'isomorphisme de groupes des restes chinois est donné par

$$\mathbb{Z}/nm\mathbb{Z} \xrightarrow{\sim} \left(\mathbb{Z}/n\mathbb{Z}\right) \times \left(\mathbb{Z}/m\mathbb{Z}\right),\ \ k \bmod nm \mapsto (k \bmod n, k \bmod m)$$

   et dire qu'il s'agit d'un morphisme d'anneaux équivaut à dire que

$$\forall (k,l) \in \mathbb{Z}^2,\ (kl \bmod n) = (k \bmod n)(\bmod n)$$

   ainsi que son analogue pour m. En appliquant la première question à cette isomorphisme d'anneaux, on conclut.

3. On se souvient (cf. le corollaire 3.7 du polycopié) que le morphisme de groupes

$$\left(\mathbb{Z}/n\mathbb{Z}\right)^\times \to \mathrm{Aut}\left(\mathbb{Z}/n\mathbb{Z}\right),\ \ x \mapsto [\overline{k} \mapsto x\overline{k}]$$

est un isomorphisme, dont l'inverse s'écrit $\varphi \mapsto \varphi(\overline{1})$. Dans le cas où $\mathrm{pgcd}(n,m) = 1$, nous pouvons appliquer l'exercice 12 pour obtenir l'isomorphisme de groupes

$$\mathrm{Aut}\left(\mathbb{Z}/n\mathbb{Z}\right) \times \mathrm{Aut}\left(\mathbb{Z}/m\mathbb{Z}\right) \xrightarrow{\sim} \mathrm{Aut}\left(\mathbb{Z}/nm\mathbb{Z}\right)$$

qui s'interprète ensuite comme l'isomorphisme désiré.

4. Le groupe $(\mathbb{Z}/p\mathbb{Z})^\times$ étant cyclique d'ordre $p-1$, nous choisissons un élément a de $\mathbb{Z}/p^k\mathbb{Z}$ tel que $(a \bmod p)$ est d'ordre $p-1$. Soit $n \geq 1$ tel que $a^n = 1$. Ceci implique que

$$(a \bmod p)^n = 1.$$

Puisque $(a \bmod p)$ est d'ordre $p-1$, il en découle que $p-1|n$. Ceci étant vrai pour tout entier n tel que $a^n = 1$, nous en déduisons que $p-1$ divise l'ordre de a. En définissant l'entier m par $\mathrm{ord}(a) = (p-1)m$, l'élément a^m qui est d'ordre $(p-1)m/\mathrm{pgcd}((p-1)m, m) = p-1$.

5. Soit $r \geq 1$ et $(a,b) \in \mathbb{Z}^2$ tels que $a \equiv b \bmod p^r$. Nous réécrivons a^p en utilisant le binôme de Newton comme

$$\begin{aligned} a^p &= (b + (a-b))^p \\ &= b^p + \sum_{k=1}^{p-1} \binom{k}{p} (a-b)^k b^{p-k} + (a-b)^p \end{aligned}$$

Chaque terme de la somme est divisible par p^{r+1} puisque $p^r|(a-b)$ et que p divise le coefficient binomial. Le dernier terme est divisible par $(p^r)^2$, donc par p^{r+1} puisque $r \geq 1$ et $p \geq 2$. Nous obtenons bien la congruence $a^p \equiv b^p \bmod p^{r+1}$.

Par conséquent, puisque $1 + p \equiv 1 \bmod p$, une application récursive de l'implication précédente démontre que $(1+p)^{p^{k-1}} \equiv 1 \bmod p^k$. L'ordre de $\overline{1+p}$ divise ainsi p^{k-1} ; pour conclure qu'il s'agit effectivement de p^{k-1}, il va cependant falloir être plus fins.

Raffinons le calcul précédent en supposant que b est premier à p, que p^{r+1} ne divise pas $a-b$.

$$a^p - b^p = p(a-b)b^{p-1} + (a-b)^2 \left(\sum_{k=2}^{p-1} \binom{k}{p} (a-b)^{k-2} b^{p-k} \right) + (a-b)^p$$

Le premier terme est divisible par p^{r+1} mais pas par p^{r+2}. Dans la somme, chaque coefficient binomial est divisible par p ce qui implique que la somme est divisible par p^{2r+1} et en particulier par p^{r+2}. Le dernier terme est divisible par p^{rp} : lorsque p est impair ou que $r \geq 2$, nous avons $rp \geq r+2$ ce qui implique que le terme est divisible par p^{r+2}. Toutes ces informations ensemble démontrent que $a^p - b^p$ est divisible par p^{r+1} mais pas par p^{r+2}.

