FEUILLES D'EXERICES N°1

Groupes

1. Exercices

Exercice 1. (Solution)
On munit l'ensemble $G = \{x, y, z, t\}$ d'une loi de composition interne dont la table est

$\star$	x	y	z	t
x	z	x	z	x
y	x	t	z	y
z	z	z	z	z
t	x	y	z	t

(La première ligne se lit $x \star x = z$, $x \star y = x$, $x \star z = z$, etc.)

1) Cette loi possède-t-elle un élément neutre ?

2) Cette loi est-elle commutative ?

3) Cette loi est-elle associative ?

4) Est-ce une loi de groupe ?

Exercice 2. (Solution)
Soient les quatre fonctions f_i $(1 \leq i \leq 4)$ de $\mathbb{R} \setminus \{0\}$ dans $\mathbb{R} \setminus \{0\}$ définies par :

$$f_1(x) = x,\ f_2(x) = \frac{1}{x},\ f_3(x) = -x \text{ et } f_4(x) = -\frac{1}{x},\ \text{pour tout } x \in \mathbb{R} \setminus \{0\}.$$

Montrer que $G = \{f_1, f_2, f_3, f_4\}$ est un groupe pour la loi $\circ$. Est-il abélien ?

Exercice 3. (Solution)

1) Dresser les tables d'addition et de multiplication de $\mathbb{Z}/4\mathbb{Z}$.

2) L'ensemble $\mathbb{Z}/4\mathbb{Z} \setminus \{\overline{0}\}$ muni de la loi $\cdot$ est-il un groupe ?

3) Mêmes questions pour $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}$ et $\mathbb{Z}/5\mathbb{Z}$.

Exercice 4. (Solution)
Soit le groupe $G = \mathbb{Z}/12\mathbb{Z}$ (muni de l'addition).

1) Déterminer le sous-groupe H de G engendré par $\overline{6}$ et $\overline{8}$ et déterminer son ordre.

2) Déterminer les générateurs de G.

3) Quel est l'ordre de l'élément $\overline{9}$ dans G ?

Exercice 5. (Solution)
Soit un entier $n \geq 2$. Si $k \in \mathbb{Z}$, on note $\overline{k}$ la classe de k dans $\mathbb{Z}/n\mathbb{Z}$ et on note G l'ensemble des éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$ muni de la multiplication.

1) Montrer qu'un élément $\overline{k}$ de $\mathbb{Z}/n\mathbb{Z}$ est inversible pour la multiplication si et seulement si les entiers k et n sont premiers entre eux.

2) Montrer que G est un groupe.

3) Montrer que $G = \mathbb{Z}/n\mathbb{Z} \setminus \{\overline{0}\}$ si et seulement si n est premier.

4) On pose $n = 10$.

(1) Donner la liste des éléments de G.
(2) Quel est l'ordre de $\overline{3}$ dans G ?
(3) Le groupe G est-il cyclique ?

5) Même question avec $n = 8$.

Exercice 6. (Solution)
Pour tout $n \geq 1$, on note $U_n = \{z \in \mathbb{C} \mid z^n = 1\}$ l'ensemble des racines n-ièmes de l'unité de $\mathbb{C}$.

1) Montrez que $U_n = \{e^{2i\pi k/n} \mid 0 \leq k \leq n-1\}$. Représentez géométriquement U_6.

2) Montrez que U_n est un groupe pour la multiplication et qu'il est d'ordre n.

3) Déterminez les ordres des éléments de U_6.

4) Montrez que U_n est cyclique pour tout $n \geq 1$.

Exercice 7. (Solution)
Soient G un groupe, H et K deux sous-groupes de G.

1) Montrez que $H \cap K$ est un sous-groupe de G.

2) Montrez que $H \cup K$ est un sous-groupe de G si et seulement si $H \subseteq K$ ou $K \subseteq H$.

Exercice 8. (Solution)
Soient G un groupe et $x \in G$ un élément d'ordre n. Quel est l'ordre de x^2? (Indication : distinguez les cas n pair et n impair.)

Exercice 9. (Solution)
Soit G un groupe fini d'ordre pair. Montrer que G contient un élément d'ordre 2. (Indication : considérez $\{x \in G \mid x \neq x^{-1}\}$).

Exercice 10. (Solution)
Soient G un groupe fini, g un élément de G d'ordre n.

1) Montrer que pour tous entiers $1 \leq k, \ell \leq n$,

$$g^k = g^\ell \Rightarrow k = \ell.$$

2) Montrer que si $h, h' \in G$ alors soit $\{hg, \ldots, hg^n\}$ et $\{h'g, \ldots, h'g^n\}$ sont deux sous-ensembles à n éléments de G qui sont soit égaux, soit d'intersection vide.

