Enoncés : Michel Emsalem,
Corrections : Pierre Dèbes

Groupes, sous-groupes, ordre

Exercice 1

On dispose d'un échiquier et de dominos. Les dominos sont posés sur l'échiquier soit horizontalement, soit verticalement de façon à couvrir deux cases contiguës. Est-il possible de couvrir ainsi entièrement l'échiquier à l'exception des deux cases extrèmes, en haut à gauche et en bas à droite ? Reprendre cette question dans le cas où l'on exclut deux cases quelconques à la place des deux cases extrèmes ci-dessus.

Indication ▼ [002101]

Exercice 2

(I) Soit X un ensemble et $\mathscr{P}(X)$ l'ensemble des parties de X ordonné par l'inclusion. Soit φ une application croissante de $\mathscr{P}(X)$ dans lui-même.

(a) Montrer que l'ensemble E des parties A de X qui vérifient $\varphi(A) \subset A$ est non vide et admet un plus petit élément A_0.

(b) Montrer que $\varphi(A_0) = A_0$.

(II) Soit deux ensembles X et Y munis de deux injections g de X dans Y et h de Y dans X.

(a) Montrer que l'application de $\mathscr{P}(X)$ dans lui-même défini par

$$\varphi(A) = X - h(Y - g(A))$$

est croissante.

(b) Déduire de ce qui précède qu'il existe une bijection de X sur Y.

Indication ▼ Correction ▼ [002102]

Exercice 3

Soit X un ensemble non vide et ordonné. Montrer qu'il existe une partie Y totalement ordonnée de X qui vérifie la propriété

$$\forall x \notin Y \quad \exists y \in X \quad x \text{ et } y \text{ non comparables}$$

L'ensemble Y est-il unique ?

Correction ▼ [002103]

Exercice 4

Un jardinier doit planter 10 arbres en 5 rangées de 4 arbres. Donner une disposition possible. Quel est le nombre minimal d'arbres dont il doit disposer pour planter 6 rangées de 5 arbres ? Généraliser.

Indication ▼ [002104]

Exercice 5

Soit n et p deux entiers, $p \leq n$. Démontrer, grâce à un dénombrement, la formule suivante :

$$\sum_{0 \leq k \leq p} C_n^k C_{n-k}^{p-k} = 2^p C_n^p$$

Indication ▼ [002105]

Exercice 6

Soit n un entier impair non divisible par 3. Montrer que 24 divise $n^2 - 1$.

Indication ▼ [002106]

Exercice 7

On considère sur $\mathbb{R}$ la loi de composition définie par $x \star y = x + y - xy$. Cette loi est-elle associative, commutative ? Admet-elle un élément neutre ? Un réel x admet-il un inverse pour cette loi ? Donner une formule pour la puissance n-ième d'un élément x pour cette loi.

Indication ▼ Correction ▼ [002107]

Exercice 8

Soit E un monoïde unitaire. On dit qu'un élément a de E admet un *inverse à gauche* (resp. *inverse à droite*) s'il existe $b \in E$ tel que $ba = e$ (resp. $ab = e$).

(a) Supposons qu'un élément a admette un inverse à gauche b qui lui-même admet un inverse à gauche. Montrer que a est inversible.

(b) Supposons que tout élément de E admette un inverse à gauche. Montrer que E est un groupe.

Correction ▼ [002108]

Exercice 9

Soit E un ensemble muni d'une loi $\star$ associative
(i) admettant un élément neutre à gauche e (i.e. $\forall x \in E \quad e \star x = x$) et
(ii) tel que tout élément possède un inverse à gauche (i.e. $\forall x \in E \quad \exists y \in E \quad y \star x = e$).
Montrer que E est un groupe pour la loi $\star$.

Indication ▼ Correction ▼ [002109]

Exercice 10

Les rationnels non nuls forment-ils un sous-groupe multiplicatif de $\mathbb{R}^\times$?

