Structures Algébriques

Énoncés 2
Opérations 2
Groupes 4
Anneaux 17
Corps 25
Indications 28
Solutions 40

Énoncés

Dans tout le TD on utilisera l'abus de notation (si cela est sans ambiguïté) consistant à dire «le groupe G» pour «le groupe $(G,\cdot)$», et de même pour les anneaux et corps.

Opérations

Exercice 1 (◔★♣ Puissances d'un inversible dans un monoïde)
Soit $(M,\cdot)$ un monoïde.

On note $M^\times$ le groupe des éléments inversibles de M.

Pour $n\in\mathbb{Z}$ et $x\in M^\times$ on note

$$x^n=\begin{cases}x^n & \text{si } n\geq 0\\ (x^{-1})^{-n} & \text{si } n<0.\end{cases}$$

Expliquer comment démontrer les propositions suivantes:
- ▷ $\forall x\in M^\times,\forall n\in\mathbb{Z},\ x^n\in M^\times$ et $(x^n)^{-1}=x^{-n}$.
- ▷ $\forall (n,m)\in\mathbb{Z}^2,\ x^nx^m=x^{n+m}$ et $(x^n)^m=x^{nm}$.
- ▷ $\forall (x,y)\in (M^\times)^2$ **si** $xy=yx$ **alors** $\forall (n,m)\in\mathbb{Z}^2, x^ny^m=y^mx^n$ et $(xy)^n=x^ny^n$.

Indication p. 28

Exercice 2 (◔★ Juste la droite ou juste la gauche suffit)
Soit G un ensemble muni d'une opération $\cdot$.

1. On suppose
- ▷ L'opération $\cdot$ est associative.
- ▷ Il existe $e\in G$ tel que $\forall x\in G, xe=x$.
- ▷ Étant donné un tel e, $\forall x\in G,\exists y\in G, xy=e$.

Montrer que $(G,\cdot)$ est un groupe.

2. On munit $M=\mathbb{C}^*$ de l'opération ♦ définie par

$$\forall (z,\xi)\in M^2, z\blacklozenge\xi=|z|\cdot\xi.$$

Montrer que
- ▷ L'opération ♦ est associative.
- ▷ Il existe $e\in M$ tel que $\forall z\in M, e\blacklozenge z=z$.
- ▷ Étant donné un tel e, $\forall z\in M,\exists\xi\in M, z\blacklozenge\xi=e$.

Puis montrer que $(M,\blacklozenge)$ n'est **pas** un groupe.

3. Commenter.

Indication p. 28

Exercice 3 (◔☆ Maximum et minimum comme opérations)
Soit $(E, \leq)$ un ensemble ordonné tel que $\leq$ est un ordre total.

1. Montrer l'opération max définie par

$$\begin{aligned} \max : E \times E &\to E \\ (x, y) &\mapsto \max(x, y) \end{aligned}$$

est associative et commutative.
2. Déterminer une CNS sur $(E, \leq)$ pour que $(E, \max)$ soit un monoïde.

Indication p. 28

Exercice 4 (◔★ Encore la relation de similitude)
Soit $(M, \cdot)$ un monoïde.

On munit M d'une relation $\sim$ définie par

$$\forall (x, y) \in M^2, x \sim y \Leftrightarrow \exists u \in M^\times, x = uyu^{-1}.$$

Commenter.

Indication p. 28

Exercice 5 (◑★ Opération opposée)
Soit $(M, \perp)$ un monoïde.

On défini une opération $\top$ sur M par

$$\forall (x, y) \in M, x \top y = y \perp x.$$

1. Montrer que $(M, \top)$ est un monoïde.
2. Donner un exemple où $(M, \top)$ et $(M, \perp)$ ne sont pas isomorphes.
3. On suppose de plus que $(M, \perp)$ est un groupe.

   Montrer que $(M, \top)$ est un groupe et expliciter un isomorphisme de groupe entre $(M, \perp)$ et $(M, \top)$.

Indication p. 29

Groupes

Exercice 6 (◔★♣ Groupes isomorphes)
Soient $(G_1, *_1)$ et $(G_2, *_2)$ deux groupes.

On dit qu'ils sont *isomorphes* ssi il existe un isomorphisme de G_1 vers G_2. On note alors $G_1 \simeq G_2$.

1. Donner un exemple de deux groupes isomorphes, et un exemple de deux groupes non isomorphes.
2. Montrer que
   - ▷ Étant donné un groupe G, $G \simeq G$
   - ▷ Étant donnés des groupes G_1, G_2 et G_3 **si** $G_1 \simeq G_2$ et $G_2 \simeq G_3$ **alors** $G_1 \simeq G_3$.
   - ▷ Étant donnés des groupes G_1 et G_2 **si** $G_1 \simeq G_2$ **alors** $G_2 \simeq G_1$.
3. Commenter.

Indication p. 29

Exercice 7 (◔★ Groupes non isomorphes)

1. Montrer que les groupes $(\mathbb{R}, +)$ et $(\mathbb{R}^*, \times)$ ne sont pas isomorphes.
2. Montrer que les groupes $(\mathbb{U}_4, \cdot)$ et $(\mathbb{U}_2 \times \mathbb{U}_2, \cdot)$ ne sont pas isomorphes.

Indication p. 29

Exercice 8 (◔☆ Sous-groupes ? I)
Pour chacun des ensembles suivants, déterminer si il s'agit de sous-groupes de $(\mathbb{C}^*, \times)$.

1. $\{a + i0, a \in \mathbb{R}_+^*\}$
2. $\{z \in \mathbb{C}^* \mid |z| \geq 1\}$
3. $\{a + bi, (a, b) \in \mathbb{Q}^2 \setminus \{(0, 0)\}\}$
4. $\{z \in \mathbb{C}^* \mid \mathrm{Re}(z) \times \mathrm{Im}(z) > 0\}$
5. $\{\mathrm{ch}(t) + \mathrm{sh}(t)i, t \in \mathbb{R}\}$
6. $\{z \in \mathbb{C}^* \mid \exists n \in \mathbb{N}^*, z^n = 1\}$

Indication p. 29

Exercice 9 (◔★♠ Un classique)
Soit $(G, \cdot)$ un groupe de neutre e_G tel que pour tout $x \in G$, $x^2 = e_G$.

Montrer que G est abélien.

Indication p. 29

Exercice 10 (◕☆ Raffinement d'un exercice précédent)
Soit $(G, \cdot)$ un groupe **fini** de neutre e_G tel que pour tout $x \in G$, $x^2 = e_G$.

Montrer qu'il existe $n \in \mathbb{N}$ tel que G est isomorphe à $(\mathbb{U}_2)^n$.

Indication p. 30

Exercice 11 (◔★ Union de sous-groupes ?)
Soit $(G, \cdot)$ un groupe et H_1, H_2 deux sous-groupes de G.

1. Redémontrer brièvement que $H_1 \cap H_2$ est un sous-groupe de G.
2. Donner un exemple où $H_1 \cup H_2$ n'est **pas** un sous-groupe de G.
3. Montrer que **si** $H_1 \cup H_2$ est un sous-groupe de G **alors** $H_1 \subset H_2$ ou $H_2 \subset H_1$.

Indication p. 30

Exercice 12 (◔★ Loi de composition des vitesses relativistes)
On définit une opération $\oplus$ sur $]-1,1[$ par

$$\forall (x,y) \in]-1,1[, x \oplus y = \frac{x+y}{1+xy}.$$

Montrer que $(]-1,1[, \oplus)$ est un groupe abélien.

Indication p. 30

Exercice 13 (◔★ Transport de loi)
Soit $(G, \cdot)$ un groupe.

Soit E un ensemble et $\varphi : E \to G$ une application **bijective**.

On muni E de l'opération $*$ définie par

$$\forall (x,y) \in E^2, x * y = \varphi^{-1}(\varphi(x) \cdot \varphi(y)).$$

Montrer que $(E, *)$ est un groupe.

Indication p. 30

Exercice 14 (◔☆ Petite translation)
Soit $(G, *)$ un groupe et $a \in G$. On définit une opération $\star_a$ sur G par

$$\forall (x, y) \in G^2, x \star_a y = x * a * y.$$

Montrer que $(G, \star_a)$ est un groupe, et qu'il est isomorphe à $(G, *)$.

Indication p. 30

Exercice 15 (◔★♣ Sous-groupes additifs de $\mathbb{Z}$)
Soit H un sous-groupe de $(\mathbb{Z}, +)$.

Montrer qu'il existe $m \in \mathbb{N}$ tel que $H = m\mathbb{Z}$.

(C'est à dire tel que $H = \{mk, k \in \mathbb{Z}\}$).

Indication p. 30

Exercice 16 (◑★♣ Groupe des automorphismes)
Soit $(G, \cdot)$ un groupe.

On note $\mathrm{Aut}(G)$ l'ensemble des automorphismes de G.

Montrer que $(\mathrm{Aut}(G), \circ)$ est un groupe.

Indication p. 31

Exercice 17 (◔★♠ Conjugaisons et automorphismes intérieurs)
Soit $(G, \cdot)$ un groupe.

Pour $u \in G$ on note

$$\begin{aligned} \varphi_u : G &\to G \\ x &\mapsto uxu^{-1}. \end{aligned}$$

1. Montrer que pour tout $u \in G$, $\varphi_u \in \mathrm{Aut}(G)$.
2. Montrer que

$$\begin{aligned} \Phi : G &\to \mathrm{Aut}(G) \\ u &\mapsto \varphi_u \end{aligned}$$

est un morphisme de groupe.
3. Donner un exemple où Φ n'est pas injectif, et un exemple où Φ n'est pas surjectif.

Indication p. 31

Exercice 18 (◔★ Les groupes des permutations sont compliqués !)
Soit $(G, \cdot)$ un groupe.

Étant donné un ensemble E, on rappelle que l'on note $\mathcal{S}_G = \mathrm{Bij}(G, G)$ l'ensemble des bijections de G vers G.