3) En déduire que n divise l'ordre de G.

4) À l'aide de l'Exercice 5, déduire de ce qui précède le petit théorème de Fermat: si p est un nombre premier et si a est un entier quelconque, alors $a^p - a$ est un multiple de p.

Exercice 11. (Solution)
Soient σ_1 et σ_2 les permutations de $\mathfrak{S}_5$ suivantes :

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{pmatrix} \text{ et } \sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 2 & 1 \end{pmatrix}.$$

Calculer les signatures de σ_1, σ_2, σ_1^{-1} et $\sigma_1 \circ \sigma_2$.

Exercice 12. (Solution)
On considère les permutations suivantes de $\mathfrak{S}_{10}$:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 7 & 1 & 4 & 2 & 6 & 9 & 8 & 5 & 10 \end{pmatrix},$$

$$\varphi = (10, 3, 4, 1)\,(8, 7)\,(4, 7)\,(5, 6)\,(2, 6)\,(2, 9)\,.$$

1) Trouver la décomposition en produit de cycles à supports disjoints, la signature, l'ordre et une décomposition en produit de transpositions de σ et φ.

2) Calculer σ^{2020} et φ^{2020}.

Exercice 13. (Solution)

Soit un entier $n \geq 2$. On désigne par $\varepsilon(\sigma)$ la signature d'une permutation σ de $\mathfrak{S}_n$.

1) Montrer que l'on a $\displaystyle\sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) = 0$.

2) Calculer $\displaystyle\sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma)\sigma(1)\sigma(2)$.

Indication pour les deux questions : remplacer σ par $\sigma \circ (1,2)$.

Exercice 14. (Solution)

Soit un entier $n \geq 1$. Dans $\mathbb{R}^n$, on désigne par $(e_1, ..., e_n)$ la base canonique. À une permutation $\sigma \in \mathfrak{S}_n$, on associe l'endomorphisme u_σ de $\mathbb{R}^n$ suivant :

$$u_\sigma \ : \ \begin{array}{ccc} \mathbb{R}^n & \to & \mathbb{R}^n \\ (x_1, \ldots, x_n) & \mapsto & (x_{\sigma^{-1}(1)}, \ldots, x_{\sigma^{-1}(n)}) \end{array}$$

1) Pour tout $i \in \{1, \ldots, n\}$ déterminer $u_\sigma(e_i)$. En déduire la matrice de u_σ dans la base canonique.

2) Montrer que pour tous $\sigma, \sigma' \in \mathfrak{S}_n$, $u_\sigma \circ u_{\sigma'} = u_{\sigma \circ \sigma'}$. En déduire que u_σ est inversible et déterminer u_σ^{-1}.

Exercice 15. (Solution)

Si n est un entier naturel et a un entier relatif, on note $a[n]$ la classe de a dans $\mathbb{Z}/n\mathbb{Z}$. Soient deux entiers $p, q \geq 2$.

1) Supposons p et q premiers entre eux. Montrer que l'application

$$\begin{array}{ccc} \mathbb{Z}/pq\mathbb{Z} & \to & \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \\ n[pq] & \mapsto & (n[p], n[q]) \end{array}$$

est bien définie et est un morphisme d'anneaux bijectif.

2) En déduire le nombre de solutions de l'équation $x^2 + \overline{2}x - \overline{3} = \overline{0}$ dans $\mathbb{Z}/91\mathbb{Z}$.

2. Solutions

Solution 1. (Enoncé)
1) On voit en utilisant la table de G que t est un élément neutre.
2) Le tableau est symétrique par rapport à la diagonale donc la loi est commutative.
3) Il s'agit de vérifier que $(a \star b) \star c = a \star (b \star c)$ pour tout $(a, b, c) \in \{x, y, z, t\}^3$. Si un des éléments vaut z, alors c'est immédiat car les deux membres valent z. De même, si un éléments vaut t, alors l'égalité est vérifiée. Par commuativité, il suffit donc de le vérifier pour $a = x$ et $b = y$, et la vérification est immédiate.
4) On voit que l'élément z n'a pas d'inverse car aucun élément $a \in \{x, y, z, t\}$ ne vérifie $a \star z = t$ donc la loi $\star$ n'est pas une loi de groupe sur G.

