Groupes

1 Groupes

Exercice 1. ♡* Soit G est un groupe fini de cardinal pair et de neutre e. Montrer qu'il existe au moins un élément $g \in G \setminus \}$ tel que $g^2 = e$.

Exercice 2. ♡* Soit G un ensemble muni d'une loi de composition interne . associative, qui possède un élément neutre à droite e (ie pour tout x de G, $x.e = x$) et tel que tout élément x possède un inverse à droite x' (ie $xx' = e$). Montrer que G est un groupe.

Exercice 3. ** Soit $(G, *)$ un groupe tel qu'il existe un entier $n \in \mathbb{N}^*$ pour lequel on a

$$\forall k \in \{n-1, n, n+1\},\ \forall (x, y) \in G^2,\ (x * y)^k = x^k * y^k.$$

Montrer que G est abélien.
Bonus : Le résultat est-il encore juste pour tout $k \in \{n-1, n\}$?

Exercice 4. ** Soit $(G, *)$ un groupe et $H \subset G$ une partie non vide finie de G. Montrer que H est un sous-groupe de G si et seulement si $\forall a, b \in H,\ a * b \in H$.

2 Sous-groupes

Exercice 5. * Soit H un sous-groupe strict de G. Déterminer le sous-groupe engendré par le complémentaire de H.

Exercice 6. ♡ Montrer que

$$\left\{x + y\sqrt{3} \mid x \in \mathbb{N}, y \in \mathbb{Z}, x^2 - 3y^2 = 1\right\}$$

est un sous-groupe de $(\mathbb{R}_+^\star, \times)$.

Exercice 7. * Soit $(G, \cdot)$ un groupe fini et A, B deux sous-groupes de G.
On note $AB = \{ab;\ a \in A,\ b \in B\}$. Montrer que AB est un sous-groupe de G si et seulement si $AB = BA$.

Exercice 8. ♡♡** On note $\mathrm{GL}_n(\mathbb{Z})$ l'ensemble des matrices de $\mathcal{M}_n(\mathbb{R})$, à coefficients dans $\mathbb{Z}$, qui sont inversibles et dont l'inverse est à coefficients dans $\mathbb{Z}$.

1. Démontrer que si M est à coefficients dans $\mathbb{Z}$, alors $M \in GL_n(\mathbb{Z})$ si et seulement si $\det(M) = \pm 1$.
2. En déduire que $\mathrm{SL}_n(\mathbb{Z})$ est un sous-groupe de $\mathrm{GL}_n(\mathbb{R})$.

Exercice 9. ***

1. Montrer que tout sous-groupe additif de $\mathbb{R}$ qui n'est pas monogène est dense dans $\mathbb{R}$.
2. Soit $x \in \mathbb{R} \setminus \mathbb{Q}$. Montrer qu'il existe une infinité de $(p, q) \in \mathbb{Z} \times \mathbb{N}^\star$ tels que

$$\left|x - \frac{p}{q}\right| < \frac{1}{q^2}$$

3. Montrer la divergence de la suite de terme général

$$u_n = \frac{1}{n \sin n}$$

3 Morphismes

Exercice 10. ♡* Soit $(G, *)$ un groupe. Montrer que l'application $\varphi : x \mapsto x^2$ est un endomorphisme de groupes ssi G est abélien.

Exercice 11. * Soit φ un morphisme d'un groupe fini $(G, *)$ vers $(\mathbb{C}^*, \times)$.
On suppose que φ n'est pas une application constante. Calculer

$$\sum_{x \in G} \varphi(x)$$

Exercice 12. ** Un sous-groupe H de $(G, .)$ est dit distingué si

$$\forall x \in H, \forall a \in G, axa^{-1} \in H$$

1. Montrer que le noyau d'un morphisme de groupes $\varphi : (G, .) \to (G', \star)$ est distingué, où $(G', \star)$ est un groupe.
2. Soient H, K deux sous-groupes de $(G, .)$ On suppose le sous-groupe H distingué, montrer que l'ensemble
$$HK = \{xy \mid x \in H, y \in K\}$$
est un sous-groupe de $(G, .)$.
3. Groupe quotient :
   (a) Soit H un sous-groupe de G. Montrer que la relation $a\mathcal{R}b$ si $a^{-1}b \in H$ définit une relation d'équivalence. Montrer que aH est la classe d'équivalence de a suivant $\mathcal{R}$.
   (b) On note $G/H = \{aH,\ a \in G\}$ l'ensemble des classe d'équivalence de $\mathcal{R}$.
   Montrer que si H est distingué, on peut définir une loi de compsoition interne sur G/H en posant pour tous a, $a' \in G$, $aH * bH = (ab)H$.
   Montrer que de plus l'application de G dans G/H définie par $g \mapsto gH$ est un morphisme de groupes. Quel est son noyau ?