1. Soit E un ensemble. Rappeler très brièvement pourquoi $(\mathcal{S}_E, \circ)$ est un groupe.
2. Montrer que l'application
$$\begin{aligned} G &\to \mathcal{S}_G \\ g &\mapsto (x \mapsto gx) \end{aligned}$$
est bien définie, et est un morphisme de groupes injectif.
3. Montrer qu'il existe un ensemble E et un sous-groupe H de $\mathcal{S}_E$ tel que $(G, \cdot)$ est isomorphe à $(H, \circ)$.
4. Commenter.

Indication p. 31

Exercice 19 (◔★ Centre)
Soit $(G, \cdot)$ un groupe.

On appelle *centre* de G, noté $Z(G)$, l'ensemble des éléments commutant avec tous les autres éléments c'est à dire
$$Z(G) = \{z \in G \mid \forall x \in G, xz = zx\}.$$

1. Montrer que $Z(G)$ est un sous-groupe de G.
2. En utilisant l'exercice 17 montrer en une ligne que $Z(G)$ est un sous-groupe de G.

Indication p. 31

Exercice 20 (◑★ Centralisateur d'une partie)
Soit $(G, \cdot)$ un groupe.

Pour $A \subset G$ on appelle *centralisateur* de A, noté $C_G(A)$ l'ensemble des éléments qui commutent avec tout élément de A c'est à dire

$$C_G(A) = \{y \in G \mid \forall x \in A, xy = yx\}.$$

1. Montrer que pour toute partie A, $C_G(A)$ est un sous-groupe de G.
2. Soient A et B des parties de G.

   Montrer que si $A \subset B$ alors $C_G(A) \supset C_G(B)$.
3. Soit A une partie de G.

   Montrer que $A \subset C_G(C_G(A))$.
4. Soit A une partie de G.

   Montrer que $C_G(C_G(C_G(A))) = C_G(A)$.

Indication p. 31

Exercice 21 (◔★♣ Groupe engendré par une partie)
Soit $(G, \cdot)$ un groupe.

Soit $A \subset G$ une partie quelconque.

Montrer que l'ensemble des sous-groupes de G contenant A admet un minimum (pour l'inclusion).

{*Ce groupe est appelé sous-groupe engendré par A, noté parfois* $\langle A \rangle$.}

Indication p. 32

Exercice 22 (◔★♠ Vers l'ordre d'un élément)
Soit $(G, \cdot)$ un groupe. On rappelle que $(\mathbb{Z}, +)$ est un groupe.

Soit $x \in G$.

1. Montrer que
$$\begin{aligned} \varphi : \mathbb{Z} &\to G \\ n &\mapsto x^n \end{aligned}$$
est un morphisme de groupes.
2. On note $\langle x \rangle$ le plus petit (pour l'inclusion) sous-groupe de G contenant x.
Montrer que $\mathrm{Im}(\varphi) = \langle x \rangle$.
3. Montrer que $\langle x \rangle$ est fini ssi il existe $d \in \mathbb{N}^*$ tel que
$$\forall n \in \mathbb{Z}, x^n = e_G \Leftrightarrow d \mid n.$$
{*On dit alors que x est d'ordre fini et on appelle d l'ordre de x.*}

Indication p. 32

Exercice 23 (◔★♠ Classes d'équivalence à droite)
Soit $(G, \cdot)$ un groupe.

Soit H un sous-groupe de G.

On définit une relation $\mathcal{R}_H$ sur G par
$$\forall (x, y) \in G^2, x \mathcal{R}_H y \Leftrightarrow xy^{-1} \in H.$$

1. Montrer que $\mathcal{R}_H$ est une relation d'équivalence.
2. Soit $x \in G$. Montrer que la classe d'équivalence de x est
$$Hx = \{hx, h \in H\}.$$
3. Soient $x_1, x_2 \in H$. Expliciter une bijection de Hx_1 vers Hx_2.

Indication p. 32

Exercice 24 (◑★♠ Théorème de Lagrange)
Soit $(G, \cdot)$ un groupe **fini**.

1. Soit H un sous-groupe de G. En utilisant l'exercice 23 montrer que
$$\boxed{|H| \mid |G|}.$$
2. Avec les notations de l'exercice 23, montrer que pour tout $x \in G$, l'ordre de x divise $|G|$.

Indication p. 32

Exercice 25 (◔★ Une version très allégée de Lagrange)
Soit $(G, \cdot)$ un groupe **fini** et **abélien**.

Soit $a \in G$.

1. Montrer que
$$\begin{aligned} \tau_a : G &\to G \\ x &\mapsto ax \end{aligned}$$
est une bijection.
2. En déduire que
$$\prod_{x \in G} x = a^{|G|} \prod_{x \in G} x.$$
3. Que peut-on conclure ?

Indication p. 32

Exercice 26 (◑★ Sous-groupes finis de $\mathbb{C}^*$)
Soit $(G, \cdot)$ un sous-groupe fini de $\mathbb{C}^*$.
1. Montrer que $G \subset \mathbb{U}$.
2. Montrer que pour tout $z \in G$, il existe $d_z \in \mathbb{N}$ tel que $z^{d_z} = 1$.
3. Montrer qu'il existe $N \in \mathbb{N}^*$ tel que $G \subset \mathbb{U}_N$.
4. Montrer qu'il existe $n \in \mathbb{N}^*$ tel que $G = \mathbb{U}_n$.

Indication p. 32

Exercice 27 (◑☆♠ Sous-groupes distingués, le tout début)
Soit $(G, \cdot)$ un groupe.

Soit H un sous-groupe de G.

On dit que H est *distingué* (ou *normal*) ssi
$$\forall (x, h) \in G \times H, xhx^{-1} \in H.$$

1. Pour $x \in G$, on note $Hx = \{hx, h \in H\}$ et $xH = \{xh, h \in H\}$.
Montrer que H est distingué ssi $Hx = xH$.
2. Montrer que le noyau d'un morphisme de groupes est distingué.

Indication p. 32

Exercice 28 (◕★♠ Sous-groupes distingués, la suite mais pas la fin)
On utilise dans cet exercice les notations de l'exercice 27.

Soit $(G,\cdot)$ un groupe et H un sous-groupe **distingué** de G.

1. Montrer que $\mathcal{R}_H$ définie par

$$\forall (x,y)\in G^2, x\mathcal{R}_H y \Leftrightarrow xy^{-1}\in H$$

est une relation d'équivalence sur G.

On note $\frac{G}{H}$ l'ensemble quotient (au lieu de $\frac{G}{\mathcal{R}_H}$).

Soient $X,Y\in\frac{G}{H}$.

On choisit $x,y\in G$ tels que $X=\mathrm{Cl}(x)$ et $Y=\mathrm{Cl}(y)$. On pose

$$X\cdot Y=\mathrm{Cl}(x\cdot y).$$

1. Justifier la bonne définition de $\cdot$.
2. Montrer que $\left(\frac{G}{H},\cdot\right)$ est un groupe.
3. En déduire que tout groupe distingué est noyau d'un morphisme de groupes.

Indication p. 33

Exercice 29 (◔☆ Sous-groupes ! II)
Montrer que chacun des ensembles suivants,muni du produit matriciel, est un groupe.

1. $\left\{\begin{pmatrix}a&b\\c&d\end{pmatrix}\in M_2(\mathbb{Z})\mid ad-bc=1\right\}$

2. $\left\{\begin{pmatrix}a&b\\-b&a\end{pmatrix},(a,b)\in\mathbb{R}^2\setminus\{(0,0)\}\right\}$

3. $\left\{\begin{pmatrix}1&\alpha\\0&1\end{pmatrix},\alpha\in\mathbb{C}\right\}$

4. $\left\{\begin{pmatrix}a&b\\c&d\end{pmatrix}\in M_2(\mathbb{C})\mid b=0 \text{ et } ad>0\right\}$

5. $\left\{\begin{pmatrix}\cos(\theta)&-\sin(\theta)\\\sin(\theta)&\cos(\theta)\end{pmatrix},\theta\in\mathbb{R}\right\}$

6. $\left\{\begin{pmatrix}a&b\\c&d\end{pmatrix}\in M_2(\mathbb{C})\mid a+b=c+d=1\right\}$

1. $\left\{\begin{pmatrix}a&b\\c&d\end{pmatrix}\in M_2(\mathbb{C})\mid |a|^2+|c|^2=|b|^2+|d|^2=1 \text{ et } a\overline{b}+c\overline{d}=0\right\}$

2. $\left\{\varepsilon M,(\varepsilon,M)\in\{1,i,-1,-i\}\times\left\{I_2,\sigma_x,\sigma_y,\sigma_z\right\}\right\}$

où $I_2=\begin{pmatrix}1&0\\0&1\end{pmatrix}$, $\sigma_x=\begin{pmatrix}0&1\\1&0\end{pmatrix}$, $\sigma_y=\begin{pmatrix}0&-i\\i&0\end{pmatrix}$, $\sigma_z=\begin{pmatrix}1&0\\0&-1\end{pmatrix}$.

Indication p. 33

Exercice 30 (◑☆ Morphismes de $\mathbb{Q}$ dans les groupes finis)
Soit $(G, \cdot)$ un groupe **fini**.

Montrer que tout morphisme de groupe de $(\mathbb{Q}, +)$ vers $(G, \cdot)$ est constant.

Indication p. 33

Exercice 31 (◔☆ Groupes des similitudes directes)
On rappelle qu'une similitude directe est une application de la forme

$$\begin{aligned} \mathbb{C} &\to \mathbb{C} \\ z &\mapsto az + b \end{aligned}$$

où $(a, b) \in \mathbb{C}^* \times \mathbb{C}$.

1. Montrer que l'ensemble des similitudes directes muni de la composition est un groupe.
2. Montrer que l'ensemble des translations (c'est à dire des $z \mapsto 1z + b$, $b \in \mathbb{C}$) est un groupe.
3. L'ensemble des rotations (c'est à dire des $z \mapsto e^{i\theta}(z - \omega) + \omega$, $(\theta, \omega) \in \mathbb{R} \times \mathbb{C}$) est-il un groupe ?

Indication p. 33

Exercice 32 (◔★ Commutateurs)
Soit $(G, \cdot)$ un groupe.