Solution 2. (Enoncé)
L'associativité de $\circ$ a été prouvée en première année. Pour vérifier si G est un groupe, on peut établir sa table de Cayley :

$\circ$	f_1	f_2	f_3	f_4
f_1	f_1	f_2	f_3	f_4
f_2	f_2	f_1	f_4	f_3
f_3	f_3	f_4	f_1	f_2
f_4	f_4	f_3	f_2	f_1

On voit alors que la loi $\circ$ sur G est interne, que l'élément f_1 est neutre pour $\circ$ et que chaque élément possède un symétrique (lui même) donc G est bien un groupe. De plus, le tableau est symétrique par rapport à la diagonale et donc G est un groupe abélien.

Solution 3. (Enoncé)
1)

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{1}$	$\overline{2}$

et

$\times$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{0}$	$\overline{2}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

2) Non, car cette loi n'est pas interne, $\overline{2} \times \overline{2} = \overline{0} \notin \mathbb{Z}/4\mathbb{Z} \setminus \{0\}$.

3) Pour $\mathbb{Z}/2\mathbb{Z}$:

$+$	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{1}$
$\overline{1}$	$\overline{1}$	$\overline{0}$

et

$\times$	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$

.

L'ensemble $\mathbb{Z}/2\mathbb{Z} \setminus \{\overline{0}\} = \{\overline{1}\}$ est bien un groupe pour $\times$.

Pour $\mathbb{Z}/3\mathbb{Z}$:

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{1}$

et

$\times$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{1}$

.

L'ensemble $\mathbb{Z}/3\mathbb{Z} \setminus \{\overline{0}\} = \{\overline{1}, \overline{2}\}$ est bien un groupe pour $\times$.

Pour $\mathbb{Z}/5\mathbb{Z}$:

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$

et

$\times$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{1}$	$\overline{3}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{1}$	$\overline{4}$	$\overline{2}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

.

L'ensemble $\mathbb{Z}/5\mathbb{Z} \setminus \{\overline{0}\} = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}\}$ est bien un groupe pour $\times$.

Solution 4. (Enoncé)
1) Ce sous groupe contient $\overline{2} = \overline{8} - \overline{6}$. Donc H contient $\{\overline{2}, \overline{4}, \overline{6}, \overline{8}, \overline{10}\}$ et on vérifie que cet ensemble est bien sous-groupe donc il y a égalité.
2) Un élément $x \in G$ engendre G si et seulement s'il est d'ordre $|G| = 12$. On vérifie alors à la main que les générateurs de G sont $\overline{1}, \overline{5}, \overline{7}, \overline{11}$.
3) On calcule, $2 \cdot \overline{9} = \overline{18} = \overline{6}$, $3 \cdot \overline{9} = \overline{27} = \overline{3}$ et $4 \cdot \overline{9} = \overline{36} = \overline{0}$ donc l'élément $\overline{9}$ est d'ordre 4.

Solution 5. (Enoncé)
1) Supposons $\overline{k}$ inversible pour la multiplication, alors il existe $\overline{r} \in \mathbb{Z}/n\mathbb{Z}$ tel que $\overline{k}\overline{r} = \overline{1}$ *i.e.* $\overline{kr} = \overline{1}$. Donc n divise $kr - 1$, il existe un entier a tel que $kr - an = 1$ et donc k et n sont premiers entre eux par la réciproque du théorème de Bézout. Inversement, si k et n sont premiers entre eux, par le théorème de Bésout, il existe des entiers a et b tels que $ak + bn = 1$ et donc $\overline{a}\overline{k} = \overline{k}\overline{a} = \overline{1}$ et donc $\overline{k}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$.
2) L'associativité de $\times$ sur G est immédiate. Montrons que la multiplication est bien une loi interne. Si $(\overline{k}, \overline{r}) \in G^2$, alors $k \wedge n = 1$ et $r \wedge n = 1$, donc $kr \wedge n = 1$, en effet si ce n'était pas le cas, en prenant p premier qui divise n et kr, le lemme d'Euclide assurerait que p divise k ou p divise r et ces deux cas sont impossibles par hypothèse. Ensuite, on vérifie facilement que $\overline{1} \in G$ est bien l'élément neutre pour la multiplication, et que tout élément $\overline{k} \in G$ admet un inverse dans G par définition de G.
3) Si $G = \mathbb{Z}/n\mathbb{Z} \setminus \{0\}$, alors tout élément $k \in [\![1; n-1]\!]$ est premier avec n, donc n est premier car si $n = ab$ avec $a < n$, alors a divise n et a premier avec n donc $a = 1$ *i.e.* n n'admet pas de diviseurs autre que 1 et lui même. Inversement, si n est premier, tout élément $k \in [\![1; n]\!]$ est premier avec n et donc $G = \setminus \{0\}$.
4) (1) Les éléments de $[\![1; 10]\!]$ premier avec 10 sont $1, 3, 7, 9$ donc :