Exercice 13. ♡* Pour tout $\theta \in \mathbb{R}$, montrer que les ensembles

$$G = \{\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix},\ \theta \in \mathbb{R}\} \text{ et } G' = \{\begin{pmatrix} \mathrm{ch}\,\theta & \mathrm{sh}\,\theta \\ \mathrm{sh}\,\theta & \mathrm{ch}\,\theta \end{pmatrix},\ \theta \in \mathbb{R}\}$$

munis de la multiplication matricielle sont des groupes non-isomorphes.

4 Ordre et groupes cycliques

Exercice 14. * Soit $(G, \times)$ un groupe.

1. Montrer que si a et b sont conjugués dans G, c'est-à-dire $\exists c \in G$ tel que $a = cbc^{-1}$, alors $\omega(a) = \omega(b)$, où $\omega(x)$ est l'ordre de x.
2. Montrer que si a, $b \in G$, alors $\omega(ab) = \omega(ba)$.

Exercice 15. ♡♡♡** Soit $(G, *)$ un groupe cyclique d'ordre $n \geq 2$ et $a \in G$ un générateur. Montrer que si H est un sous-groupe d'ordre d, alors $d|n$ et $H =< a^{\frac{n}{d}} >$.

Exercice 16. * Soit G un groupe et $x \in G$ un élément d'ordre n. Quel est l'ordre de x^2.

Exercice 17. ♡*

1. Si m, $n \geq 1$ et $m \wedge n = 1$. Déterminer $\mathrm{Hom}\,(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z})$, l'ensemble des morphismes de groupes de $(\mathbb{Z}/n\mathbb{Z}, +)$ vers $(\mathbb{Z}/m\mathbb{Z}, +)$.
2. Déterminer $\mathrm{Hom}\,(\mathbb{Z}/6\mathbb{Z}, \mathbb{Z}/8\mathbb{Z})$.

Exercice 18. ** Soit G un groupe abélien, x et y deux éléments de G d'ordre respectif p et q.

1. On suppose que p et q sont premiers entre eux. Démontrer que xy est d'ordre pq.
2. Dans $\mathrm{GL}_2(\mathbb{R})$, on pose $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ et $B = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$. Montrer que A et B sont d'ordre finis mais AB ne l'est pas. Est-ce contradictoire avec le 1/ ?
3. Si p et q ne sont pas premiers entre eux, montrez que xy n'est pas nécessairemenr d'ordre pq ni même $\mathrm{PPCM}(p, q)$.
4. Soit d un diviseur de p. Démontrer qu'il existe un élément d'ordre d dans G.
5. En déduire que G admet des éléments d'ordre $\mathrm{PPCM}(p, q)$.
6. Si G est de cardinal fini. Démontrer qu'il existe un élément dont l'ordre est le ppcm des ordres des éléments de G.

Exercice 19. *** Soit $(G, *)$ un groupe abélien fini et p un nombre premier tel que $\forall g \in G$, $\omega(g) = p$. Montrer qu'il existe $n \in \mathbb{N}$ tel que G est isomorphe à $(\mathbb{Z}/p\mathbb{Z})^n$.

5 Permutations

Exercice 20. ♡♡** Soit $(S_n, \circ)$ le groupe des permutations de $[\![1, n]\!]$. On pose $\tau = (1, 2)$ et $\sigma = (1\ 2\ \cdots\ n)$.

1. Pour $k \in [\![0, n-2]\!]$, calculer $\sigma^k \tau \sigma^{-k}$.
2. Montrer que toute transposition (i, j) peut s'écrire comme un produit de transposition de la forme $(m, m+1)$.
3. En déduire le sous-groupe de S_n engendré par σ et τ.

Exercice 21. ♡** Soit ϕ un automorphisme de S_n qui transforme une transposition en une transposition. On note t_i la transposition $(1\ i)$.