Pour deux éléments g_1 et g_2 de G on appelle *commutateur* de g_1 et g_2 l'élément

$$[g_1, g_2] = g_1^{-1} g_2^{-1} g_1 g_2.$$

1. Montrer que pour tous $(g_1, g_2) \in G^2$, g_1 et g_2 commutent ssi $[g_1, g_2] = e_G$.
2. Montrer que
$$\forall (g_1, g_2) \in G^2, ([g_1, g_2])^{-1} = [g_2, g_1].$$
3. Soit $(H, *)$ un groupe et $f : G \to H$ un morphisme de groupe.

   Montrer que
$$\forall (g_1, g_2) \in G^2, f([g_1, g_2]) = [f(g_1), f(g_2)].$$

Indication p. 33

Exercice 33 (◔★♣ Inclusions des noyaux et images version essentielle)
Soient $(F, *_F)$, $(G, *_G)$,$(H, *_H)$ des groupes, $\varphi : F \to G$ et $\psi : G \to H$ des morphismes de groupes.

Montrer que

$$\mathrm{Ker}(\varphi) \subset \mathrm{Ker}(\psi \circ \varphi)$$

et que

$$\mathrm{Im}(\psi \circ \varphi) \subset \mathrm{Im}(\psi).$$

Indication p. 33 · Solution p. 40

Exercice 34 (◔★♠ Inclusion des noyaux, version cas d'égalité)
Soient $(F, *_F)$, $(G, *_G)$,$(H, *_H)$ des groupes, $\varphi : F \to G$ et $\psi : G \to H$ des morphismes de groupes.

Montrer que

$$\mathrm{Ker}(\varphi) = \mathrm{Ker}(\psi \circ \varphi) \Leftrightarrow \mathrm{Ker}(\psi) \cap \mathrm{Im}(\varphi) = \{e_G\}.$$

Indication p. 33 · Solution p. 40

Exercice 35 (◑★ Inclusion des images, version cas d'égalité)
Soient $(F, *_F)$, $(G, *_G)$,$(H, *_H)$ des groupes, $\varphi : F \to G$ et $\psi : G \to H$ des morphismes de groupes.

Montrer que

$$\mathrm{Im}(\psi) = \mathrm{Im}(\psi \circ \varphi) \Leftrightarrow G = \{\kappa *_G \xi, (\kappa, \xi) \in \mathrm{Ker}(\psi) \times \mathrm{Im}(\varphi)\}.$$

Indication p. 33 · Solution p. 41

Exercice 36 (◑★ Une formule ayant beaucoup de noms)
Soient $(G, \cdot)$ et $(H, *)$ deux groupes. On suppose de plus que G est **finie**.

Montrer que $\mathrm{Ker}(\varphi)$ et $\mathrm{Im}(\varphi)$ sont finis et que

$$|\ G\ | = |\ \mathrm{Ker}(\varphi)\ \|\ \mathrm{Im}(\varphi)|.$$

Indication p. 34

Exercice 37 (◕★ Actions, orbites et stabilisateurs)
Soit $(G, \cdot)$ un groupe et E un ensemble.

Soit φ un morphisme de groupes $\varphi : (G, \cdot) \to (\mathcal{S}_E, \circ)$ (on dit alors que φ est une *action* de G sur E).

1. Pour $x \in E$ on définit *l'orbite* de x par
$$\mathrm{Orb}(x) = \{\varphi(g)(x), g \in G\}.$$
Montrer que l'ensemble des orbites est une partition de E.
2. Pour $x \in E$ on définit le *stabilisateur* de x par
$$\mathrm{Stab}(x) = \{g \in G \mid \varphi(g)(x) = x\}.$$
Montrer que pour tout $x \in E$, le stabilisateur de x est un sous-groupe de G.
3. Montrer que si G est fini, pour tout $x \in E$, $\mathrm{Orb}(x)$ est fini et
$$|\mathrm{Orb}(x)| = \frac{|G|}{|\mathrm{Stab}(x)|}.$$

Indication p. 34

Exercice 38 (◑☆ Beaucoup de sous-groupes)
Soit $(G, \cdot)$ un groupe.

On suppose que G est infini. Montrer que G admet une infinité de sous-groupes.

Indication p. 34

Exercice 39 (◑☆ Trop d'éléments)
Soit $(G, \cdot)$ un groupe fini.

Soient A et B deux parties de G telles que $|A| + |B| > |G|$.

Montrer que tout élément de G peut s'écrire sous la forme ab, où $a \in A$ et $b \in B$.

Indication p. 34

Exercice 40 (●★ Probabilité de commuter)
Soit $(G, \cdot)$ un groupe fini **non abélien**.

Soit X et Y deux variables aléatoires indépendantes de loi uniforme sur G.

Montrer que

$$\mathbb{P}(XY = YX) \leq \frac{5}{8}.$$

Indication p. 34

Exercice 41 (◑★ Produit semi-direct)
Soient $(G, *)$ et $(H, \cdot)$ deux groupes.

Soit $\varphi : (H, \cdot) \to (\mathrm{Aut}(G), \circ)$ un morphisme de groupes.

On définit une opération $\star$ sur $G \times H$ par

$$\forall ((g,h),(g',h')) \in (G \times H)^2, (g,h) \star (g',h') = (g * \phi(h)(g), h \cdot h').$$

Montrer que $(G \times H, \star)$ est un groupe.

(*Ce groupe est appelé produit semi-direct de G par H relativement à φ et noté $G \rtimes_\varphi H$.*)

Indication p. 34

Exercice 42 (◑☆ Produit et sous-groupes)
Soit $(G, \cdot)$ un groupe, H et K deux sous-groupes de G.

On note $HK = \{hk, (h,k) \in H \times K\}$ et $KH = \{kh, (k,h) \in K \times H\}$.

Montrer que HK est un groupe ssi $HK = KH$.

Indication p. 35

Exercice 43 (◔★ Union croissante)
Soit $(G, \cdot)$ un groupe.

Soient $(H_n)_{n\in\mathbb{N}}$ une suite croissante (pour l'inclusion) de sous-groupes de G.

Montrer que

$$\bigcup_{n\in\mathbb{N}} H_n$$

est un sous-groupe de G.

Commenter.

Indication p. 35

Exercice 44 (◕★ Groupe de Prüfer)
Soit p un nombre premier.

On pose

$$\mathbb{U}_{p^\infty} = \bigcup_{n\in\mathbb{N}} \mathbb{U}_{p^n}.$$

1. Montrer que $\mathbb{U}_{p^\infty}$ est un sous-groupe de $(\mathbb{C}^*, \times)$.
2. Déterminer tous les sous-groupes de $\mathbb{U}_{p^\infty}$.

Indication p. 35

Exercice 45 (◔☆ La finitude arrange beaucoup de choses)
Soit $(G, \cdot)$ un groupe.

Soit $A \subset G$ une partie **finie** de G.

On suppose A non vide et stable par produit.

Montrer que A est un sous-groupe de G.

Indication p. 35

Exercice 46 (◑★ Sous-groupes de $\mathbb{Z}^2$)
On considère $\mathbb{Z}^2$ muni de la loi $+$.

1. Soient $u_1, u_2 \in \mathbb{Z}^2$.

Montrer que

$$\mathbb{Z}u_1 + \mathbb{Z}u_2 = \{a_1u_1 + a_2u_2, (a_1, a_2) \in \mathbb{Z}^2\}$$

est un sous-groupe de $\mathbb{Z}^2$.

Soit $H \subset \mathbb{Z}^2$ un sous-groupe de $\mathbb{Z}^2$.

On note π_1 la projection de $\mathbb{Z}^2$ sur $\mathbb{Z}$:

$$\pi : \mathbb{Z}^2 \to \mathbb{Z}$$
$$\begin{pmatrix} x \\ y \end{pmatrix} \mapsto x.$$

1. Montrer qu'il existe un et unique $d_1 \in \mathbb{N}$ tel que $\pi_1(H) = d_1\mathbb{Z}$.

2. Que dire si $d_1 = 0$?

On suppose désormais $d_1 > 0$.

3. Soit $u_1 \in H$ tel que $\pi_1(u_1) = d_1$.

Montrer qu'il existe $u_2 \in H$ tel que

$$H = \mathbb{Z}u_1 + \mathbb{Z}u_2.$$

Indication p. 35

Anneaux

Exercice 47 (◔★♣ Un bout du cours sur les anneaux)

1. Montrer qu'une intersection de sous-anneaux est un sous-anneau.

2. Montrer qu'un sous-anneau est un anneau.

Indication p. 35

Exercice 48 (◔★♣ Un bout du cours sur les anneaux II)

1. Montrer qu'une composée de morphismes d'anneaux est un morphisme d'anneaux.

2. Montrer que la réciproque d'un morphisme d'anneaux bijectif est un morphisme d'anneaux.

Indication p. 35

Exercice 49 (◔★♣ Binôme et Bernoulli)
Soit $(A, +, \cdot)$ un anneau.

Soient a et b deux éléments de A **qui commutent** entre eux (c'est à dire tels que $ab = ba$).

1. Montrer que pour tout $n \in \mathbb{N}$,
$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}.$$
2. Montrer que pour tout $n \in \mathbb{N}$,
$$a^n - b^n = (a-b) \sum_{k=0}^{n-1} a^k b^{n-1-k}.$$

Indication p. 35

Exercice 50 (◔★ Un bout du cours: Idéaux et noyaux de morphismes d'anneaux)
Soit $(A, +, \cdot)$ un anneau.

On rappelle que $I \subset A$ est appelée *idéal* de A ssi
- ▷ I est un sous-groupe de $(A, +)$
- ▷ I est stable par produit à gauche et à droite par des éléments quelconques de l'anneau
$$\forall x \in I, \forall a \in A, ax \in I \quad \text{et} \quad xa \in I.$$

1. Montrer que l'intersection de deux idéaux est un idéal.
2. Donner un exemple de morphisme d'anneaux dont le noyau n'est **pas** un sous-anneau de l'anneau de départ.
3. Montrer que le noyau d'un morphisme d'anneaux est un idéal de l'anneau de départ.

Indication p. 35

Exercice 51 (◔★ Il faudra faire attention en arithmétique)
Soit $(A, +, \cdot)$ un anneau **intègre**.