Indication ▼ [002110]

Exercice 11

Montrer que l'ensemble $\{2^n \mid n \in \mathbb{Z}\}$ est un sous-groupe multiplicatif de $\mathbb{Q}^*$, ainsi que l'ensemble $\{\frac{1+2m}{1+2n} \mid n, m \in \mathbb{Z}\}$.

Indication ▼ [002111]

Exercice 12

Montrer que l'ensemble des matrices carrées à n lignes et n colonnes de déterminant non nul est un groupe pour la multiplication.

Indication ▼ [002112]

Exercice 13

On considère l'ensemble E des matrices carrées à coefficients réels de la forme

$$\begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix}, \quad a \in \mathbb{R}^\times, \quad b \in \mathbb{R}$$

muni du produit des matrices.

(a) Montrer que E est ainsi muni d'une loi de composition interne associative.

(b) Déterminer tous les éléments neutres à droite de E.

(c) Montrer que E n'admet pas d'élément neutre à gauche.

(d) Soit e un élément neutre à droite. Montrer que tout élément de E possède un inverse à gauche pour cet élément neutre, i.e.

$$\forall g \in E \quad \exists h \in E \quad hg = e$$

Indication ▼ [002113]

Exercice 14

Soit G un groupe vérifiant

$$\forall x \in G \quad x^2 = e$$

Montrer que G est commutatif. Déduire que si G est fini, alors l'ordre de G est une puissance de 2.

Correction ▼ [002114]

Exercice 15

Soit G un groupe d'ordre pair. Montrer qu'il existe un élément $x \in G$, $x \neq e$ tel que $x^2 = e$.

Indication ▼ Correction ▼ [002115]

Exercice 16

Soit G un groupe d'ordre impair. Montrer que l'application f de G sur lui-même donnée par $f(x) = x^2$ est une bijection. En déduire que l'équation $x^2 = e$ a une unique solution, à savoir $x = e$.

Indication ▼ [002116]

Exercice 17

Soient G un groupe fini et m un entier premier à l'ordre de G. Montrer que pour tout $a \in G$ l'équation $x^m = a$ admet une unique solution.

Indication ▼ [002117]

Exercice 18

Soit G un groupe et $H < G$, $K < G$ deux sous-groupes de G. On suppose qu'il existe deux éléments $a, b \in G$ tels que $Ha \subset Kb$. Montrer que $H < K$.

Correction ▼ [002118]

Exercice 19

Soit H une partie non vide d'un groupe G. On pose $H^{-1} = \{x^{-1}; x \in H\}$. Montrer les équivalences suivantes :

(a) $H < G \Leftrightarrow HH^{-1} \subset H$

(b) $H < G \Leftrightarrow \forall a \in H \quad Ha = H$.

Indication ▼ [002119]

Exercice 20

Soit G un groupe et H, K deux sous-groupes de G.

(a) Montrer que $H \cup K$ est un sous-groupe de G si et seulement si $H < K$ ou $K < H$.

(b) Montrer qu'un groupe ne peut être la réunion de deux sous-groupes propres.

Correction ▼ [002120]

Exercice 21

Montrer que dans un groupe G, toute partie non vide finie stable par la loi de composition est un sous-groupe. Donner un contre-exemple à la propriété précédente dans le cas d'une partie infinie.

Correction ▼ [002121]

Exercice 22

(a) Montrer que les seuls sous-groupes de $\mathbb{Z}$ sont de la forme $n\mathbb{Z}$ où n est un entier.

(b) Un élément x d'un groupe est dit d'ordre fini s'il existe un entier k tel que $x^k = e_G$. Montrer que $\{k \in \mathbb{Z} \mid x^k = e_G\}$ est alors un sous-groupe non nul de $\mathbb{Z}$. On appelle ordre de x le générateur positif de ce sous-groupe.