1. Montrez que deux transpositions distinctes commutent ssi elles ont des supports disjoints.
2. Montrer qu'il existe trois éléments $a_1,\ a_2$ et a_3 tels que $\phi(t_2) = (a_1\ a_2)$ et $\phi(t_3) = (a_1\ a_3)$.
3. Montrer que pour tout $i > 3$, il existe a_i tel que $\phi(t_i) = (a_1\ a_i)$.
4. Montrer que l'application s qui à i associe a_i est bijective.
5. On appelle automorphisme intérieur h_s associé à s l'application définie par $h_s : S_n \to S_n\ \sigma \mapsto s\sigma s^{-1}$.
   (a) Montrer que pour tout $i,\ j \geq 2$, $\phi((i\ j)) = h_s((i\ j))$.
   (b) En déduire que $\phi = h_s$.

Exercice 22. *** Soit n un entier naturel non nul, $(e_1, \ldots, e_n)$ la base canonique de $E = \mathbb{R}^n$.
Soit $\mathcal{S}_n$ l'ensemble des permutations de $\{1, 2, \ldots, n\}$. Soit $t_i = (1, i)$.
Pour $s \in \mathcal{S}_n$, on définit $u_s(e_i) = e_{s(i)}$.

1. Montrer que $(t_2, t_3, \ldots, t_n)$ engendre $\mathcal{S}_n$.
2. Interpréter géométriquement u_s lorsque s est une transposition.
3. Soit $s = (1\ 2\ \ldots\ n-1\ n)$. On suppose que s est la composée de p transpositions. Montrer que $p \geq n - 1$.
4. Quel est le cardinal minimal d'une famille de transpositions génératrice de $\mathcal{S}_n$?

Groupes

(Solutions)

Solution 1. Pour $g \in G$, on considère $H_g = \{g, g^{-1}\}$. Les ensembles H_g sont soit soit égaux soit disjoints. H_e est de cardinal 1. On en déuit qu'au moins un H_g est aussi de cardinal 1, pour $g \neq e$.

Solution 2. Soit $x \in G$, d'inverse à droite x'. Soit y inverse à droite de x' :

$$x'y = e \text{ et } xx'y = ey \Rightarrow x.e = e.y = x$$

et donc $x'ey = e$ soit $x'x = e$. Il reste à vérifier que e est bien un élément neutre à gauche : $ex = xx'x = xe = x$. Ou encore : $\varphi_x : g \mapsto x'gx$ est un endomorphisme de G : $\varphi(gh) = x'gx'xhx = \varphi(g)\varphi(h)$ et donc $\varphi_x(e) = x'ex = e$. On en duit $xx' = x'x = e$ pour tout x, $ex = xx'x = xe = x$. L'élément neutre à droite est neutre à gauche aussi.

Solution 3. On éccrit $(x*y)^n = (x*y)*(x*y)^{n-1} = x*y*x^{n-1}*y^{n-1} = x^ny^n$, d'où en simplifiant par y^{n-1} à droite et par x à gauche, $y*x^{n-1} = x^{n-1}*y$. De même, $x*y^n = y^n*x$.
On en déduit

$$y*x^n = (y*x^{n-1})*x = x^{n-1}*y*x = x^n*y \Rightarrow x*y = y*x.$$

Ou encore : $x^{n+1}y^{n+1} = (x*y)^{n+1} = x*(y*x*\cdots*y*x)*y = x*y^nx^n*y$ implique que $(x*y)^n = x^ny^n = y^nx^n$ et de même $(x*y)^{n-1} = x^{n-1}y^{n-1} = y^{n-1}x^{n-1}$.
Pour conclure

$$(xy)^n = \begin{cases} (xy)^{n-1}xy \\ (yx)^n = (yx)^{n-1}yx = (xy)^{n-1}yx \end{cases}$$

On a montré que si $x^ny^n = y^nx^n$ et $x^{n-1}y^{n-1} = y^{n-1}x^{n-1}$, alors G est abélien. Mais pour cela on avait besoin de de trois rangs consécutifs sur n. Mais dans l'exercice 12, on montre que si la propriété est vraie pour $n = 2$, alors G est abélien. Pour un contre exemple, il faudrait prendre $n - 1 \geq 3$.

Solution 4. Il est clair que si H est un sous-groupe, alors il est stable par la loi $*$.
Réciproquement, si H est stable par la loi $*$, alors pour tout $h \in H$, $\gamma_h : g \mapsto h*g$ est une bijection de G dans G de réciproque $\gamma_{h^{-1}}$. γ_h induit une bijection de H dans $\gamma(H)$. Par hypothèse, $\gamma_h(H) \subset H$.
De plus, H est supposé fini, donc par cardinalté, $H = \varphi(H)$. En particulier, $\gamma_h^{-1}(e_g) = h^{-1} \in H$, ce qui termine la preuve.