$$G = \{\overline{1}, \overline{3}, \overline{7}, \overline{9}\}$$

(2) On calcule : $\overline{3}^2 = \overline{9}$, $\overline{3}^3 = \overline{27} = \overline{7}$, $\overline{3}^4 = \overline{21} = \overline{1}$ donc $\overline{3}$ est d'ordre 4.
(3) le groupe G est de cardinal 4 et $\overline{3} \in G$ est d'ordre $4 = |G|$ donc G est cyclique.
5) (1) Les éléments de $[\![1; 8]\!]$ premier avec 8 sont $1, 3, 5, 7$ donc :

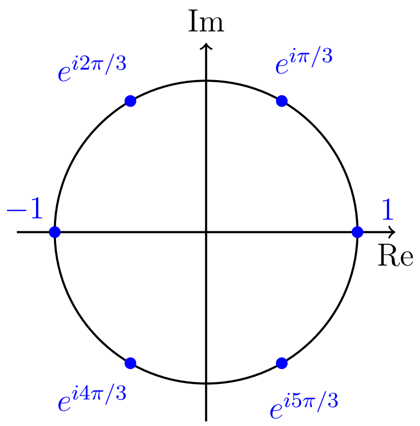
$$G = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}$$

(2) On calcule : $\overline{3}^2 = \overline{9} = \overline{1}$ donc $\overline{3}$ est d'ordre 2.
(3) le groupe G est de cardinal 4 et on peut montrer que $\overline{1}$ est d'ordre 1, et que $\overline{3}, \overline{5}, \overline{7}$ sont d'ordre 2 donc aucun élément de G n'est d'ordre $|G|$ et donc G n'est pas cyclique.

Solution 6. (Enoncé)
1) Il est clair que tout élément de la forme $z = e^{2i\pi k/n}$ vérifie $z^n = 1$. Inversement, Soit $z \in \mathbb{C}$ tel que $z^n = 1$, alors z n'est pas nul, en écrivant $z = re^{i\theta}$, il vient $r^n = 1$ et $e^{in\theta} = 1$. Donc $r = 1$ car $r > 0$ et $n\theta = m\pi$ avec $m \in \mathbb{Z}$. En écrivant $m = nq + k$ avec $0 \leq k \leq n-1$ la division euclidienne de m par n, il vient :

$$z = e^{i\pi m/n} = e^{i\pi \frac{nq+k}{n}} = e^{i\pi k/n} \in \{e^{2i\pi k/n} \mid 0 \leq k \leq n-1\},$$

et cela conclut.
La représentation graphique de U_6 est donnée ci-dessous.



2) L'ensemble U_n est clairement d'ordre n car tous les éléments $e^{2i\pi k/n}$, $0 \leq k \leq n-1$ sont distincts. Montrons que U_n est un sous-groupe de $(\mathbb{C}^*, \times)$. On a $1^n = 1$ donc $1 \in U_n$ donc U_n contient l'élément neutre. De plus, pour $(z, z') \in U_n^2$,

$$(zz'^{-1})^n = z^n(z'^{-1})^n = 1((z')^n)^{-1} = 1 \times 1 = 1$$

donc $zz'^{-1} \in U_n$ et finalement, U_n est bien un sous-groupe de $(\mathbb{C}^*, \times)$.
3) On a $U_6 = \left\{1, e^{i\pi/3}, e^{2i\pi/3}, -1, e^{4i\pi/3}, e^{5i\pi/3}\right\}$. En calculant les puissances successives de chaque éléments, on trouve que :

- 1 est d'ordre 1.
- -1 est d'ordre 2.
- $e^{2i\pi/3}$ et $e^{4i\pi/3}$ sont d'ordre 3.
- $e^{i\pi/3}$ et $e^{5i\pi/3}$ sont d'ordre 6.

4) L'élément $e^{2i\pi/n} \in U_n$ est d'ordre $n = |U_n|$ donc U_n est cyclique.