(c) Soit x un élément d'un groupe G. Montrer que x est d'ordre d si et seulement si le sous-groupe $< x >$ de G engendré par x est d'ordre d.

Indication ▼ [002122]

Exercice 23

On pose $SL_2(\mathbb{Z}) = \{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid a,b,c,d \in \mathbb{Z}, ad-bc = 1\}$.

(a) Montrer que $SL_2(\mathbb{Z})$ est un sous-groupe du groupe des matrices inversibles à coefficients dans $\mathbb{Z}$.

(b) On considère les deux matrices

$$\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \quad \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix}$$

Démontrer que A et B sont d'ordres finis mais que AB est d'ordre infini.

Indication ▼ [002123]

Exercice 24

Soit G un groupe abélien et a et b deux éléments d'ordres finis. Montrer que ab est d'ordre fini et que l'ordre de ab divise le ppcm des ordres de a et b. Montrer que si les ordres de a et b sont premiers entre eux, l'ordre de ab est égal au ppcm des ordres de a et de b.

Correction ▼ [002124]

Exercice 25

Soit G un groupe commutatif. Montrer que l'ensemble des éléments d'ordre fini de G forme un sous-groupe de G.

Indication ▼ [002125]

Exercice 26

Déterminer tous les sous-groupes de $\mu_2 \times \mu_2$.

Indication ▼ [002126]

Exercice 27

Soient G un groupe fini et commutatif et $\{G_i\}_{i\in I}$ la famille des sous-groupes propres maximaux de G. On pose $F = \bigcap_{i\in I} G_i$. Montrer que F est l'ensemble des éléments a de G qui sont tels que, pour toute partie S de G contenant a et engendrant G, $S - \{a\}$ engendre encore G.

Correction ▼ [002127]

Exercice 28

Déterminer tous les groupes d'ordre ≤ 5. En déduire qu'un groupe non commutatif possède au moins 6 éléments. Montrer que le groupe symétrique S_3 est non commutatif.

Indication ▼ [002128]

Exercice 29

Le centre d'un groupe G est l'ensemble $Z(G)$ des éléments de G qui commutents à tous les éléments de G. Vérifier que $Z(G)$ est un sous-groupe abélien de G. Montrer que si G possède un unique élément d'ordre 2, alors cet élément est dans le centre $Z(G)$.

Indication ▼ [002129]

Exercice 30

Soient G un groupe et H et K deux sous-groupes de G.

(a) Montrer que l'ensemble $HK = \{xy \mid x \in H, y \in K\}$ est un sous-groupe de G si et seulement si $HK = KH$.

(b) Montrer que si H et K sont finis alors $|HK| = \dfrac{|H| \cdot |K|}{|H \cap K|}$.

Correction ▼ [002130]

Exercice 31

Déterminer tous les sous-groupes du groupe symétrique S_3.

Correction ▼ [002131]

Exercice 32

Montrer que dans un groupe d'ordre 35, il existe un élément d'ordre 5 et un élément d'ordre 7.

Indication ▼ Correction ▼ [002132]

Exercice 33

Soit G un groupe d'ordre $2p$ avec p un nombre premier. Montrer qu'il existe un élément d'ordre 2 et un élément d'ordre p.

Correction ▼ [002133]

Exercice 34

Soient $n \geq 0$ un entier et p un nombre premier tels que p divise $2^{2^n} + 1$. Montrer que p est de la forme $p = k2^{n+1} + 1$ où k est un entier.

Indication ▼ Correction ▼ [002134]

Exercice 35

Montrer que tout entier $n > 0$ divise toujours $\varphi(2^n - 1)$ (où φ est la fonction indicatrice d'Euler).

Indication ▼ Correction ▼ [002135]

Indication pour l'exercice 1 ▲

Considérer la couleur des cases exclues.