On définit la relation de divisibilité $|$ sur A par
$$\forall (a,b) \in A^2, a \mid b \Leftrightarrow \exists q \in A, b = aq.$$

1. Montrer que $|$ est réflexive et transitive.
2. Montrer que pour tout $a, b \in A$ on a
$$(a|b \quad \text{et} \quad b|a) \Leftrightarrow (\exists u \in A^\times, a = bu).$$
3. Commenter.

Indication p. 36

Exercice 52 (◑★ Encore des manipulations d'idéaux)
Soit $(A, +, \cdot)$ un anneau.

1. On suppose que A est **commutatif**.

   Soit $x \in A$. Montrer que
   $$xA = \{xa, a \in A\}$$
   est un idéal de A.
2. Donner un exemple d'anneau et d'idéal qui n'est pas de la forme xA pour un certain $x \in A$.
3. Soient I et J deux idéaux de A.

   Montrer que
   $$I + J = \{i + j, (i, j) \in I \times J\}$$
   est un idéal de A.
4. On suppose que A est **commutatif**.

   Soient I et J deux idéaux de A.

   Montrer que
   $$IJ = \left\{ a \in A \mid \exists n \in \mathbb{N}, \exists \Big((i_k)_{k\in[\![1,n]\!]}, (j_k)_{k\in[\![1,n]\!]} \Big) \in I^n \times J^n, a = \sum_{k=1}^{n} i_k j_k \right\}$$
   est un idéal de A.
5. On suppose que A est **commutatif**.

   Soient I, J, K des idéaux de A.

   Montrer que
   $$I(J + K) = IJ + IK.$$

Indication p. 36

Exercice 53 (◔★ Inversibles d'un sous anneau)

1. Soit $(A, +, \cdot)$ un anneau et B un sous-anneau de A.

Montrer que

$$B^\times \subset A^\times \cap B.$$

2. On munit $\mathbb{Q}$ de sa structure d'anneau usuelle.

Comparer

$$\mathbb{Z}^\times \quad \text{et} \quad \mathbb{Q}^\times \cap \mathbb{Z}.$$

Commenter.

3. Soit A un anneau, et B un sous-anneau **fini** de A.

Soit $a \in A^\times \cap B$.

3.1. Montrer que

$$\tau_a : \begin{array}{c} B \longrightarrow B \\ x \longmapsto ax \end{array}.$$

est bien défini et un morphisme de groupes (additif).

3.2. Montrer que τ_a est injectif.

3.3. En déduire que τ_a est bijectif.

3.4. Conclure que $a \in B^\times$.

3.5. Commenter

Indication p. 36

Exercice 54 (◔★ Non inversibles et diviseurs de zéro)

Soit $(A, +, \cdot)$ un anneau.

1. Un élément inversible peut-il être diviseur de 0 ? Un diviseur de 0 peut-il être inversible ?

2. Dans $(\mathbb{Z}, +, \cdot)$, 2 est-il inversible ? est-il diviseur de 0 ?

3. Soit A un anneau fini. Montrer que tout élément est soit inversible soit un diviseur de 0.

Indication p. 36

Exercice 55 (◔★ Différence symétrique et anneau de Boole)
Soit E un ensemble.

On rappelle que la différence symétrique Δ est l'opération définie sur $\mathcal{P}(E)$ par

$$\forall (A,B) \in \mathcal{P}(E), A\Delta B = (A \cup B) \cap \overline{(A \cap B)}.$$

1. Montrer brièvement que $(\mathcal{P}(E), \Delta)$ est un groupe abélien.
2. Montrer que $(\mathcal{P}(E), \Delta, \cap)$ est un anneau commutatif.
3. Déterminer l'ensemble des éléments inversibles de cet anneau.

Indication p. 36

Exercice 56 (◑☆ Différence symétrique et anneau de Boole II)
On reprend les notations de l'exercice 55.

1. Soit I un idéal de $(\mathcal{P}(E), \Delta, \cap)$. Montrer que I est stable par union finie.
2. Soit I un idéal de $(\mathcal{P}(E), \Delta, \cap)$. Montrer que pour tout $A \subset E$, on a
$$A \in I \Rightarrow (\forall B \in \mathcal{P}(E), B \subset A \Rightarrow B \in I).$$
3. On suppose dans cette question que E est fini.

   Montrer que l'ensemble des idéaux de $(\mathcal{P}(E), \Delta, \cap)$ est l'ensemble des $\mathcal{P}(A)$ où $A \subset B$.
4. Pour $E = \mathbb{N}$, on pose $I = \{X \in \mathcal{P}(E) \mid X \text{ fini.}\}$.

   Montrer que I est un idéal de $(\mathcal{P}(\mathbb{N}), \Delta, \cap)$
5. Commenter.

Indication p. 36

Exercice 57 (◔★♠ Entiers de Gauss)
On note

$$\mathbb{Z}[i] = \{a + ib, (a,b) \in \mathbb{Z}^2\}.$$

1. Montrer que $\mathbb{Z}[i]$ est un anneau commutatif.
2. Déterminer l'ensemble des éléments inversibles.

Indication p. 37

Exercice 58 (◔★♠ Introduction aux nilpotents)
Soit $(A, +, \cdot)$ un anneau.

On dit que $x \in A$ est *nilpotent* ssi il existe $n \in \mathbb{N}$ tel que $x^n = 0_A$.

1. Donner un exemple d'anneau contenant un élément nilpotent non nul.
2. Soit u un élément nilpotent non nul. Montrer qu'il existe $n_0 \in \mathbb{N}^*$ tel que
$$u^{n_0-1} \neq 0_A \quad \text{et} \quad \forall n \geq n_0, u^n = 0_A.$$

On dit alors que n_0 est l'ordre de nilpotence de u.

1. Un élément nilpotent peut-il être régulier ?
2. Soit u un élément nilpotent. Montrer que $1_A - u$ est inversible.

Indication p. 37

Exercice 59 (◔★ Un peu de nilpotents et produits)
Soit $(A, +, \cdot)$ un anneau.

On rappelle que $x \in A$ est *nilpotent* ssi il existe $n \in \mathbb{N}$ tel que $x^n = 0_A$.

1. Donner un exemple d'anneau contenant deux éléments nilpotents dont le produit n'est **pas** nilpotent.
2. Montrer que le produit de deux éléments **qui commutent** et donc l'un est nilpotent est un élément nilpotent.
3. Soient u un élément inversible et n un élément nilpotent **qui commutent**. Montrer que $u + n$ est inversible.
4. Soient a et b des éléments de A tels que ab est nilpotent. Montrer que ba est nilpotent.

Indication p. 37

Exercice 60 (◑★ Vers un lien spectral entre AB et BA)
Soit $(A, +, \cdot)$ un anneau.

Soient $a, b \in A$ tels que $1_A - ab \in A^\times$.

Montrer que $1_A - ba \in A^\times$.

Indication p. 37

Exercice 61 (◑☆ Un cas très particulier d'un théorème de Jacobson)
Soit $(A, +, \cdot)$ un anneau tel que pour tout $x \in A$, $x^2 = x$.

Montrer que A est commutatif.

Indication p. 37

Exercice 62 (◔★ Début d'étude de $\mathbb{Z}\left[\sqrt{d}\right]$)
Soit $d \in \mathbb{N}$ n'étant pas le carré d'un entier.

On note

$$\mathbb{Z}\left[\sqrt{d}\right] = \left\{a + b\sqrt{d}, (a,b) \in \mathbb{Z}^2\right\}.$$

1. Montrer que l'application

$$\begin{aligned} p : \mathbb{Z}^2 &\to \mathbb{Z}\left[\sqrt{d}\right] \\ (a,b) &\mapsto a + b\sqrt{d} \end{aligned}$$

est bijective.

2. Montrer que $\mathbb{Z}\left[\sqrt{d}\right]$ est un anneau.

3. Montrer que l'application $\sigma : \mathbb{Z}\left[\sqrt{d}\right] \to \mathbb{Z}\left[\sqrt{d}\right]$ définie par

$$\forall (a,b) \in \mathbb{Z}^2, \sigma\left(a + b\sqrt{d}\right) = a - b\sqrt{d}$$

est **bien définie** et est un automorphisme d'anneau.

4. Montrer que

$$\mathbb{Z}\left[\sqrt{d}\right]^\times = \left\{u \in \mathbb{Z}\left[\sqrt{d}\right] \mid u\sigma(u) = \pm 1\right\}.$$

Indication p. 37

Exercice 63 (◑☆ Radical d'un idéal)
Soit $(A, +, \cdot)$ un anneau **commutatif**.

Pour I un idéal de A on note

$$\sqrt{I} = \{x \in A \mid \exists n \in \mathbb{N}, x^n \in I\}$$

1. Soit I un idéal de A.

Montrer que $\sqrt{I}$ est un idéal de A contenant I.

2. Soit I un idéal.

Montrer que

$$\sqrt{\sqrt{I}} = \sqrt{I}.$$

3. Soient I et J des idéaux de A.

Montrer que

$$\sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$$

et

$$\sqrt{I + J} \supset \sqrt{I} + \sqrt{J}.$$

Indication p. 37

Exercice 64 (◕☆ Jouons encore avec des idéaux radicaux)
Soit $(A, +, \cdot)$ un anneau **commutatif**.

On réutilise les notations de l'exercice 63. Les questions suivantes sont indépendantes.

1. Soient I et J des idéaux de A.

Montrer que

$$\sqrt{I + J} = \sqrt{\sqrt{I} + \sqrt{J}}.$$

2. Quel nom donner à $\sqrt{\{0\}}$?

3. On considère dans cette question $A = \mathbb{Z}$ muni des opérations usuelles.

Soit $n \in \mathbb{N}$.

Déterminer $\sqrt{n\mathbb{Z}}$.

Indication p. 38

Corps

Exercice 65 (◔★♠ Morphismes entre corps)
Montrer que tout morphisme d'anneaux entre deux corps est injectif.

Indication p. 38

Exercice 66 (◔★♠ Caractéristique d'un corps)
Soit $(\mathbb{K}, +, \cdot)$ un corps.