Solution 7. (Enoncé)
1) On a $e \in H$ et $e \in K$ car H et K sont des sous-groupes de G donc $e \in H \cap K$ et donc $H \cap K$ contient l'élément neutre de G. Soit maintenant $(x, y) \in (H \cap K)^2$, alors $x, y \in H$ et $x, y \in K$, donc comme H est un sous-groupe de G, $xy^{-1} \in H$. De même $xy^{-1} \in K$ et donc $xy^{-1} \in H \cap K$ et $H \cap K$ est bien un sous-groupe de G.
2) Si $H \subseteq K$, alors $H \cup K = K$ est un sous-groupe de G. De même, si $K \subseteq H$ alors $H \cup K = H$ est un sous-groupe de G.
Inversement, supposons que l'on a ni $H \subseteq K$ et ni $K \subseteq H$ et montrons que $H \cup K$ n'est pas un sous-groupe de G. Par hypothèse, on peut trouver $x \in K \setminus H$ (car K n'est pas inclus dans H) et $y \in H \setminus K$ (car H n'est pas inclus dans K), alors $(x, y) \in (H \cup K)^2$. Il suffit de montrer que $xy \notin H \cup K$. Si $xy \in H$, alors :

$$x = \underbrace{(xy)}_{\in H} \underbrace{y^{-1}}_{\in H} \in H$$

car H est un sous-groupe de G, ce qui contredit la définition de x. De même, si $xy \in K$, alors :

$$y = \underbrace{x^{-1}}_{\in K} \underbrace{xy}_{\in K} \in K$$

car K est un sous-groupe de G, ce qui contredit la définition de y. Donc $H \cup K$ n'est pas stable par la loi de G et donc n'est pas un sous-groupe de G.

Solution 8. (Enoncé)
Si $n = 2k$ est pair, alors $(x^2)^k = x^{2k} = x^n = e$ donc x^2 est d'ordre au plus k. Montrons que x^2 est d'ordre exactement k. Si $(x^2)^d = e$, alors $x^{2d} = e$ donc $n = 2k$ divise $2d$ donc k divise d et donc $d \geq k$: x^2 est bien d'ordre k.

Si $n = 2k+1$ est impair montrons que x^2 est d'ordre n. Déjà, on a $(x^2)^n = x^{2n} = (x^n)^2 = e^2 = e$. Enfin, si $(x^2)^d = e$, alors $x^{2d} = e$ donc n divise $2d$ par le cours. Mais comme n est impair, $n \wedge 2 = 1$ et le lemme de GAUSS assure que n divise d et donc x^2 est bien d'ordre n.

Solution 9. (Enoncé)
Soit $X = \{x \in G \mid x \neq x^{-1}\}$, montrons que X est de cardinal pair. Si $X = \emptyset$, alors $|X| = 0$ est pair. Sinon, pour $x \in X$, alors $x^{-1} \in X$ car :

$$(x^{-1})^{-1} = x \neq x^{-1}.$$

Donc X est de la forme $\{x_1, x_1^{-1}, \dots, x_k, x_k^{-1}\}$ pour un $k \geq 1$, donc $|X| = 2k$ est pair.
Comme G est de cardinal pair, $|X^c| = |G| - |X|$ est aussi pair. Or $X^c = \{x \in G \mid x = x^{-1}\}$ et $e \in X^c$ donc $|X^c| \geq 2$. Soit $x \in X^c$ avec $x \neq e$. Alors $x = x^{-1}$ donc (en multipliant par x des deux côtés) $x^2 = e$ et donc x est d'ordre 2 et cela conclut.

Solution 10. (Enoncé)
1) Quitte à échanger le rôle de l et k, on peut supposer $k \geq l$, on a alors $g^{k-l} = e$ donc n divise $k - l$, mais comme $0 \leq k - l < n$ nécessairement $k - l = 0$ et donc $k = l$.
2) Si $hg^k = hg^l$, alors $g^k = g^l$ en simplifiant par h, alors $k = l$ par la question **1)** et donc l'ensemble $\{hg, \dots, hg^n\}$ contient bien n éléments. Montrons d'abord que :

$$\{hg, \dots, hg^n\} \subset \{hg^j \mid j \in \mathbb{Z}\},$$

l'inclusion directe est claire. Pour l'inclusion réciproque, soit hg^j, $j \in \mathbb{Z}$ dans l'ensemble de droite, alors en faisant la division euclidienne de j par n, on peut écrire $j = nq + r$ avec $r \in [\![0; n-1]\!]$. On a alors :

$$hg^j = hg^{nq}g^r = hg^r,$$

si $1 \leq r \leq n-1$ alors $hg^j \in \{hg, \dots, hg^n\}$. Si $r = 0$, alors $hg^j = h = hg^n \in \{hg, \dots, hg^n\}$.
Si $\{hg, \dots, hg^n\} \cap \{h'g, \dots, h'g^n\} \neq \emptyset$, alors en prenant $hg^k = h'g^l$ un élément dans l'intersection, il vient $h = h'g^{l-k}$ et donc :