Solution 5. Soit K le sous-groupe engendré par le complémentaire de H. Alors $H \cup K = G$ est un groupe. Il vient d'après un exercice précédent que $H \subset K$ et $K = G$.

Solution 6. On commence par montrer $H \subset \mathbb{R}_+^*$: comme $x^2 - 3y^2 = 1 > 0$ et $x \in \mathbb{N}$ on a $x > \sqrt{3}|y|$ et en particulier $x + y\sqrt{3} > 0$.
H est stable par produit car

$$(x + y\sqrt{3})(x' + y'\sqrt{3}) = (xx' + 3yy') + \sqrt{3}(yx' + xy')$$

avec

$$\begin{aligned} (xx' + 3yy')^2 - 3(yx' + xy')^2 &= x^2x'^2 + 9y^2y'2 - 3x^2y'2 - 3x'2y^2 \\ &= x^2(x'2 - 3y'2) + 3y^2(3y'2 - x'^2) \\ &= x^2 - 3y^2 = 1 \end{aligned}$$

Solution 7. Supposons d'abord que $AB = BA$. Alors AB est un sous-groupe de G car :

1. $e \in AB$, car $e = ee$ avec $e \in A$ et $e \in B$ (ce sont des sous-groupes) ;
2. AB est stable par passage au produit. En effet, si $x = ab \in AB$ et $y = a'b' \in AB$, alors $xy = aba'b'$. Or, ba' est un élément de BA, c'est donc aussi un élément de AB et donc $ba' = a''b''$ avec $a'' \in A$ et $b'' \in B$. On en déduit que
$$xy = aa''b''b \in AB$$
puisque $aa'' \in A$ et $bb'' \in B$.
3. AB est stable par passage à l'inverse. En effet, si $x = ab \in AB$, alors $x^{-1} = b^{-1}a^{-1}$ est élément de BA et $BA = AB$.

Réciproquement, supposons que AB est un sous-groupe de G et prouvons que $AB = BA$. Soit d'abord $x = ab \in AB$. Alors $x^{-1} = b^{-1}a^{-1} \in AB$ et donc $b^{-1}a^{-1} = a'b'$ avec $a' \in A$ et $b' \in B$. On passe à l'inverse :
$$ab = b'^{-1}a'^{-1} \in BA.$$
De même, si $y = ba \in BA$, alors $y^{-1} = a^{-1}b^{-1} \in AB$, et donc $y = (y^{-1})^{-1} \in AB$.

Solution 8. Utiliser $\det M^{-1} = \dfrac{1}{\det M}$ ainsi que la comatrice pour calculer l'inverse de M.

Solution 9.

1. C'est du cours
2. Soit $x \in \mathbb{R} \setminus \mathbb{Q}$. Pour $N \in \mathbb{N}^*$, on définit l'application $\varphi : [\![0, N]\!] \to [0, 1[,\ k \mapsto kx - \lfloor kx \rfloor$.
Montrons que φ est injective :
$$\varphi(k) = \varphi(k') \Leftrightarrow kx - \lfloor kx \rfloor = k'x - \lfloor k'x \rfloor \Leftrightarrow x = \frac{\lfloor k'x \rfloor - \lfloor kx \rfloor}{k - k'} \quad \text{si } k - k' \neq 0$$
Par hypothèse, $x \notin \mathbb{Q}$ donc $k = k'$ et φ est injective.
On a donc $|\operatorname{Im}\varphi| = N + 1$, et on peut poser $x_0 = 0 < x_1 < \cdots < x_N < 1$. $\displaystyle\sum_{i=1}^{N}(x_i - x_{i-1}) < 1$. On en déduit qu'il existe i_0 tel que $x_{i_0} - x_{i_0-1} < \dfrac{1}{N}$.
D'où l'existence de $0 \leq k \neq k' \leq N$ tels que $|\varphi(k) - \varphi(k')| < \dfrac{1}{N}$.
On pose $p = \lfloor k'x \rfloor - \lfloor kx \rfloor \in \mathbb{Z}$ et $q = k' - k \in \{0, \cdots, N\}$.
$$|qx - p| = |(k'x - \lfloor k'x \rfloor) - (kx - \lfloor kx \rfloor)| < \frac{1}{N}$$
et en divisant par q et en remarquant que $0 < q \leq N$, on obtient un couple avec les bonnes propriétés.
Comme $\dfrac{1}{N}$ tend vers 0 quand N tend vers $+\infty$, on en déduit une infinité de couples, vu que $x - \frac{p}{q} \neq 0$.
3. Appliquons le résultat à π : il existe une infinité de couples $(p_n, q_n)_{n\mathbb{N}} \in (\mathbb{Z} \times \mathbb{N}^*)^{\mathbb{N}}$ tels que $q_n \to +\infty$
$$|q_n\pi - p_n| \leq \frac{1}{q_n}.$$
On a alors
$$|u_n| = \left|\frac{1}{p_n \sin p_n}\right| = \left|\frac{1}{p_n \sin(q_n\pi - p_n)}\right| \geq \frac{q_n}{p_n}$$
Comme par construction $\dfrac{q_n}{p_n}$ tend vers $\dfrac{1}{\pi}$, la suite u_{p_n} ne tend pas vers 0.
D'autre part, $\mathbb{Z} + \pi\mathbb{Z}$ est dense dans $\mathbb{R}$ car π est irrationnel. On en déduit qu'il existe une suite