1. Montrer que
$$\begin{aligned}\varphi : \mathbb{Z} &\to \mathbb{K}\\ n &\mapsto n1_{\mathbb{K}}\end{aligned}$$
est un morphisme d'anneaux.
2. Montrer qu'il existe un unique $p \in \mathbb{N}$ tel que $\mathrm{Ker}(\varphi) = p\mathbb{Z}$.
3. Montrer que p est premier ou nul.

L'entier p est appelé la caractéristique du corps $\mathbb{K}$.

1. On suppose que $p \neq 0$.
Montrer que
$$\begin{aligned}\mathbb{K} &\to \mathbb{K}\\ x &\mapsto x^p\end{aligned}$$
est un endomorphisme (appelé morphisme de Frobenius).
2. Montrer que si $\mathbb{K}$ est fini alors le morphisme de Frobenius est un automorphisme de $\mathbb{K}$.
3. $\star$ (*Nécessite le cours d'algèbre linéaire*)
Soit $\mathbb{K}$ un corps **fini**.
Montrer que sa caractéristique p est non nulle et qu'il existe un entier n tel que $|\mathbb{K}| = p^n$.
4. $\star$ (*Nécessite le cours de fractions rationnelles*)
Montrer que pour $\mathbb{K} = \frac{\mathbb{Z}}{p}\mathbb{Z}(X)$, le corps des fractions rationnelles à coefficients dans $\frac{\mathbb{Z}}{p}\mathbb{Z}$, on a $\mathbb{K}$ de caractéristique p et le morphisme de Frobenius n'est pas surjectif.

Indication p. 38

Exercice 67 (◔★ Une construction matricielle des complexes)
On note

$$\tilde{\mathbb{C}} = \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix}, (a,b) \in \mathbb{R}^2 \right\}.$$

1. Montrer que $\tilde{\mathbb{C}}$ est un sous-anneau de $M_2(\mathbb{R})$.
2. Montrer que $\tilde{\mathbb{C}}$ est un corps.
3. Commenter.

Indication p. 38

Exercice 68 (◑★ Une construction matricielle des quaternions)
On note

$$\mathbb{H} = \left\{ \begin{pmatrix} u & -\overline{v} \\ v & \overline{u} \end{pmatrix}, (u,v) \in \mathbb{C}^2 \right\}.$$

1. Montrer que $\mathbb{H}$ est un sous-anneau de $M_2(\mathbb{C})$.
2. Montrer tout élément non nul de $\mathbb{H}$ est inversible.
3. Commenter.

Indication p. 38

Exercice 69 (◑★ Un zeste d'algébriques)
Soit $\alpha \in \mathbb{C}$. On suppose qu'il existe un polynôme P de degré 2 à **coefficients rationnels** tel que

$$P(\alpha) = 0.$$

On pose

$$\mathbb{Q}(\alpha) = \{x + y\alpha, (x,y) \in \mathbb{Q}^2\}$$

1. Que dire si $\alpha \in \mathbb{Q}$?

On suppose désormais que $\alpha \notin \mathbb{Q}$.

1. Montrer que $\mathbb{Q}(\alpha)$ est un anneau.
2. Montrer que $\mathbb{Q}(\alpha)$ est un corps.

Indication p. 39

Exercice 70 (◔☆ i versus j)
On note $j = e^{\frac{2i\pi}{3}}$.

Montrer que les corps $\mathbb{Q}(i)$ et $\mathbb{Q}(j)$ (définis à l'exercice 69) ne sont pas isomorphes.

Indication p. 39

Exercice 71 (◔☆ Corps fini à 4 éléments)
Construire un corps fini à 4 éléments.

Indication p. 39

Indications

Indication 1 · Énoncé p. 2 (Puissances d'un inversible dans un monoïde)
Par récurrence, pour $n \in \mathbb{N}$.

Avec $n = -(-n)$ pour $n \in \mathbb{Z} \setminus \mathbb{N}$.

Indication 2 · Énoncé p. 2 (Juste la droite ou juste la gauche suffit)

1. Il faut vérifier que e est aussi un « neutre à gauche » et que les éléments sont aussi « inversibles à gauche ».

On fixe un tel $e \in G$.

Soit $x \in G$ et soit $\tilde{x} \in G$ tel que $x\tilde{x} = e$.

En calculant avec précautions:

- ▷ Montrer que $(x\tilde{x})(x\tilde{x}) = (x\tilde{x})$
- ▷ En notant $y = (x\tilde{x})$ et $\tilde{y}$ un inverse à droite de y, calculer $yy\tilde{y}$ et en déduire que $y = e$.
- ▷ Conclure que $\tilde{x}x = e$.

Un inverse à droite est donc un inverse à gauche.

- ▷ Remarquer que $ex = (x\tilde{x})x$ pour montrer que $ex = e$.

Le neutre est donc aussi le neutre à gauche.

Conclure.

2. Vérifier que

- ▷ Pour tous $x, y, z \in \mathbb{C}^*$, $(x\blacklozenge y)\blacklozenge z = |x|\ |y|\ z = x\blacklozenge(y\blacklozenge z)$.
- ▷ Tout nombre complexe de module 1 est un neutre à gauche.
- ▷ Étant donné $\omega \in \mathbb{U}$, pour tout $z \in \mathbb{C}^*$, $\frac{\omega}{|z|}$ est un inverse à droite.

Mais ce n'est pas un groupe car il n'y a pas exemple pas de neutre à gauche (pourquoi ?).

3. Si l'existence de neutres à droite et d'inverses à droite (ou à gauche et à gauche) implique les autres côtés, ce n'est pas le cas de l'existence de neutres à droite et d'inverses à gauches (ou à gauche et à droite).

Dans le doute mieux vaut donc vérifier la définition complète.

Indication 3 · Énoncé p. 3 (Maximum et minimum comme opérations)

1. Pour l'associativité, montrer que $\max(\max(x, y), z) = \max(x, y, z)$.

2. Remarquer que si E admet un plus petit élément alors ce dernier est neutre pour max (et un plus grand neutre pour min).

Indication 4 · Énoncé p. 3 (Encore la relation de similitude)
Montrer que c'est une relation d'équivalence (cf TD relations).

C'est un cas général de par exemple la relation de similitude sur les matrices carrés ($M = \mathrm{M}_n(\mathbb{R})$).

Indication 5 · Énoncé p. 3 (Opération opposée)

1. Vérifier les définitions.
2. Prendre $(\mathcal{F}(E,E),\circ)$ et remarquer que les constantes sont absorbantes à gauche mais qu'il n'y a pas d'éléments absorbants à droite.
3. Que dire de l'inverse ?

Indication 6 · Énoncé p. 4 (Groupes isomorphes)

1. Par exemple $\mathbb{U}_n$ et $\frac{\mathbb{Z}}{n\mathbb{Z}}$ sont isomorphes ou encore $(\mathbb{R},+)$ et $(\mathbb{R}_+^*,\times)$.

   Pour deux groupes non isomorphes on peut prendre deux groupes qui n'ont pas le même cardinal.

   Ou bien constater que $\mathbb{U}_4$ et $\mathbb{U}_2\times\mathbb{U}_2$ ne sont pas isomorphes, ou encore $(\mathbb{R},+)$ et $(\mathbb{R}^*,\times)$, cf exercice 7.

   Voir aussi les exemples des autres exercices.
2. Cf cours:
   - ▷ L'identité est un morphisme.
   - ▷ La composée de morphismes est un morphisme.
   - ▷ La réciproque d'un morphisme bijectif est un morphisme.
3. Cela ressemble très fort à une relation d'équivalence. Mais a priori mieux vaut éviter de parler «d'ensemble de tous les groupes».

Indication 7 · Énoncé p. 4 (Groupes non isomorphes)
Dans les deux cas identifier une propriété stable par isomorphisme que satisfait un élément dans un groupe et pas dans l'autre.

Par exemple (mais ce n'est pas le seul), l'ordre.

1. Existe-t-il un élément x tel que $x\neq e$ et $x^2=e$?
2. Existe-t-il un élément tel que $x^2\neq e$ et $x^4=e$?

Indication 8 · Énoncé p. 4 (Sous-groupes ? I)
Pour montrer que c'est un sous-groupe vérifier la définition, ou exhiber un morphisme dont c'est le noyau ou l'image.

Pour montrer que ce n'en n'est pas un sous-groupe montrer sur un contre-exemple qu'une des propriétés de la définition n'est pas vérifiée.

On obtient (sauf erreur de ma part)

1. Oui.
2. Non.
3. Oui.
4. Non.
5. Non.
6. Oui.

Indication 9 · Énoncé p. 4 (Un classique)
Soient x et y deux éléments de G.

Constater que

$$x(xy)^2y = x^2yxy^2.$$

Indication 10 · Énoncé p. 5 (Raffinement d'un exercice précédent)
Le groupe est commutatif par l'exercice 9.

Il y a ensuite plusieurs méthodes selon les connaissances:

- ▷ Si on connaît l'algèbre linéaire alors on peut le munir d'une structure de $\frac{\mathbb{Z}}{2}\mathbb{Z}$-espace vectoriel.
- ▷ Si on connaît le théorème de structure des groupes abéliens finis on peut directement conclure.
- ▷ Sinon ⋮

Indication 11 · Énoncé p. 5 (Union de sous-groupes ?)

1. Vérifier que la définition de sous-groupe est stable par intersection (cf cours).
2. D'après la question précédente il suffit de prendre deux sous-groupes quelconques dont aucun n'est inclus dans l'autre.

   Pour démontrer que $H_1 \cup H_2$ n'est **pas** un sous-groupe, montrer qu'il n'est par exemple pas stable par produit (ne pas oublier de faire la preuve).
3. Pour montrer «$H_1 \subset H_2$ ou $H_2 \subset H_1$» on peut par exemple montrer «$H_1 \not\subset H_2 \Rightarrow H_2 \subset H_1$».

   Et pour montrer cette implication remarquer si $H_1 \cup H_2$ est un sous-groupe, alors si il existe $\xi_1 \in H_1 \cap \overline{H_2}$ (fixons le), pour tout $x_2 \in H_2$ on a $x_2\xi_1 \in H_1 \cup H_2$.