$$\begin{aligned}
\{hg, \dots, hg^n\} &= \{hg^j \mid j \in \mathbb{Z}\} \\
&= \{h'g^{l-k+j} \mid j \in \mathbb{Z}\} \\
&= \{h'g^{j'} \mid j' \in \mathbb{Z}\} \quad \text{(L'application } j \mapsto l-k+j \text{ est une bijection de } \mathbb{Z} \text{ dans } \mathbb{Z}) \\
&= \{h'g, \dots, h'g^n\}
\end{aligned}$$

et donc les deux ensembles sont bien égaux.
3) Par la question précédente, on peut écrire une partition de G de la forme $G = \sqcup_{i=1}^r \{h_i g, \dots, h_i g^n\}$ avec $(h_1, \dots, h_r) \in G^r$. Donc :

$$|G| = \sum_{i=1}^r |\{h_i g, \dots, h_i g^n\}| = \sum_{i=1}^r n = nr$$

et donc n divise bien $|G|$.
4) Si p divise a, alors p divise $a^p - a$. Sinon $\overline{a} \in (\mathbb{Z}/p\mathbb{Z}) \setminus \{0\}$ est un groupe pour la multiplication d'après l'Exercice 5. Notons k l'ordre de $\overline{a}$ dans $(\mathbb{Z}/p\mathbb{Z}) \setminus \{0\}$, alors d'après la question **3)**, k divise $|(\mathbb{Z}/p\mathbb{Z}) \setminus \{0\}| = p - 1$ donc $\overline{a}^{p-1} = \overline{1}$. En multipliant par $\overline{a}$ il vient $\overline{a}^p = \overline{a}$ et donc $a^p - a$ est un multiple de p.

Solution 11. (Enoncé)
On décompose σ_1 et σ_2 en produit de cycles à supports disjoints et on trouve :

$$\sigma_1 = (1\ 3)(4\ 5) \text{ et } \sigma_2 = (1\ 3\ 5)(2\ 4)$$

donc comme la signature d'un l-cycle est $(-1)^{l-1}$ et que ε est un morphisme de groupes, il vient :

$$\varepsilon(\sigma_1) = \varepsilon((1\ 3))\varepsilon((4\ 5)) = (-1) \times (-1) = 1,$$

et

$$\varepsilon(\sigma_2) = \varepsilon((1\ 3\ 5))\varepsilon((2\ 4)) = 1 \times (-1) = -1.$$

De même, comme ε morphisme de groupes, il vient :

$$\varepsilon(\sigma_1^{-1}) = 1^{-1} = 1 \text{ et } \varepsilon(\sigma_1 \circ \sigma_2) = \varepsilon(\sigma_1) \times \varepsilon(\sigma_2) = 1 \times (-1) = -1.$$

Solution 12. (Enoncé)
1) La décomposition en produit de cycles à supports disjoints pour σ est :

$$\sigma = (1\ 3)(2\ 7\ 9\ 5)$$

donc comme ε un morphisme de groupes, σ est de signature $(-1)^{2-1} \times (-1)^{4-1} = 1$. L'ordre de σ est le ppcm des ordres des cycles qui interviennent dans la décomposition de cycles à supports disjoints, donc $o(\sigma) = \text{ppcm}(2, 4) = 4$. Pour écrire σ en produit de transpositions, on utilise la relation $(a_1\ \ldots\ a_k) = (a_1\ a_2)(a_2\ a_3)\ldots(a_{k-1}a_k)$ et il vient alors $\sigma = (1\ 3)(2\ 7)(7\ 9)(9\ 5)$.
La décomposition en produit de cycles à supports disjoints pour φ est :

$$\varphi = (1\ 10\ 3\ 4\ 8\ 7)(2\ 9\ 5\ 6)$$

donc $\varepsilon(\varphi) = (-1)^{6-1} \times (-1)^{4-1} = 1$ et $o(\varphi) = \text{ppcm}(6, 4) = 12$. Une décomposition de φ en produit de transpositions est $\varphi = (1\ 10)(10\ 3)(3\ 4)(4\ 8)(8\ 7)(2\ 9)(9\ 5)(5\ 6)$.
2) On sait que $2020 = 505 \times 4$ et $2020 = 12 \times 168 + 4$ donc :

$$\sigma^{2020} = (\sigma^4)^{505} = (\text{Id})^{505} = \text{Id},$$

et,

$$\begin{aligned}
\varphi^{2020} &= (\varphi^{12})^{168}\varphi^4 \\
&= \varphi^4 \\
&= (1\ 10\ 3\ 4\ 8\ 7)^4(2\ 9\ 5\ 6)^4 \\
&= (1\ 8\ 3)(10\ 7\ 4)\,\text{Id} \\
&= (1\ 8\ 3)(10\ 7\ 4)
\end{aligned}$$

où la deuxième égalité provient du fait que $(1\ 10\ 3\ 4\ 8\ 7)$ et $(2\ 9\ 5\ 6)$ commutent car ce sont des cycles à supports disjoints.

