EPFL Automne 2022
Algebre Lineaire Avancee, MATH-110

Corrections Série 2

Exercice 1. Montrer qu'un groupe fini $(G, \star, e_G, \bullet^{-1})$ de cardinal $|G| = 2$ est toujours commutatif.

Solution 1. On a $G = \{e_G, g\}$ pour un $g \neq e_G$. Pour la definition d'element neutre on a

$$e_G \star g = g \star e_G = g.$$

Chaque element commute avec lui-meme. On conclut que G est commutatif.

Exercice 2. Dans un exercice de la serie precedente, on a defini pour $q \geqslant 1$ un entier non nul, l'ensemble des classes de congruences modulo q

$$\mathbb{Z}/q\mathbb{Z} = \{a \,(\mathrm{mod}\, q),\ a \in \mathbb{Z}\} \subset \mathscr{P}(\mathbb{Z})$$

avec

$$a \,(\mathrm{mod}\, q) := a + q\mathbb{Z} = \{a + q.k,\ k \in \mathbb{Z}\} \subset \mathbb{Z}.$$

On a egalement defini l'application

$$\pi_q : a \in \mathbb{Z} \mapsto a \,(\mathrm{mod}\, q) \in \mathbb{Z}/q\mathbb{Z}.$$

D'autre part, pour $A, B \in \mathscr{P}(\mathbb{Z})$ des sous-ensembles de $\mathbb{Z}$, on a pose

$$A \boxplus B := \{a + b,\ a \in A,\ b \in B\} \in \mathscr{P}(\mathbb{Z}).$$

On definit egalement

$$\boxminus A := \{-a,\ a \in A\} \in \mathscr{P}(\mathbb{Z}),$$

l'ensemble des opposes des elements de A.

1. Que vaut $\pi_q^{(-1)}(\{a \,(\mathrm{mod}\, q)\}) \subset \mathbb{Z}$?
2. Quel est le cardinal de $\mathbb{Z}/q\mathbb{Z}$?
3. Calculer $\boxminus(a \,(\mathrm{mod}\, q))$?
4. Montrer que $(\mathbb{Z}/q\mathbb{Z}, \boxplus, 0 \,(\mathrm{mod}\, q), \boxminus)$ forme un groupe commutatif.
5. Montrer que l'application $\pi_q : \mathbb{Z} \mapsto \mathbb{Z}/q\mathbb{Z}$ est un morphisme de groupes.

Solution 2.

1. On peut verifier que les ensembles $a \pmod q$ et $b \pmod q$ sont les memes si et seulement si $b = a + q.n$ pour un certain $n \in \mathbb{Z}$. Donc

$$\pi_q^{(-1)}(\{a(\mathrm{mod}\, q)\}) = \{a + nq, n \in \mathbb{Z}\}.$$

2. En utilisant l'observation precedente, nous notons que pour tout $a(\mathrm{mod}\, q)$, il existe un $0 \leqslant r < q$, t.q. $a(\mathrm{mod}\, q) = r(\mathrm{mod}\, q)$. et que si $0 \leqslant r < r' < q$ on a $r(\mathrm{mod}\, q) \neq r'(\mathrm{mod}\, q)$. On a donc

$$\mathbb{Z}/q\mathbb{Z} = \{r \pmod q, 0 \leqslant r < q\}$$

et

$$|\mathbb{Z}/q\mathbb{Z}| = q.$$

3.

$$\begin{aligned}\boxminus(a \pmod q) &= \{-(a + nq), n \in \mathbb{Z}\} = \{-a - nq, n \in \mathbb{Z}\} \\ &= \{-a + mq, m \in \mathbb{Z}\} = (-a) \pmod q\end{aligned}$$

4. (a)

$$\begin{aligned}(a \pmod q \boxplus b \pmod q) \boxplus c \pmod q &= a + b \pmod q \boxplus c \pmod q \\ &= (a + b) + c \pmod q \\ &= a + (b + c) \pmod q = a \pmod q \boxplus (b + c) \pmod q \\ &= a \pmod q \boxplus (b \pmod q \boxplus c \pmod q)\end{aligned}$$

Donc l'operation $\boxplus$ est associative.

(b)

$$\begin{aligned}a \pmod q \boxplus 0 \pmod q &= a + 0 \pmod q = a \pmod q \\ &= 0 + a \pmod q = 0 \pmod q \boxplus a \pmod q.\end{aligned}$$

Donc $0 \pmod q$ est neutre pour $\boxplus$.

(c)

$$a \pmod q \boxplus \boxminus a \pmod q = a - a \pmod q = 0 \pmod q$$

et

$$\boxminus a \pmod q \boxplus a \pmod q = -a + a \pmod q = 0 \pmod q.$$

Donc $\boxminus a \pmod q$ est l'inverse de $a \pmod q$.