$(\widetilde{p}_n, \widetilde{q}_n)$ telle que $\widetilde{p}_n + \widetilde{q}_n\pi \in [\frac{\pi}{3}, \frac{\pi}{2}]$ avec $\widetilde{p}_n \to \infty$.
Et alors

$$|U_{\widetilde{p}_n}| = \left|\frac{1}{\widetilde{p}_n \sin \widetilde{p}_n}\right| \leq \frac{2}{p_n}$$

ce qui montre qu'une suite extraite converge vers 0. On en déduit que la suite u_n diverge.

Solution 10. Il est clair que si G est abélien $\varphi(x * y) = (x * y)^2 = x^2 * y^2 = \varphi(x) * \varphi(y)$.
Si φ est un morphisme. $x^2 * y^2 = x * y * x * y$ et on simplifie à gauche par x, à droite par y et on obtient $x * y = y * x$.

Solution 11. On commence par remarquer que si φ était constante, elle vaudrait $\varphi(e) = 1$. Donc par hypoyhèse, il existe $a \in G$, tel que $\varphi(a) \neq 1$.
L'application $G \to G$, $g \mapsto ag$ est bijective. Donc la somme S recherchée vaut aussi $\varphi(a)S$, d'où $S = 0$.

Solution 12.

1. Soit $\varphi : G \to G'$ un tel morphisme et $H = \{x \in G \mid \varphi(x) = e_{G'}\}$ son noyau. On sait déjà que H est un sous-groupe de $(G, .)$. Soient $x \in H$ et $a \in G$. On a

   $$\varphi\left(axa^{-1}\right) = \varphi(a)\varphi(x)\varphi(a)^{-1} = \varphi(a)e_{G'}\varphi(a)^{-1} = e_{G'}$$

   donc $axa^{-1} \in H$
2. $HK \subset G$ et $e = e.e \in HK$. Soient $a, b \in HK$. On peut écrire

   $$a = xy \text{ et } b = x'y' \text{ avec } x, x' \in H \text{ et } y, y' \in K$$

   On a alors

   $$ab = xyx'y'$$

   Puisque $z = yx'y^{-1} \in H$, on a encore

   $$ab = (xz)(yy') \in HK$$

   Aussi

   $$a^{-1} = y^{-1}x^{-1} = zy^{-1} \in HK$$

   avec $z = y^{-1}x^{-1}y \in H$ Ainsi HK est bien un sous-groupe de $(G, .)$.
3. (a) La relation est réflexive ($e \in H$), symétrique (H stable par inverse) et transitive (assiciativité). De plus, si $ba^{-1} \in H$, alors $a^{-1}b = h \in H$ et $b = ah \in aH$.
   (b) Remarquons que pour tout $a \in G$, $aHa^{-1} = H$: par définition d'un sous-groupe distingué, $aHa^{-1} \subset H$; Et si $h \in H$, alors $a^{-1}ha \in H$ et $a(a^{-1}ha)a^{-1} = h$, donc $H \subset aHa^{-1}$.
   Ainsi, $aH * bH = a * bHb^{-1}bH = (ab)H^2 = (ab)H$, donc la loi est bien définie car elle ne dépend pas des représentants a et b. La loi est bien définie et l'inverse de aH et $a^{-1}H$ l'élément neutre étant H. L'associativité résulte de celle de la loi . sur G.
   On a en fait montré que $\varphi : G \to G/H$, $a \mapsto aH$ est un morphisme de groupes et le noyau vaut exactement H.

Solution 13. On montre que ce sont des sous-groupes de $GL_n(\mathbb{R})$. On reconnait G, le groupe des matrices de rotations. Et l'autre se traite de manière identique.
On vérifie que l'équation $X^2 = I_2$ a deux solutions dans $\mathbb{G}$ et une seule dans G', donc ils ne sont pas isomorphes.