Indication 12 · Énoncé p. 5 (Loi de composition des vitesses relativistes)
Vérifier à la main la définition. Ou bien «tangente hyperbolique» et exercice 13

Indication 13 · Énoncé p. 5 (Transport de loi)
Attention ici φ^{-1} est la bijection réciproque (et non l'application image réciproque).

Vérifier toutes les propriétés d'un groupe.

Sans surprise le neutre est $\varphi^{-1}(e_G)$ et l'inverse de x est $\varphi^{-1}(\varphi(x)^{-1})$.

Ne pas hésiter à faire un schéma.

Indication 14 · Énoncé p. 6 (Petite translation)
Vérifier à la main toutes les propriétés.

Ou bien regarder l'exercice 13 et l'application $x \mapsto a * x$ (ou $x \mapsto x * a$).

Indication 15 · Énoncé p. 6 (Sous-groupes additifs de $\mathbb{Z}$)
Traiter le cas $H = \{0\}$.

Justifier ensuite l'existence de $m = \min(H \cap \mathbb{N}^*)$.

Procéder ensuite par double inclusion.

Pour $H \subset m\mathbb{Z}$, soit $h \in H$.

Remarquer que le reste de la division de h par m est dans $H \cap [\![0, m-1]\!]$.

Indication 16 · Énoncé p. 6 (Groupe des automorphismes)
Montrer que c'est un sous-groupe de $\mathrm{Bij}(G, G)$. Pour cela montrer:

- ▷ Id_E est un automorphisme.
- ▷ Une composée d'automorphismes de groupes est un automorphisme de groupe.
- ▷ La bijection réciproque d'un automorphisme de groupes est aussi un automorphisme de groupe.

Indication 17 · Énoncé p. 6 (Conjugaisons et automorphismes intérieurs)

1. Il faut donc vérifier que φ_u est un morphisme et qu'il est bijectif. Pour le premier point écrire la définition. Pour le second par exemple proposer une réciproque.

2. Par la question précédent Φ est bien défini. Pour montrer que c'est un morphisme, il faut donc montrer

$$\forall (u, v) \in G^2, \varphi_{uv} = \varphi_u \circ \varphi_v$$

c'est à dire (égalité d'applications)

$$\forall (u, v) \in G^2, \forall x \in G, \varphi_{uv}(x) = \varphi_u(\varphi_v(x)).$$

3. On a non-injectivité de Φ dès qu'un élément différent de l'identité commute avec tous les autres (cf exo 19). Choisir par exemple un groupe commutatif, par exemple $(G, \cdot) = (\mathbb{C}^*, \cdot)$.

Remarquer que pour cet exemple particulier il y a aussi non-surjectivité.

Indication 18 · Énoncé p. 7 (Les groupes des permutations sont compliqués !)

1. Identité, composée de bijections, bijection réciproque d'une bijection.

2. Plusieurs points à vérifier:

- ▷ Que $x \mapsto gx$ est bien bijective (par exemple proposer une bijection réciproque),
- ▷ Que c'est un morphisme de groupes,
- ▷ Qu'il est injectif (i.e son noyau est $\{1_G\}$).

Pour chacun des points écrire les définitions et procéder par rédaction automatique.

3. Que dire de l'image de l'application précédente.

4. Tout groupe est donc isomorphe à un sous-groupe d'un groupe de permutations.

Indication 19 · Énoncé p. 7 (Centre)
Avec les notations de l'exercice 17, que dire de $\mathrm{Ker}(\Phi)$.

Indication 20 · Énoncé p. 8 (Centralisateur d'une partie)

1. Par exemple intersection de sous-groupes.

2. Rédaction automatique: déplier et replier les définitions.

3. Encore rédaction automatique.

4. Par double inclusion.

Indication 21 · Énoncé p. 8 (Groupe engendré par une partie)
Intersection de tous les sous-groupes contenant A (à justifier).

Indication 22 · Énoncé p. 9 (Vers l'ordre d'un élément)
Cf DM.

Indication 23 · Énoncé p. 9 (Classes d'équivalence à droite)

1. Remarquer que chaque point de la définition d'une relation d'équivalence correspond à un point de la définition de groupe.
2. Procéder par double équivalence ou par équivalences avec précaution.
3. Penser à une translation.

Indication 24 · Énoncé p. 9 (Théorème de Lagrange)

1. Remarquer que toutes les classes d'équivalence à droite de l'exercice 23 sont finies et de même cardinal (car en bijections).
2. L'ordre est le cardinal du sous-groupe engendré par x.

Indication 25 · Énoncé p. 10 (Une version très allégée de Lagrange)

1. Bijection réciproque $\tau_{a^{-1}}$.
2. Montrer que $\prod_{x\in G} x = \prod_{\xi\in G}(a\xi)$ et utiliser le caractère abélien.
3. On en déduit:

$$a^{|G|} = 1_G$$

ce qui peut s'interpréter de plusieurs façons:

- ▷ l'ordre (cf exercice 22) d'un élément divise le cardinal du groupe.
- ▷ que le cardinal du groupe engendré $\langle a\rangle$, c'est à dire l'ordre, divise le cardinal du groupe.

On remarque que l'hypothèse de commutativité, si elle est essentielle dans la preuve précédente, n'est en fait pas nécessaire, cf l'exercice 24

Indication 26 · Énoncé p. 10 (Sous-groupes finis de $\mathbb{C}^*$)

1. Sinon, prendre un élément de module différent de 1 et remarquer que toutes ses puissances sont distinctes, car par exemple de modules distincts. Or toute partie de G est finie.
2. Même argument que précédemment, si ce n'est pas le cas alors il y a une infinité de puissance de z distinctes.
3. L'ensemble des $\{d_z, z \in G\}$ admet un majorant non nul (et même un supremum) au sens de la divisibilité car il est fini.
4. S'inspirer des méthodes d'ordre.

Indication 27 · Énoncé p. 10 (Sous-groupes distingués, le tout début)

1. Rédaction automatique.
2. Pour $k \in \mathrm{Ker}(\varphi)$, écrire $\varphi(xkx^{-1}) = \varphi(x)1\varphi(x)^{-1}$.

Indication 28 · Énoncé p. 11 (Sous-groupes distingués, la suite mais pas la fin)

1. Cf par exemple 23.
2. Il faut montrer que le résultat **ne dépend pas du représentant** choisi.
3. Vérification des définitions.
4. Que dire de la «projection canonique»:

$$\begin{aligned} G &\to \frac{G}{H} \\ x &\mapsto \mathrm{Cl}(x) \end{aligned}$$

Indication 29 · Énoncé p. 11 (Sous-groupes ! II)
Dans chaque cas montrer que c'est un sous-groupe de $\mathrm{GL}_n(\mathbb{K})$, ou bien exhiber un morphisme dont c'est le noyau ou l'image.

Indication 30 · Énoncé p. 12 (Morphismes de $\mathbb{Q}$ dans les groupes finis)
On rappelle que comme G est fini, il existe $N \in \mathbb{N}^*$ tel que pour tout $x \in G$, il existe $x^N = 1_G$ (cf ordre).

Et constater qu'étant donné un morphisme φ, pour tout $r \in \mathbb{Q}$ et pour tout $n \in \mathbb{N}^*$, $\varphi(r) = \left(\varphi\left(\frac{r}{n}\right)\right)^n$.

Indication 31 · Énoncé p. 12 (Groupes des similitudes directes)
Montrer qu'il s'agit de sous-groupes.

Remarquer qu'une composée de rotations est une rotation ou une translation.

Indication 32 · Énoncé p. 12 (Commutateurs)
Faire les calculs directement.

Indication 33 · Énoncé p. 13 (Inclusions des noyaux et images version essentielle)
Rédaction automatique.

Solution p. 40

Indication 34 · Énoncé p. 13 (Inclusion des noyaux, version cas d'égalité)
Commencer par traiter l'exercice 33 pour déterminer l'inclusion pertinente.

Rédaction automatique par double implication encore.

Solution p. 40

Indication 35 · Énoncé p. 13 (Inclusion des images, version cas d'égalité)
Commencer par traiter l'exercice 33 pour déterminer quelle est l'inclusion pertinente. Rédaction automatique par double implication encore.

Solution p. 41

Indication 36 · Énoncé p. 13 (Une formule ayant beaucoup de noms)
Considérer la relation d'équivalence $\sim$ sur G définie par

$$\forall (x,y) \in G^2, x \sim y \Leftrightarrow \varphi(x) = \varphi(y)$$

Constater qu'il y a $|\operatorname{Im}(\varphi)|$ classes d'équivalence et qu'elles sont toutes de cardinal $|\operatorname{Ker}(\varphi)|$.

Indication 37 · Énoncé p. 14 (Actions, orbites et stabilisateurs)

1. Vérifier à la main ou bien construire une relation d'équivalence.
2. Vérifier à la main ou bien considérer le noyau d'un morphisme bien choisi de G vers $\mathcal{S}_E$.
3. Considérer la relation d'équivalence de l'exercice 23. Et exhiber une bijection entre $\frac{G}{\operatorname{Stab}}(x)$ et $\operatorname{Orb}(x)$.

Indication 38 · Énoncé p. 14 (Beaucoup de sous-groupes)
Procéder par contraposée.

Si il y a un nombre fini de sous-groupes alors il y a un nombre fini de sous-groupes engendrés par un élément et G et la réunion de ces derniers.

De plus si un sous-groupe engendré par un élément était infini il serait isomorphe à $\mathbb{Z}$ et donc admettrait une infinité de sous-groupes.

Indication 39 · Énoncé p. 14 (Trop d'éléments)
On veut montrer que pour tout $g \in G$, il existe $a \in A$ et $b \in B$ tels que $g = ab$ i.e $gb^{-1} = a$.

On veut donc montrer que $\{a, a \in A\} \cap \{gb^{-1}, b \in B\} \neq \varnothing$.

Indication 40 · Énoncé p. 15 (Probabilité de commuter)
Commencer par traiter les exercices 23, 24, 19, 20.

On a $\mathbb{P}(XY = YX) = \mathbb{P}(Y \in C(X))$ où $C(X)$ est l'ensemble des éléments de G qui commutent avec X (cf exo 32).