Solution 13. (Enoncé)
1) L'application :

$$\begin{aligned}
\Phi : \mathfrak{S}_n &\longrightarrow \mathfrak{S}_n \\
\sigma &\longmapsto \sigma \circ (1\ 2)
\end{aligned}$$

est bien définie (car $\sigma \circ (1\ 2) \in \mathfrak{S}_n$) et est bijective de bijection réciproque $\Phi^{-1} = \Phi$. En effet :

$$\forall \sigma \in \mathfrak{S}_n, \quad (\Phi \circ \Phi)(\sigma) = \Phi(\Phi(\sigma)) = \Phi(\sigma \circ (1\ 2)) = (\sigma \circ (1\ 2)) \circ (1\ 2) = \sigma \circ (1\ 2)^2 = \sigma = \text{Id}_{\mathfrak{S}_n}(\sigma),$$

d'où $\Phi \circ \Phi = \mathrm{Id}_{\mathfrak{S}_n}$ et $\Phi = \Phi^{-1}$. On a alors en notant $S = \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma)$:

$$\begin{aligned}
S &= \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) \\
&= \sum_{\sigma' \in \mathfrak{S}_n} \varepsilon(\Phi(\sigma')) \qquad \text{Changement d'indice } \sigma = \Phi(\sigma') \\
&= \sum_{\sigma' \in \mathfrak{S}_n} \varepsilon(\sigma' \circ (1\ 2)) \\
&= \sum_{\sigma' \in \mathfrak{S}_n} \varepsilon(\sigma')\varepsilon((1\ 2)) \qquad \text{car } \varepsilon \text{ est un morphisme de groupes} \\
&= \sum_{\sigma' \in \mathfrak{S}_n} \varepsilon(\sigma') \times (-1) \\
&= -\sum_{\sigma' \in \mathfrak{S}_n} \varepsilon(\sigma') \\
&= -S \qquad (\sigma' \text{ indice muet}).
\end{aligned}$$

Donc $S = -S$ *i.e.* $S = 0$.

2) On fait le même changement d'indice, en notant $T = \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma)\sigma(1)\sigma(2)$ on a :

$$\begin{aligned}
T &= \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma)\sigma(1)\sigma(2) \\
&= \sum_{\sigma' \in \mathfrak{S}_n} \varepsilon(\Phi(\sigma'))(\Phi(\sigma'))(1)(\Phi(\sigma'))(2) \qquad \text{Changement d'indice } \sigma = \Phi(\sigma') \\
&= \sum_{\sigma' \in \mathfrak{S}_n} \varepsilon(\sigma' \circ (1\ 2))(\sigma' \circ (1\ 2))(1)(\sigma' \circ (1\ 2))(2) \\
&= \sum_{\sigma' \in \mathfrak{S}_n} \varepsilon(\sigma')\varepsilon((1\ 2))\sigma'(2)\sigma'(1) \qquad (\sigma' \circ (1\ 2))(1) = \sigma'((1\ 2)(1)) = \sigma'(2) \\
&= \sum_{\sigma' \in \mathfrak{S}_n} \varepsilon(\sigma') \times (-1)\sigma'(1)\sigma'(2) \qquad \sigma'(1) \text{ et } \sigma'(2) \text{ sont des entiers donc commutent} \\
&= -\sum_{\sigma' \in \mathfrak{S}_n} \varepsilon(\sigma')\sigma'(1)\sigma'(2) \\
&= -T \qquad (\sigma' \text{ indice muet}).
\end{aligned}$$

Donc $T = -T$ *i.e.* $T = 0$.