Indication pour l'exercice 2 ▲

Pour la question (II) (b) on considèrera la partie A_0 minimale associée à φ et l'on montrera que A_0 et $h(Y - g(A_0))$ forment une partition de X. La bijection sera définie par g sur A_0 et par h^{-1} sur $h(Y - g(A_0))$.

Indication pour l'exercice 4 ▲

Ne voir dans le mot "rangée" qu'une condition d'alignement.

Indication pour l'exercice 5 ▲

Compter, dans un ensemble E à n éléments, le nombre de parties à p éléments obtenues en réunissant une partie X à k éléments à une partie à $p-k$ éléments du complémentaire de X dans E, k décrivant $\{0,\dots,p\}$.

Indication pour l'exercice 6 ▲

$n^2 - 1 = (n-1)(n+1)$ et $24 = 2^3 \cdot 3$.

Indication pour l'exercice 7 ▲

Les premières questions ne présentent aucune difficulté.
Pour la dernière, le plus difficile (et le plus intéressant) est de deviner la formule. Pour cela, calculer la puissance n-ième pour $n = 1,2,3,4,5\dots$. (La formule est donnée dans la page "Corrections").

Indication pour l'exercice 9 ▲

On pourra montrer les points suivants :
(a) $x \star y = e \Rightarrow y \star x = e$
(b) L'élément neutre à gauche est unique.
(c) L'élément neutre à gauche est un élément neutre à droite aussi.
(d) Tout élément est inversible.

Indication pour l'exercice 10 ▲

Oui.

Indication pour l'exercice 11 ▲

Aucune difficulté.

Indication pour l'exercice 12 ▲

Pour l'existence d'un inverse pour toute matrice $n \times n$ de déterminant non nul, noter que $\det(A) \neq 0$ entraîne que la matrice A est inversible (comme matrice) et que la matrice A^{-1}, qui est de déterminant $1/\det(A) \neq 0$ est alors l'inverse de A pour le groupe en question.

Indication pour l'exercice 13 ▲

Aucune difficulté.

Indication pour l'exercice 15 ▲

Considérer la partition de G en sous-ensembles du type $\{x, x^{-1}\}$.

Indication pour l'exercice 16 ▲

On commence par montrer que f est surjective, en notant que si $|G| = 2m+1$, alors pour tout $y \in G$ on a $y = (y^{m+1})^2$.

Indication pour l'exercice 17 ▲

$x^m = a \Leftrightarrow x = a^u$ où $um + v|G| = 1$.

Indication pour l'exercice 19 ▲

Standard.

Indication pour l'exercice 22 ▲

Pour le (c), introduire le morphisme $\mathbb{Z} \to < x >$ qui associe nx à tout entier $n \in \mathbb{Z}$. Ce morphisme est surjectif et de noyau $d\mathbb{Z}$ où d est l'ordre de x.

Indication pour l'exercice 23 ▲

Aucune difficulté.

Indication pour l'exercice 25 ▲

Conséquence de l'exercice 24.

Indication pour l'exercice 26 ▲

$\{1\}, \mu_2 \times \{1\}, \{1\} \times \mu_2, \{(1,1),(i,i)\}, \mu_2 \times \mu_2$.

Indication pour l'exercice 28 ▲

Standard.

Indication pour l'exercice 29 ▲

Pour la seconde question, noter que si x est d'ordre 2 dans G, alors yxy^{-1} l'est aussi, pour tout $y \in G$.

Indication pour l'exercice 32 ▲

Commencer par analyser l'ordre possible des éléments de G.

Indication pour l'exercice 34 ▲

Trouver l'ordre de 2 dans $(\mathbb{Z}/p\mathbb{Z})^\times$.

Indication pour l'exercice 35 ▲

Trouver l'ordre de 2 modulo $2^n - 1$.

Correction de l'exercice 2 ▲

(I) (a) $E \neq \emptyset$ car $X \in E$. L'ensemble $A_0 = \bigcap_{A \in E} A$ est de manière évidente le plus petit élément de E.