Solution 14.

1. On sait que φ_c est un auromorphisme de G. Donc $\varphi_c(< a >) =< b >$ et $\omega(a) = | < a > | = | < b > | = \omega(b)$.
2. On a $\varphi_b(ab) = ba$. D'après la question précédente, $\omega(ab) = \omega(ba)$.

Solution 15. Si H est d'ordre 1, alors $H = \{e\}$. On suppose dans la suite $d \geq 2$.
Le groupe G est ismorphe à $\mathbb{Z}/n\mathbb{Z}$ par $a \mapsto \bar{1}$.
Il suffit donc de montrer le résultat $G = \mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \cdots, \overline{n-1}\}$. Soit H un sous-groupe d'ordre $d \geq 2$ et $\bar{k} \in H$, avec k minimal non nul.
Alors pour tout $\bar{k'} \in H$ avec $k' \in [\![1, n-1]\!]$, la division euclidienne de k' par k : $k' = qk+r$ montre que $r = 0$ par minimalité de k. On a montré que que $H \subset <\bar{k}> \subset H$, donc on a égalité et $H = \{\bar{0}, \bar{k}, \cdots, (d-1)\bar{k}\}$.
De plus, $(d-1)k < n$, d'où $dk < n + k < 2n$. Comme $dk \equiv 0[n]$, on en déduit $dk = n$, d'où le résultat.
Une autre méthode : On a un morphisme surjectife $\mathbb{Z} \to G$, $k \mapsto a^k$. L'image réciproque de H est un sous-groupe de $\mathbb{Z}$ donc est de la forme $m\mathbb{Z}$ et contient le noyau, donc $n\mathbb{Z} \subset m\mathbb{Z} : m|n$. De plus, on a un morphisme $m\mathbb{Z} \to H$. C'est-à-dire $H = < a^m >$, il est donc cyclique. Comme $m|n$ et H d'ordre d, on a $m = \dfrac{n}{d}$.

Solution 16. On a $< x >= \{1, x, \cdots, x^{n-1}\}$.
Si n est pair, l'ordre est $\dfrac{n}{2}$ car $< x >= \{1, x^2, \cdots, x^{n/2}\}$.
Si n est impair, comme $(x^2)^n = e$, l'ordre d de x^2 divise n. De plus, $x^{2d} = e$, donc n divise $2d$, mais alors n divise d car n et 2 sont premier entre eux. Donc $d = n$.

Solution 17. Pour tous entiers $p \geq 0$ et $k \geq 1$, $\overline{p}_k$ la classe de p modulo k pour tout entier.

1. Soit $\varphi \in \mathrm{Hom}\,(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z})$. L'image $\varphi(\bar{1}_k)$ engendre un groupe d'ordre qui divise n, car l'ordre du noyau de φ divise n. Comme $m \wedge n = 1$, $\omega\left(\varphi(\bar{1}_k)\right) = 1$ et $\varphi(\bar{1}_k) = \bar{0}_m$. Donc il n'y a que l'endomorphisme nul.
2. Soit $\varphi \in \mathrm{Hom}\,(\mathbb{Z}/6\mathbb{Z}, \mathbb{Z}/8\mathbb{Z})$. L'image $\varphi(\bar{1}_6)$ engendre un groupe d'ordre qui divise 6 : donc soit 1 (morphisme nul), soit 2 (alors l'mage de $\bar{1}_6$ est $\bar{4}_8$), soit d'ordre 3 ou 6, mais on sait que l'ordre de l'image de $\bar{1}$ divise 8, ce qui est imopssible.
   Vérifions que $\bar{1}_6 \mapsto \bar{4}_8$ donne bien un morphisme. On a $\overline{2k}_6 \to \bar{0}_8$ et $\overline{2k+1}_6 \to \bar{4}_8$ et c'est bien un morphisme.

Solution 18.