Solution 14. (Enoncé)
On regarde d'abord un cas particulier $n = 3$. Alors en notant $e_1 = (1, 0, 0) = (x_1, x_2, x_3)$ et en prenant $\sigma = (1\ 2\ 3)$, alors $\sigma^{-1} = (1\ 3\ 2)$ et :

$$u_\sigma(e_1) = u((x_1, x_2, x_3)) = (x_{\sigma^{-1}(1)}, x_{\sigma^{-1}(2)}, x_{\sigma^{-1}(3)}) = (x_3, x_1, x_2) = (0, 1, 0) = e_2 = e_{\sigma(1)}.$$

On conjecture donc que $u_\sigma(e_i) = e_{\sigma(i)}$, montrons le dans le cas général.
On écrit $e_i = (x_1, \dots, x_n)$ avec $x_k = 1$ si $k = i$ et 0 sinon. Alors $u_\sigma(e_i) = (x_{\sigma^{-1}(1)}, \dots, x_{\sigma^{-1}(n)})$, comme u_σ permute les coordonnées, il est clair que $u_\sigma(e_i)$ est encore un vecteur de la base canonique, c'est donc un e_j pour $j \in [\![1; n]\!]$ à déterminer. Le 1 dans $e_j = u_\sigma(e_i)$ est en position j, or le 1 dans $(x_{\sigma^{-1}(1)}, \dots, x_{\sigma^{-1}(n)})$ et en position k telle que $\sigma^{-1}(k) = i$ soit encore $k = \sigma(i)$, donc $j = \sigma(i)$ et finalement $u_\sigma(e_i) = e_{\sigma(i)}$.
2) Il suffit de vérifier que $u_\sigma \circ u_{\sigma'}$ et $u_{\sigma \circ \sigma'}$ coïncident sur la base $(e_1, \dots, e_n)$. Or pour $i \in [\![1; n]\!]$:

$$(u_\sigma \circ u_{\sigma'})(e_i) = u_\sigma(u_{\sigma'}(e_i)) = u_\sigma(e_{\sigma'(i)}) = e_{\sigma(\sigma'(i))} = u_{\sigma \circ \sigma'}(e_i),$$

et cela conclut. On remarque enfin que $u_{\mathrm{Id}_{[\![1;n]\!]}} = \mathrm{Id}_{\mathbb{R}^n}$, donc u_σ est inversible d'inverse $u_{\sigma^{-1}}$ car :

$$u_\sigma \circ u_{\sigma^{-1}} = u_{\sigma^{-1}} \circ u_\sigma = u_{\sigma\circ\sigma^{-1}} = u_{\mathrm{Id}_{[\![1;n]\!]}} = \mathrm{Id}_{\mathbb{R}^n}$$

et cela conclut.

Solution 15. (Enoncé)

1) Notons f l'application. Pour montrer que f est bien définie, il faut montrer que si $n[pq] = m[pq]$ alors $f(n) = f(m)$. Si $n[pq] = m[pq]$, alors pq divise $n - m$, donc p divise $n - m$ et donc $n[p] = m[q]$. De même, $n[q] = m[q]$ et donc f est bien définie. Montrons que f est bijective, comme $|\mathbb{Z}/pq\mathbb{Z}| = |\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}| = pq$, il suffit de montrer que f est injective. Soit $(n[pq], n'[pq]) \in (\mathbb{Z}/pq\mathbb{Z})^2$ tels que $f(n) = f(n')$. Alors $n[p] = n'[p]$ donc p divise $n - n'$ et de même q divise $n - n'$. Comme p et q sont premiers entre eux, le lemme de Gauss assure que pq divise $n - n'$, donc $n[pq] = n'[pq]$, f est bien injective et donc bijective.

2) On a $91 = 13 \times 7$ et 7 et 13 sont premiers entre eux. Il s'agit donc de regarder le nombre de solutions de $x^2 + \overline{2}x - \overline{3}$ dans $\mathbb{Z}/13\mathbb{Z}$ et $\mathbb{Z}/7\mathbb{Z}$. Il y a $\overline{1}$ et $-\overline{3}$ comme racines évidentes et comme on regarde une équation de degré 2 dans un corps (car 7 et 13 sont premiers) ce sont les seules. Il y a donc 4 solutions dans $\mathbb{Z}/91\mathbb{Z}$ qui sont :

$$\{f^{-1}(1[13], 1[7])), f^{-1}((1[13], -3[7])), f^{-1}((-3[13], 1[7])), f^{-1}((-3[13], -3[7]))\}.$$

Remarque : On peut montrer que l'inverse de f (dans le cas $p = 13$ et $q = 7$) est donné par : $(a[13], b[7]) \mapsto -13a + 14b\ [91]$. Donc les solutions de l'équations dans $\mathbb{Z}/91\mathbb{Z}$ sont :

$$\{1[91],\ 36[91],\ 53[91],\ -3[91]\}.$$