(b) On a $\varphi(A_0) \subset A_0$ puisque $A_0 \in E$. On déduit, par la croissance de φ, que $\varphi(\varphi(A_0)) \subset \varphi(A_0)$, ce qui donne $\varphi(A_0) \in E$ et donc $A_0 \subset \varphi(A_0)$.

(II) (a) La croissance de φ est immédiate.

(b) Considérons la partie A_0 associée à φ. D'après le (b) du (I), on a $X \setminus h(X \setminus g(A_0)) = A_0$. Autrement dit, les parties A_0 et $h(X \setminus g(A_0))$ constituent une partition de X. Considérons l'application $f : X \to X$ définie comme étant g sur A_0 et h^{-1} sur $h(Y \setminus g(A_0))$. On voit sans difficulté que f est une bijection (noter que les images respectives des deux restrictions précédentes sont $g(A_0)$ et $Y \setminus g(A_0)$ et qu'elles constituent une partition de Y).

Correction de l'exercice 3 ▲

Pour tout $x \in X$, posons $C(x) = \{y \in X \mid x \text{ et } y \text{ sont comparables}\}$ et considérons $Y = \bigcap_{x \in X} C(x)$. La partie Y est totalement ordonnée puisque dès que $y, y' \in Y$, alors $y' \in C(y)$ et donc y et y' sont comparables. De plus, pour tout $x \notin Y$, il existe $y \in X$ tel que $x \notin C(y)$, c'est-à-dire, y et x non comparables.

Il n'y a pas unicité de l'ensemble Y en général. En effet, dans un ensemble ordonné où il existe un élément y qui n'est comparable qu'à lui-même, on peut prendre $Y = C(y) = \{y\}$. Il est facile de construire des ensembles ordonnés possédant plusieurs tels éléments y (penser à la relation d'égalité, dont le graphe est la diagonale).

Correction de l'exercice 7 ▲

Pour la dernière question, vérifier par récurrence que $x^{\star\, n} = \sum_{k=1}^{n} (-1)^{k-1} C_n^k x^k$.

Correction de l'exercice 8 ▲

(a) Désignant par b l'inverse à gauche de a et par c l'inverse à gauche de b, on a $ab = (cb)(ab) = c(ba)b = cb = e$. L'élément b est donc l'inverse de a.

(b) découle immédiatement de (a).

Correction de l'exercice 9 ▲

(a) Pour $x, y \in E$ quelconques, notons x' et y' leurs inverses à gauche respectifs. Si $xy = e$, on a aussi $yx = (x'x)yx = x'(xy)x = x'x = e$.

(b) Soit f un élément neutre à gauche. On a donc $fe = e$. D'après (a), on a aussi $ef = e$, c'est-à-dire $f = e$.

(c) Pour tout $x \in E$, on a $xe = x(x'x) = (xx')x = x$ puisque d'après (a), $xx' = e$.

(d) résulte alors de (a), (b) et (c).

Correction de l'exercice 14 ▲

Pour tous $x, y \in G$, on a $xyx^{-1}y^{-1} = xyxy = (xy)(xy) = 1$ c'est-à-dire $xy = yx$. Donc G est abélien. Si G est fini, il peut être considéré comme espace vectoriel sur le corps $\mathbb{Z}/2\mathbb{Z}$, et est alors nécessairement de dimension finie, ce qui donne G isomorphe comme espace vectoriel à $(\mathbb{Z}/2\mathbb{Z})^n$ et donc $|G| = 2^n$.

Correction de l'exercice 15 ▲

En groupant chaque élément $x \in G$ avec son inverse x^{-1}, on obtient une partition de G en sous-ensembles $\{y, y^{-1}\}$ qui ont deux éléments sauf si $y = y^{-1}$, c'est-à-dire si $y^2 = e$. L'élément neutre e est un tel élément y. Ce ne peut pas être le seul, sinon G serait d'ordre impair.