Puisque $1+p$ est congru à 1 modulo p mais pas modulo p^2, une application récursive du raffinement précédent affirme que $(1+p)^{p^{k-2}}$ n'est pas congru à 1 modulo p^k. L'ordre de $\overline{1+p}$ ne divise donc pas p^{k-2}, ce qui conclut :

$$\mathrm{ord}(\overline{1+p}) = p^{k-1}.$$

Lorsque $p = 2$, nous voyons en revanche que $(1+2)^2$ est congru à 1 modulo 2^3 mais pas 2^4. Nous pouvons ensuite appliquer récursivement le premier calcul et son raffinement pour démontrer que $(1+2)^{2^{k-2}}$ est congru à 1 modulo 2^k mais pas $(1+2)^{2^{k-3}}$. L'ordre de $\overline{3}$ dans $(\mathbb{Z}/2^k\mathbb{Z})^\times$ est 2^{k-2}.

6. Lorsque $p \neq 2$, nous avons trouvé un élément a d'ordre $p-1$ et l'élément $(1+p)$ d'ordre p^{k-1}. Les sous-groupes multiplicatifs $\langle 1 \rangle$ et $\langle \overline{1+p} \rangle$ sont d'intersection triviales puisque les ordres de leurs

éléments sont premiers entre eux. Puisqu'ils sont dans un groupe abélien, ils vérifient les hypothèses des questions 1) et 3) de l'exercice 5. Ceci fournit un morphisme de groupes injectif

$$\mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}/p^{k-1}\mathbb{Z} \cong \langle a \rangle \times \langle \overline{1+p} \rangle \hookrightarrow \left(\mathbb{Z}/p^k\mathbb{Z}\right)^\times.$$

Par cardinalité, ce morphisme est surjectif ; c'est un isomorphisme de groupes. Le théorème des restes chinois affirme enfin que la source est isomorphe à $\mathbb{Z}/p^{k-1}(p-1)\mathbb{Z}$ ce qui conclut.

7. Le cas $k = 2$ étant évident, nous supposons $k \geq 3$. La question 5) nous a permis de démontré en particulier que pour tout entier $l \geq 2$, nous avons $3^{2^l} \equiv 1 \bmod 8$. Ceci vaut en particulier pour $3^{2^{k-3}}$ qui est l'unique élément d'ordre 2 dans $\langle 3 \rangle$. Cet élément ne vaut donc pas -1. Les sous-groupes $\langle -1 \rangle$ et $\langle 3 \rangle$ vérifient les hypothèses des questions 1) et 3) de l'exercice 5 ; nous définissons ainis un morphisme de groupes injectif
$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{k-2}\mathbb{Z} \to \left(\mathbb{Z}/2^k\mathbb{Z}\right)^\times$$
qui est un isomorphisme pour des raisons de cardinalité.

Remarque : vous verrez bientôt que la structure des groupes abéliens de type fini nous permettait d'éviter d'exhiber -1, en nous contentant de démontrer que $(\mathbb{Z}/2^k\mathbb{Z})^\times$ n'est pas cyclique. Vous pouvez réfléchir à une manière de démontrer de manière élémentaire qu'un groupe abélien d'ordre 2^l non cyclique avec un élément d'ordre 2^{l-1} est isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{l-1}\mathbb{Z}$.

8. Rappelons deux faits : tout sous-groupe d'un groupe cyclique est cyclique ; le produit de deux groupes cycliques est cyclique si et seulement si leurs ordres sont premiers entre eux. Si l'on écrit $n = 2^v \prod_I p_i^{v_i}$ avec les p_i distincts et les $v_i \geq 1$, nous avons un isomorphisme
$$\left(\mathbb{Z}/n\mathbb{Z}\right)^\times \cong \left(\mathbb{Z}/2^v\mathbb{Z}\right)^\times \times \prod_I \left(\mathbb{Z}/p_i^{v_i-1}(p_i-1)\mathbb{Z}\right)$$
Si $v = 0, 1$ le premier facteur est trivial. Ainsi, il faut et suffit que les $p_i^{v_i-1}(p_i-1)$ soient premier entre eux, ce qui se réécrit en disant que les $(p_i)_{\{i \,|\, v_i \geq 2\}}$ et les $(p_i - 1)_{i \in I}$ sont premiers entre eux. Si I est de cardinal supérieur à 2, ceci est impossible puisque les $p_i - 1$ sont pairs.

Si $v \geq 2$, le premier facteur contient une copie de $\mathbb{Z}/2\mathbb{Z}$. Puisque chaque $p_i - 1$ est pair, il faut que I soit vide pour que $(\mathbb{Z}/n\mathbb{Z})^\times$ soit cyclique. De plus, pour $v \geq 3$, le groupe n'est pas cyclique (cf. sa description en question 7)).

Finalement, les entiers n qui conviennent sont les puissances de premiers impairs, leur doubles et les cas particuliers 1,2 et 4.