1. On a $(xy)^{pq} = (x^p)^q (y^q)^p = 1$. Donc l'ordre d de xy divise pq : on peut l'écrire $d = p'q'$ avec $p = p'p''$ et $q = q'q''$:
$$x^{p'q'}y^{p'q'} = 1 \Rightarrow x^{p'q'q''}y^{p'q'q''} = 1 \Rightarrow x^{p'q} = 1$$
   et comme l'ordre p de x divise $p'q$ et p et q premiers entre eux, on en déduit $p|p'$ et $p = p'$.
   Autre méthode : l'application $< x > \times < y > \mapsto < x, y >$, $(x^k, y^{k'}) \mapsto x^k y^{k'}$ est un mrophisme surjectif car G est abélien. L'ordre du noyau vaut $| < x > \cap < y > | = |\{e\}| = 1$. Donc l'application est bijective et $| < x, y > | = pq$. De plus $< xy > \subset < x, y >$. Enfin, il existe k et l tels que $pk+ql = 1$, d'où $(xy)^{pk} = y^{pk} = y^{1-ql} = y \in < xy >$. De même $x \in < xy >$. On en déduit $< x, y > = < xy >$ et l'ordre vaut pq.
2. On calcule $A^2 = -I_2$, $A^3 = -A$ et $A^4 = I_2$, donc A est d'ordre 4. De même, on calcule $B^2 = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}$ et $B^3 = I_2$. Mais $AB = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Par récurrence, on obtient $(AB)^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$. Donc AB est d'ordre infini. Cela montre que $\mathrm{GL}_2(\mathbb{R})$ est de cardinal infini !
3. si x est d'ordre 4, alors $x^2x^2 = 1$!
4. Si $p = dp'$, alors $(x^{p'})^d = 1$, donc $\omega(x^{p'})$ est diviseur de d, car $(x^{p'})^d = 1$. Par hypothèse x est d'ordre p, donc pour $0 < k < d$, $(x^{p'})^k \neq 1$. Finalement $\omega(x^{p'})$ est d'ordre d.
5. Soit $PPCM(p, q) = \prod p^{\alpha_i}$ la décomposition en nombre premiers. Comme p^{α_i} divise soit p soit q, il existe des éléments x_i d'ordre p^{α_i}premiers entre eux. Par récurrence, $\prod x_i$ est d'ordre voulu.
6. On note $G = \{g_1, g_2, \cdots, g_n\}$ et $\omega(g_i) = \alpha_i$ pour tout $i \in [\![1, n]\!]$ tel que $\alpha_1 \leq \alpha_2 \leq \cdots \leq \alpha_n$ soit une suite croissante d'entiers. S'il existe α_i tel que $\alpha_i \not| \alpha_n$, alors il existe un élément x d'ordre $\mathrm{PPCM}\,(\alpha_i, \alpha_n) > \alpha_n$, ce qui contredit la maximalité de α_n. Finalement, g_n est d'ordre le PPCM des ordres des éléments de G.

Solution 19. On montre que G a une structure de $\mathbb{Z}/p\mathbb{Z}$-espace vectoriel :

— $(G, *)$ est un groupe commutatif.

— $\forall \bar{m} \in \mathbb{Z}/p\mathbb{Z}$ et $g \in G$, $\bar{m}.g = g^m$, dépend que de $\bar{m}$ et pas du choix de m : si $m' = m + kp$, alors $g^{m'} = g^{kp} g^m = g^m$ car g est d'ordre p.

— $\forall g \in G$, $\bar{1}.g = g^1 = g$.

— $\forall k, k' \in \mathbb{Z}$, $\forall g \in G$, $(\bar{k} \times \bar{k}').g = g^{kk'} = \bar{k}.(\bar{k}'.g)$.

— $\forall k, k' \in \mathbb{Z}$, $\forall g \in G$, $(\bar{k} + \bar{k}').g = g^{k+k'} = (\bar{k}.g) * (\bar{k}'.g)$.

— $\forall k \in \mathbb{Z}$, $\forall g, g' \in G$, $\bar{k}.(g * g') \underset{\text{abélien}}{=} g^k * g'^{k'} = (\bar{k}.g) * (\bar{k}'.g')$.

Donc il existe une base $(e_1, \cdots, e_n)$ de G. L'application $(\mathbb{Z}/p\mathbb{Z})^n \to G$, $(x_1, \cdots, x_n) \mapsto (x_1.e_1) * \cdots * (x_n.e_n)$ est un isomoprphisme d'espace vectoriel, donc en particulier de groupes.

Solution 20.

1. Par récurrence $\sigma^k \tau \sigma^{-1} = (k+1\ k+2)$ pour tout $k \in [\![0, n-2]\!]$.
2. On procède par récurrence sur j.
   Si $j = i+1$, $(i\ j) = (i\ i+1)$.
   Si la proposition est vraie pour $j > i$: $(i\ j)$ s'écrit comme un produit de transpositions de la forme $(m, m+1)$. Alors $(i\ j+1) = (j\ j+1)(i\ j)(j\ j+1)$.
   La propriété est donc vraie pour tout $j > i$.
3. Le cours nous dit que S_n est engendré par les transpositions et les questions 1 et 2 montrent que le groupe engendré par τ et σ contient toutes les permutations. On en déduit que le groupe engendré par τ et σ vaut exactement S_n.