Correction de l'exercice 18 ▲

Pour tout $h \in H$, on a $ha = k_h b$ pour un certain $k_h \in K$. En écrivant $ha = h(ea) = hk_e b$, on obtient $k_h = hk_e$, ce qui donne $h = k_h (k_e)^{-1} \in K$.

Correction de l'exercice 20 ▲

(a) Supposons que $H \cup K$ soit un sous-groupe de G et que H ne soit pas inclus dans K, c'est-à-dire, qu'il existe $h \in H$ tel que $h \notin K$. Montrons que $K \subset H$. Soit $k \in K$ quelconque. On a $hk \in H \cup K$. Mais $hk \notin K$ car sinon $h = (hk)k^{-1} \in K$. D'où $hk \in H$ et donc $k = h^{-1}(hk) \in H$.

(b) découle immédiatement de (a).

Correction de l'exercice 21 ▲

Soit H une partie finie non vide de G stable par la loi de composition. Pour montrer que H est un sous-groupe, il reste à voir que pour tout $x \in H$, $x^{-1} \in H$. Les puissances x^k où $k \in \mathbb{N}$ restant dans H, il existe $m, n \in \mathbb{N}$ tels que $m > n$ et $x^m = x^n$. On a alors $x^{m-n-1} \cdot x = 1$, soit $x^{-1} = x^{m-n-1}$, ce qui montre que $x^{-1} \in H$.

Si H est infini, la propriété précédente n'est pas vraie en général. Par exemple $\mathbb{N}$ est une partie stable de $\mathbb{Z}$ pour l'addition mais n'en est pas un sous-groupe.

Correction de l'exercice 24 ▲

Soient $a, b \in G$ d'ordre respectifs m et n. Posons $\mu = \mathrm{ppcm}(m,n)$. On a $(ab)^\mu = a^\mu \cdot b^\mu = e \cdot e = e$ ($a^\mu = b^\mu = e$ résultant du fait que m et n divisent μ). L'ordre de ab divise donc μ.

Supposons que $\mathrm{pgcd}(m,n) = 1$. Soit $k \in \mathbb{Z}$ tel que $(ab)^k = 1$, soit $a^k = b^{-k}$. On en déduit que $a^{nk} = e$ et $b^{mk} = e$. D'où $m|nk$ et $n|mk$. L'hypothèse $\mathrm{pgcd}(m,n) = 1$ donne alors $m|k$ et $n|k$ et donc $\mathrm{ppcm}(m,n)|k$. Cela combiné à la première partie montre que ab est d'ordre $\mathrm{ppcm}(m,n) = mn$.

Correction de l'exercice 27 ▲

Etant donné $a \in F$, soit S une partie de G contenant a et engendrant G. Si $< S - \{a\} > \neq G$, alors il existe un sous-groupe propre maximal G_i tel que $< S - \{a\} > \subset G_i$. Mais alors $< S > \subset < S - \{a\} >< a > \subset G_i$. Contradiction, donc $< S - \{a\} > \neq G$.
Inversement, supposons que $a \notin F$, c'est-à-dire, il existe $i \in I$ tel que $a \notin G_i$. Alors pour $S = G_i \cup \{a\}$, on a $< S >= G$ (par maximalité de G_i) mais $< S - \{a\} >= G_i \neq G$.

Correction de l'exercice 30 ▲

(a) ($\Rightarrow$) Si HK est un groupe, pour tous $h \in H$ et $k \in K$, on a $(hk)^{-1} = k^{-1}h^{-1} \in HK$ et donc $kh \in (HK)^{-1} = K^{-1}H^{-1} = KH$. D'où $HK \subset KH$. L'autre inclusion s'obtient similairement.
($\Leftarrow$) On vérifie aisément en utilisant l'hypothèse $HK = KH$ que $(HK) \cdot (HK) \subset HK$ et que $(HK)^{-1} \subset HK$.