Si $X \notin Z(G)$ alors, comme $C(X)$ est un sous-groupe de G strictement inclus dans G alors (Lagrange) $|C(X)| \leq \frac{1}{2}|G|$.

De plus montrer que $|Z(G)| \leq \frac{1}{4}\ |G|$. En effet si $|\ \frac{G}{Z(G)}\ | = 2, 3$ alors G est engendré par son centre et un élément (méditer pourquoi) et donc est abélien.

On a donc $\mathbb{P}(X \in Z(G)) \leq \frac{1}{4}$ et $\mathbb{P}(Y \in C(G) \mid X \in Z(G)) \leq \frac{1}{2}$. La formule des probabilités totales donne le résultat, car $1 \times \frac{1}{4} + \frac{1}{2} \times \frac{3}{4} = \frac{5}{8}$.

Indication 41 · Énoncé p. 15 (Produit semi-direct)
Vérifier les axiomes de groupe.

Ce produit semi-direct peut sembler artificiel, mais est en fait une notion essentielle en théorie des groupes et de manière générale en sciences. Regarder par exemple les «torseurs» et apparenté en SI.

Indication 42 · Énoncé p. 15 (Produit et sous-groupes)
Pour le sens réciproque montrer par des manipulations algébriques que si $HK = KH$ alors HK est stable par produit et inverse.

Pour le sens direct, utiliser la stabilité par inverse.

Indication 43 · Énoncé p. 16 (Union croissante)
Si la suite n'est pas croissante le résultat est faux (cf exercice 11).

De plus on peut remplacer « groupe » par d'autres structures, par exemple anneau, corps, espace vectoriel, etc. (cf la preuve).

Sinon pour l'indication elle est: rédaction automatique.

Indication 44 · Énoncé p. 16 (Groupe de Prüfer)
1. Regarder l'exercice 43.
2. S'inspirer par exemple des sous-groupes de $(\mathbb{R}, +)$ pour montrer que les sous-groupes sont soit $\mathbb{U}_{p^n}$ pour un certain n soit $\mathbb{U}_{p^\infty}$.

Indication 45 · Énoncé p. 16 (La finitude arrange beaucoup de choses)
Soit $x \in A$. On a $\{x^n, n \in \mathbb{N}^*\} \subset A$. Par tiroirs montrer qu'il existe $n_1 < n_2$ tels que $x^{n_2-n_1} = e_G$.

Indication 46 · Énoncé p. 17 (Sous-groupes de $\mathbb{Z}^2$)
1. Automatique.
2. Image d'un morphisme et sous-groupes de $\mathbb{Z}$.
3. Mq H est un sous groupe de $\mathbb{Z}e_2$ où $e_2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$.
4. Que dire pour $x \in H$ de $x - \frac{\pi(x)}{d_1} u_1$?

Indication 47 · Énoncé p. 17 (Un bout du cours sur les anneaux)
RAS, rédaction automatique.

Indication 48 · Énoncé p. 17 (Un bout du cours sur les anneaux II)
RAS, rédaction automatique.

Indication 49 · Énoncé p. 18 (Binôme et Bernoulli)
Il s'agit exactement des mêmes preuves que dans les cas « connus », en prenant garde à ne pas adapter les preuves nécessitant des inverses.
1. Par exemple par récurrence en utilisant la formule de Pascal et le fait que a et b commutent. Ou encore en développant et comptant, en utilisant la commutativité.
2. Par exemple en développant le produit en utilisant la commutativité.

Indication 50 · Énoncé p. 18 (Un bout du cours: Idéaux et noyaux de morphismes d'anneaux)
Rédaction automatique. Pour le contre-exemple constater que tout fonctionne car $f(1) \neq 0$.

Indication 51 · Énoncé p. 18 (Il faudra faire attention en arithmétique)

1. Prendre $q = 1$ et $q = q_1 q_2$.
2. Traiter le cas $a = 0$ ou $b = 0$. Sinon de $a = bq_1$ et $b = q_2 a$ déduire par intégrité que $q_1 q_2 = q_2 q_1 = 1_A$, d'où $q_1 \in A^\times$.
3. Dans $\mathbb{Z}$ comme $\mathbb{Z}^\times = \{-1, +1\}$ on donc, si $n|m$ et $m|n$ alors $n = \pm m$. Même soin à prendre dans $\mathbb{K}[X]$ où $(\mathbb{K}[X])^\times = \{\lambda, \lambda \in \mathbb{K}^\times\}$.

   Pour récupérer une relation d'ordre on pourrait considérer une structure quotient.

Indication 52 · Énoncé p. 19 (Encore des manipulations d'idéaux)
Pour les vérifications la rédaction automatique peut suffire.

Pour le contre-exemple de la question 2, on verra que si $A = \mathbb{Z}$ ou $A = \mathbb{K}[X]$ alors tous les idéaux sont de la forme sus-mentionnée (on parle d'anneaux principaux).

Prendre plutôt $A = \mathbb{Z}[X]$, ou $A = \mathcal{C}^0([0, 1], \mathbb{R})$.

Indication 53 · Énoncé p. 20 (Inversibles d'un sous anneau)

1. Automatique.
2. $\{-1, +1\} \subsetneq \mathbb{Z}\backslash\{0\}$.

   L'inclusion précédent peut donc être stricte.
3. **3.1.** Vérifier que les images sont bien dans B et que c'est un morphisme.
   3.2. Comme a inversible, il est régulier. En déduire le noyau de τ_a.
   3.3. Les cardinaux finis sont les mêmes au départ et à l'arrivée. L'injectivité implique donc la bijectivité.
   3.4. En particulier $1 \in \mathrm{Im}(\tau_a)$.
   3.5. D'où dans le cas où B est **fini** on a $B^\times = A^\times \cap B$.

Indication 54 · Énoncé p. 20 (Non inversibles et diviseurs de zéro)

1. A-t-on $1 = 0$?
2. Ni l'un ni l'autre.
3. S'inspirer de l'exercice 53

Indication 55 · Énoncé p. 21 (Différence symétrique et anneau de Boole)

1. Cf TD ensembles et applications.
2. Idem.
3. Remarquer que pour tout $X \subset E$, $X \Delta X = \varnothing$.

Indication 56 · Énoncé p. 21 (Différence symétrique et anneau de Boole II)

1. Pour X_1 et X_2 deux parties, faire un dessin. Que vaut $(X_1 \Delta X_2)\Delta(X_1 \cap X_2)$?
2. Si $B \subset A$ alors par exemple $B = B \cap A$.
3. Procéder en deux temps.

   ▷ Vérifier que pour $A \subset E$, $\mathcal{P}(A)$ est un idéal.
   ▷ Étant donné un idéal, il est alors fini. Considérer l'union de tous ses éléments. En déduire qu'il est de la forme $\mathcal{P}(A)$.
4. Vérifier la définition.

5. Montrer que I n'est **pas** de la forme $\mathcal{P}(A)$ pour $A \subset \mathbb{N}$.

Indication 57 · Énoncé p. 21 (Entiers de Gauss)

1. Vérifier que c'est un sous-anneau de $(\mathbb{C}, +, \cdot)$.

2. On obtient que ce sont les $a + ib$ tels que $a^2 + b^2 = 1$.

Indication 58 · Énoncé p. 22 (Introduction aux nilpotents)

1. Par exemple $\mathrm{M}_2(\mathbb{R})$ et $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ (il y a plein d'autres exemples matriciels, cf cours d'algèbre linéaire).

2. Toute partie non vide de $\mathbb{N}$ admet un plus petit élément.

3. Non car c'est un diviseur de 0.

4. Penser aux suites géométriques/formule de Bernoulli. Que dire de $1 + u + \cdots + u^{n_0 - 1}$?

Indication 59 · Énoncé p. 22 (Un peu de nilpotents et produits)

1. Calculer $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$.

2. Que dire de $(uv)^n$ si u et v commutent.

3. Remarquer que $u + n = u(1_A + u^{-1}n)$ et que u^{-1} et n commutent.

4. Remarquer que

$$\underbrace{(ba)(ba)\cdots(ba)(ba)}_{n \text{ fois}} = b\underbrace{(ab)\cdots(ab)}_{n-1 \text{ fois}}a.$$

Indication 60 · Énoncé p. 22 (Vers un lien spectral entre AB et BA)
S'inspirer du cas nilpotent.

Que dire de $1 + b(1 - ab)^{-1}a$?

Indication 61 · Énoncé p. 22 (Un cas très particulier d'un théorème de Jacobson)
On pourra commencer par montrer que pour tout x, $2x = 0$.

Indication 62 · Énoncé p. 23 (Début d'étude de $\mathbb{Z}\left[\sqrt{d}\right]$)

1. Le point important est l'injectivité. Le faire à la main et par exemple par l'absurde on peut utiliser que $\sqrt{d} \notin \mathbb{Q}$ pour aboutir à une contradiction.

2. À la main en remarquant que $\sqrt{d} \times \sqrt{d} = d \in \mathbb{Z}$.

Indication 63 · Énoncé p. 24 (Radical d'un idéal)
Se rappeler de l'hypothèse de commutativité: elle permet de bien simplifier les calculs mais il faut faire attention à bien identifier les lieux où on l'utilise.

1. Vérifier la définition d'idéal.

2. Une seule inclusion est intéressante. Remarquer que $(x^n)^m = x^{nm}$.

3. L'inclusion $\sqrt{I \cap J} \subset \sqrt{I} \cap \sqrt{J}$ se fait par rédaction automatique.

Pour l'inclusion $\sqrt{I \cap J} \supset \sqrt{I} \cap \sqrt{J}$ se rappeler l'existence du ppcm (ou bien juste du produit).

Pour $\sqrt{I + J} \supset \sqrt{I} + \sqrt{J}$ mettre à une puissance suffisamment grande par binôme de Newton.

Indication 64 · Énoncé p. 24 (Jouons encore avec des idéaux radicaux)
Commencer bien évidemment par traiter l'exercice 63.