Solution 21.

1. On sait que deux permutations qui ont des supports disjoints commutent. La réciproque n'est vraie que pour des transpositions. On procède par contraposée. Si τ_1 et τ_2 sont distinctes et leurs supports ne sont pas disjoints. Elles ont au moins un élément commun dans leur support, mais pas plus, car sinon elle sont égales. Donc il existe a_1, a_2 distincts tels que $\tau_1 = (a_1\ a_2)$ et $\tau_2 = (a_1\ a_3)$. Alors $\tau_2 \circ \tau_1(a_1) = \tau_2(a_2) = a_2$ et $\tau_1 \circ \tau_2(a_1) = \tau_2(a_3) = a_3$ et τ_1 et τ_2 ne commutent pas.
2. Si $\phi(t_2)$ et $\phi(t_3)$ commutaient, alors on aurait $t_2 t_3 = \phi^{-1}(\phi(t_2)\phi(t_3)) = \phi^{-1}(\phi(t_3))\phi(t_2)) = t_3 t_2$ et donc t_2 et t_3 commuteraient elles aussi. $\phi(t_2)$ et $\phi(t_3)$ n'ont donc pas un support disjoint ce qui donne immédiatement le résultat.
3. Le support de $\phi(t_i)$ n'est pas disjoint de $\phi(t_2)$ pas plus que de celui de $\phi(t_3)$. Il y a donc deux possibilités.
   — ou bien $\phi(t_i) = (a_1\ a_i)$, ce qui est le résultat voulu.
   — ou bien $\phi(t_i) = (a_2\ a_3)$. Mais $t_2 t_3 t_2 = (t_2(1)\ t_2(3)) = (2\ 3)$, donc
   $$\phi((2,3)) = \phi(t_2 t_2 t_2) = \phi(t_2)\phi(t_3)\phi(t_2) = (a_1\ a_2)(a_1\ a_3)(a_1\ a_3) = (a_2\ a_3).$$
   Comme ϕ est bijective, elle est injective et $\phi(t_i) \neq \phi((2\ 3)) = (a_2\ a_3)$.
   On en déduit $\phi(t_i) = (a_1\ a_i)$.
4. Si les a_i n'étaient pas tous distincts, alors ϕ ne saurait être bijective.
5. Soit $(i\ j)$ une permutation, alors $t_i t_j t_i = (t_i(1)\ t_i(j)) = (i\ j)$ et donc $\phi((i\ j)) = (a_i\ a_j)$. De même, On a $s(i\ j)s^{-1} = (s(i)\ s(j)) = (a_i\ a_j)$. Comme les transpositions engendrent S_n, on obtient que ϕ coïncide avec h_s.

Solution 22.

1. Soit i_1 et i_2 deux entiers distints > 1. On remarque que $(1, i_1)(1, i_2)(1, i_1) = (i_1, i_2)$. On sait que $\mathcal{S}_n$ est engendré par les transpostions, d'où le résultat.
2. u_s est la réflexion d'hyperplan engendré par $(e_i + e_j$ et les e_k, $k \neq i, j$, où $s = (i, j)$.

3. On utilise la remarque suivante : si est un E $\mathbb{K}$-espace vectoriel de dimension n et H un hyperlan, alors $\dim F + H \leq \dim E = n$. Donc,

$$\dim H \cap F = \dim H + \dim F - \dim(H + K) \leq n - 1 + \dim F - n = \dim F - 1$$

On en déduit que si τ_1, ... τ_{n-2} sont des permutations, alors

$$\bigcap_{i=1}^{n-1} E_1(P_{\tau_i}) \subset E_1\big(P_{\tau_1} \cdots P_{\tau_{n-2}}\big) = E_1\big(P_{\tau_1 \cdots \tau_{n-2}}\big).$$

D'après la remarque plus haut $\dim \bigcap_{i=1}^{n-1} E_1(P_{\tau_i}) \geq 2$. Or $P_{(1\ldots n)}$ admet un sous-espace propre E_1 de dimension 1. Donc $\mathcal{S}_n$ ne peut pas être engendré par $n-2$ transpositions. Il en faut au moins $n-1$.

4. On a montré en 1/ que ce cardinal vaut au plus $n-1$ et en 3/ qu'il en faut au moins $n-1$.