(b) Etant donnés $h_0, h \in H$ et $k_0, k \in K$, on a $h_0k_0 = hk$ si et seulement si $h_0^{-1}h = k_0k^{-1}$. Cet élément est nécessairement dans l'intersection $H \cap K$. On a donc $h_0k_0 = hk$ si et seulement s'il existe $u \in H \cap K$ tel que $h = h_0u$ et $k = u^{-1}k_0$. Pour chaque élément fixé $h_0k_0 \in HK$, il y a donc $|H \cap K|$ façons de l'écrire hk avec $(h,k) \in H \times K$. D'où le résultat.

Correction de l'exercice 31 ▲

D'après le théorème de Lagrange, les sous-groupes de S_3 sont d'ordre 1, 2, 3 ou 6. Les sous-groupes d'ordre 1 et 6 sont les sous-groupes triviaux $\{1\}$ et S_3 respectivement. Comme 2 et 3 sont premiers, les sous-groupes d'ordre 2 et 3 sont cycliques. Un sous-groupe d'ordre 2 est tout sous-groupe engendré par une transposition : il y en a 3. Il existe un seul sous-groupe d'ordre 3, celui engendré par le 3-cycle $(1\,2\,3)$.

Correction de l'exercice 32 ▲

Les éléments différents de 1 sont d'ordre 5, 7 ou 35. S'il existe un élément g d'ordre 35 (*i.e.*, si le groupe est cyclique d'ordre 35), alors g^5 est d'ordre 7 et g^7 est d'ordre 5. Supposons que le groupe n'est pas cyclique et qu'il n'existe pas d'élément d'ordre 7. Tout élément différent de 1 serait alors d'ordre 5 et le groupe serait réunion de sous-groupes d'ordre 5. Mais de tels sous-groupes sont soit égaux soit d'intersection $\{1\}$ (car 5 est premier). On aurait alors $35 = 4n+1$ avec n le nombre de sous-groupes distincts d'ordre 5, ce qui donne la contradiction cherchée. Le raisonnement est le même s'il n'existe pas d'élément d'ordre 5.

Correction de l'exercice 33 ▲

Si $p = 2$ alors $|G|$ est d'ordre 4 : G est le groupe de Klein $(\mathbb{Z}/2\mathbb{Z})^2$ dont tous les éléments différents de 1 sont d'ordre 2. On peut donc supposer pour la suite que p est impair. En procédant comme dans l'exercice 32, on montre qu'il existe forcément dans G un élément d'ordre 2. Enfin si tous les éléments différents de 1 étaient d'ordre 2, alors d'après l'exercice 14, l'ordre de G serait une puissance de 2. Il existe donc aussi un élément d'ordre p.

Correction de l'exercice 34 ▲

On a $2^{2^n} \equiv -1$ modulo p. On en déduit que $2^{2^{n+1}} \equiv 1$ modulo p. Ces deux conditions donnent que l'ordre de 2 dans $(\mathbb{Z}/p\mathbb{Z})^\times$ est 2^{n+1}. Cet ordre devant diviser l'ordre de $(\mathbb{Z}/p\mathbb{Z})^\times$, c'est-à-dire $p-1$, on obtient le résultat souhaité.

Correction de l'exercice 35 ▲

Comme $2^n \equiv 1$ modulo $2^n - 1$, l'ordre de 2 modulo $2^n - 1$, disons m, divise n. Si $m < n$, on aurait $2^m \equiv 1$ modulo $2^n - 1$, c'est-à-dire $2^n - 1$ divise $2^m - 1$, ce qui n'est pas possible. L'ordre de 2 modulo $2^n - 1$ est donc n, et celui-ci doit diviser l'ordre de $(\mathbb{Z}/(2^n-1)\mathbb{Z})^\times$, qui vaut $\varphi(2^n - 1)$.