1. Remarque que si $K_1 \subset K_2$ alors $\sqrt{K_1} \subset \sqrt{K_2}$. Ensuite utiliser les inclusions de l'exercice 63.
2. Nil
3. La réponse est: $m\mathbb{Z}$ pour $m = \prod_{p \text{ premier}} p^{\min(v_p(n),1)}$ c'est à dire le produit des facteur premiers de n avec une multiplicité de 1. Il ne reste plus qu'à le démontrer !

Indication 65 · Énoncé p. 25 (Morphismes entre corps)
Que dire des idéaux d'un corps ?

Indication 66 · Énoncé p. 25 (Caractéristique d'un corps)

1. Vérifier la définition.
2. Le noyau est un idéal de $\mathbb{Z}$ donc de la forme $p\mathbb{Z}$.
3. Tout cela reste vrai dans un anneau intègre.
4. On pourra utiliser que si p est premier, alors pour tout $k \in [\![1, p-1]\!]$, $p \mid \binom{p}{k}$.
5. Il est injectif comme morphisme de corps, et donc par cardinal fini.
6. Montrer que l'on peut munir $\mathbb{K}$ d'unes structure de $\frac{\mathbb{Z}}{p}\mathbb{Z}$ espace vectoriel.

   Il est alors de dimension finie.
7. Par degré il n'y a pas d'antécédent de X.

Indication 67 · Énoncé p. 26 (Une construction matricielle des complexes)

1. Vérifier la définition.
2. Utiliser au choix:
   - ▷ vos connaissances des matrices 2×2,
   - ▷ vos connaissances sur les nombres complexes

   pour expliciter l'inverse.
3. On a ainsi «construit» $\mathbb{C}$, le nombre complexe $a + ib$ revenant à la matrice $\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$.

   Cette «analogie» sera très utile en algèbre linéaire pour la compréhension des matrices 2×2.

   Parmi les remarques à faire on peut noter:
   - ▷ L'analogie entre 1 et $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ ainsi que i et $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$.
   - ▷ L'analogie entre $e^{i\theta}$ et la matrice de rotation d'angle θ, $R_\theta = \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix}$.
   - ▷ L'analogie entre conjuguée et transposée.
   - ▷ L'analogie entre module au carré et déterminant.
   - ▷ L'analogie entre trace et partie réelle (fois deux).
   - ▷ etc.

Indication 68 · Énoncé p. 26 (Une construction matricielle des quaternions)
S'inspirer de l'exercice 67.

Remarque: $\mathbb{H}$ est appelé ensemble des quaternions, et il a de nombreuses interprétations et usages, par exemple en algèbre linéaire.

Indication 69 · Énoncé p. 26 (Un zeste d'algébriques)

1. $\mathbb{Q}$
2. Remarquer que α^2 s'exprime comme combinaison linéaire à coefficients rationnels de α et 1.
3. Pour déterminer l'inverse d'un élément non nul on peut effectuer un algorithme d'Euclide sur des polynômes bien choisis. Ou bien résoudre un système linéaire 2×2 (mais c'est moins élégant).

Indication 70 · Énoncé p. 27 (i versus j)
Regarder les autres exercices sur les non-isomorphies.

Par exemple que dire des éléments d'ordre 3 ?

Indication 71 · Énoncé p. 27 (Corps fini à 4 éléments)
Construire à la main la table des produits.

Ou bien appeler les éléments $0, 1, \varphi, \overline{\varphi}$ et se demander pourquoi c'est une bonne idée.

Solutions

Solution pour l'exercice 33 · Énoncé p. 13 · Indication p. 33 (Inclusions des noyaux et images version essentielle)

▷ Soit $x \in \mathrm{Ker}(\varphi)$.

Alors $\varphi(x) = e_G$.

Donc $\psi(\varphi(x)) = \psi(e_G) = e_H$.

Donc $x \in \mathrm{Ker}(\psi \circ \varphi)$.

Ainsi $\boxed{\mathrm{Ker}(\varphi) \subset \mathrm{Ker}(\psi \circ \varphi)}$.

▷ Soit $z \in \mathrm{Im}(\psi \circ \varphi)$.

Alors il existe $x \in F$ tel que $z = \psi(\varphi(x))$.

Avec $y = \varphi(x) \in G$ on a $z = \psi(y)$.

Donc $z \in \mathrm{Im}(\psi)$.

Ainsi $\boxed{\mathrm{Im}(\psi \circ \varphi) \subset \mathrm{Im}(\psi)}$.

Solution pour l'exercice 34 · Énoncé p. 13 · Indication p. 33 (Inclusion des noyaux, version cas d'égalité)

On remarque que comme on a toujours $\mathrm{Ker}(\varphi) \subset \mathrm{Ker}(\psi \circ \varphi)$ (voir par exemple l'exercice 33) il faut et suffit de montrer que

$$\mathrm{Ker}(\varphi) \supset \mathrm{Ker}(\psi \circ \varphi) \Leftrightarrow \mathrm{Ker}(\psi) \cap \mathrm{Im}(\varphi) = \{e_G\}.$$

On procède par double implication.

▷ $\boxed{\Rightarrow}$

Supposons $\mathrm{Ker}(\psi \circ \varphi) \subset \mathrm{Ker}(\varphi)$.

Soit $y \in \mathrm{Ker}(\psi) \cap \mathrm{Im}(\varphi)$.

Comme $y \in \mathrm{Im}(\varphi)$, il existe $x \in F$ tel que $y = \varphi(x)$.

Comme $y \in \mathrm{Ker}(\psi)$, on a $\psi(y) = e_H$.

On a donc $\psi(\varphi(x)) = e_H$ i.e $x \in \mathrm{Ker}(\psi \circ \varphi)$.

Par l'inclusion supposée, on a alors $x \in \mathrm{Ker}(\varphi)$ i.e $\varphi(x) = e_G$.

D'où $y = \varphi(x) = e_G$.

Ainsi $\mathrm{Ker}(\psi) \cap \mathrm{Im}(\varphi) \subset \{e_G\}$.

L'inclusion réciproque est immédiate car $e_G \in \mathrm{Ker}(\psi) \cap \mathrm{Im}(\varphi)$ comme intersection de sous-groupes.

D'où $\boxed{\mathrm{Ker}(\psi) \cap \mathrm{Im}(\varphi) = \{e_G\}}$.

▷ $\boxed{\Leftarrow}$

Supposons $\mathrm{Ker}(\psi) \cap \mathrm{Im}(\varphi) = \{e_G\}$.

Soit $x \in \mathrm{Ker}(\psi \circ \varphi)$.

Alors $\psi(\varphi(x)) = e_H$.

D'où $\varphi(x) \in \mathrm{Ker}(\psi)$.

De plus $\varphi(x) \in \mathrm{Im}(\varphi)$.

D'où $\varphi(x) \in \mathrm{Ker}(\psi) \cap \mathrm{Im}(\varphi)$ et donc par hypothèse $\varphi(x) = e_G$.

Ainsi $x \in \mathrm{Ker}(\varphi)$.

D'où $\boxed{\mathrm{Ker}(\varphi) \supset \mathrm{Ker}(\psi \circ \varphi)}$.

Solution pour l'exercice 35 · Énoncé p. 13 · Indication p. 33 (Inclusion des images, version cas d'égalité)
On notera pour plus de simplicité les produits de manière implicite.

On remarque que comme on a toujours $\mathrm{Im}(\psi \circ \varphi) \subset \mathrm{Im}(\psi)$ (voir par exemple l'exercice 33) il faut et suffit de montrer que

$$\mathrm{Im}(\psi) \subset \mathrm{Im}(\psi \circ \varphi) \Leftrightarrow G = \{\kappa\xi, (\kappa, \xi) \in \mathrm{Ker}(\psi) \times \mathrm{Im}(\varphi)\}.$$

On procède par double implication.

▷ $\boxed{\Rightarrow}$

Supposons $\mathrm{Im}(\psi) \subset \mathrm{Im}(\psi \circ \varphi)$.

Soit $y \in G$.

On a alors $\psi(y) \in \mathrm{Im}(\psi)$.

Par hypothèse on a donc $\psi(y) \in \mathrm{Im}(\psi \circ \varphi)$.

Donc il existe $x \in F$ tel que $\psi(y) = \psi(\varphi(x))$.

Comme $\psi(y) = \psi(\varphi(x))$ et que ψ est un morphisme de groupes on a alors

$$\psi(y(\varphi(x))^{-1}) = \varphi(y)(\psi(\varphi(x)))^{-1} = e_H.$$

Donc $y(\varphi(x))^{-1} \in \mathrm{Ker}(\psi)$.

En posant $\kappa = y(\varphi(x))^{-1} \in \mathrm{Ker}(\psi)$ et $\xi = \varphi(x) \in \mathrm{Im}(\varphi)$ on a donc $y = \kappa\xi$.

Ainsi $G \subset \{\kappa\xi, (\kappa, \xi) \in \mathrm{Ker}(\psi) \times \mathrm{Im}(\varphi)\}$.

L'autre inclusion étant toujours vraie, on a donc $\boxed{G = \{\kappa\xi, (\kappa, \xi) \in \mathrm{Ker}(\psi) \times \mathrm{Im}(\varphi)\}}$.

▷ $\boxed{\Leftarrow}$

Supposons $G = \{\kappa\xi, (\kappa, \xi) \in \mathrm{Ker}(\psi) \times \mathrm{Im}(\varphi)\}$.

Soit $z \in \mathrm{Im}(\psi)$.

Alors il existe $y \in G$ tel que $z = \psi(y)$.

Par hypothèse il existe $(\kappa, \xi) \in \mathrm{Ker}(\psi) \times \mathrm{Im}(\varphi)$ tel que $y = \kappa\xi$.

Comme $\xi \in \mathrm{Im}(\varphi)$, il existe $x \in F$ tel que $\xi = \varphi(x)$.

On a donc, comme ψ est un morphisme de groupes,

$$\psi(y) = \psi(\kappa\xi) = \psi(\kappa)\psi(\xi) = e_H\psi(\varphi(x)) = (\psi \circ \varphi)(x).$$

D'où $z = \psi(y) \in \mathrm{Im}(\psi \circ \varphi)$.

Ainsi $\boxed{\mathrm{Im}(\psi) \subset \mathrm{Im}(\psi \circ \varphi)}$.