(d)

$$\begin{aligned}a \pmod q \boxplus b \pmod q &= a + b \pmod q \\ &= b + a \pmod q = b \pmod q \boxplus a \pmod q.\end{aligned}$$

Donc l'operation est commutatif.

5. On a pour $a, b \in \mathbb{Z}$ que :

$$\begin{aligned}\pi_q(a+b) &= (a+b) \,(\mathrm{mod}\, q) \\ &= a \,(\mathrm{mod}\, q) \boxplus b \,(\mathrm{mod}\, q) = \pi_q(a) \boxplus \pi_q(b).\end{aligned}$$

Donc π_q est un morphism des groupes.

Exercice 3. Soit $G = [0,1[$ et $\oplus : G \times G \mapsto \mathbb{R}$ la loi de composition definie par

$$x \oplus x' := \begin{cases} x + x' & \text{si } x + x' < 1 \\ x + x' - 1 & \text{si } x + x' \geqslant 1 \end{cases}.$$

Montrer que $\oplus$ est a valeurs dans G et trouver un element neutre $0_G \in G$ et une application inversion $\ominus : G \mapsto G$ telles que

$$(G, \oplus, 0_G, \ominus)$$

forme un groupe commutatif.

Solution 3. Il n'est pas difficile de voir que 0 est neutre pour l'addition. Il est aussi claire que l'operation est commutatif. Pour $x \in G$ on a que $1 - x \in G$ et que $1 - x$ est l'inverse, en fait $x + (1 - x) = 1$ et alors $x \oplus (1 - x) = 0$. Il ne reste plus qu'a montrer que l'operation est associative. Soient $x_1, x_2, x_3 \in G$, il y a trois possibilites

1. Si $x_1 + x_2,\ x_2 + x_3 < 1$, on a

$$x_1 \oplus x_2 = x_1 + x_2,\ x_2 \oplus x_3 = x_2 + x_2$$

et

$$(x_1 \oplus x_2) \oplus x_3 = (x_1 + x_2) \oplus x_3 = x_1 + x_2 + x_3 - \varepsilon$$

avec $\varepsilon = 0$ ou 1 suivant que $x_1 + x_2 + x_3$ est < 1 ou $\geqslant 1$ (on observe que comme $+$ est associative on n'a pas besoin de mettre de parantheses dans cette inegalite et que

$$\varepsilon = \varepsilon(x_1 + x_2 + x_3)$$

ne depend que de la somme des trois termes et pas de leurs valeurs individuelles). D'autre part

$$x_1 \oplus (x_2 + x_3) = x_1 + x_2 + x_3 - \varepsilon$$

avec le meme $\varepsilon = \varepsilon(x_1 + x_2 + x_3)$. Ainsi on a

$$(x_1 \oplus x_2) \oplus x_3 = x_1 \oplus (x_2 \oplus x_3). \tag{0.1}$$

2. Si $x_1 + x_2 < 1 \leqslant x_2 + x_3$, on a

$$x_1 \oplus x_2 = x_1 + x_2,\ x_2 \oplus x_3 = x_2 + x_3 - 1$$

et

$$(x_1 \oplus x_2) \oplus x_3 = (x_1 + x_2) \oplus x_3 = x_1 + x_2 + x_3 - \varepsilon$$

avec ε comme ci-dessus. On a egalement

$$x_1 \oplus (x_2 \oplus x_3) = x_1 \oplus (x_2 + x_3 - 1) = x_1 + x_2 + x_3 - \varepsilon.$$

On a donc (0.1). Par commutativite de $\oplus$ (et de $+$) cela traite aussi le cas $x_2 + x_3 < 1 \leqslant x_1 + x_2$

3. Si $1 \leqslant x_1 + x_2, x_2 + x_3$ alors

$$x_1 \oplus x_2 = x_1 + x_2 - 1 < 1,\ x_2 \oplus x_3 = x_2 + x_3 - 1 < 1$$

et

$$(x_1 \oplus x_2) \oplus x_3 = (x_1 + x_2 - 1) \oplus x_3 = x_1 + x_2 + x_3 - \varepsilon$$

alors que

$$x_1 \oplus (x_2 \oplus x_3) = x_1 \oplus (x_2 + x_3 - 1) = x_1 + x_2 + x_3 - \varepsilon$$

On a donc bien (0.1).

Remarque 0.1. (via les quotients) Posons la relation sur $\mathbb{R}$

$$x \sim_{\mathbb{Z}} x' \Longleftrightarrow x - x' \in \mathbb{Z}.$$

C'est une relation d'equivalence (car $\mathbb{Z}$ est un sous-groupe du groupe commutatif $\mathbb{R}$) dont les classes d'equivalence sont de la forme

$$x \,(\mathrm{mod}\, \mathbb{Z}) = x + \mathbb{Z}$$

pour $x \in \mathbb{Z}$.

L'espace quotient

$$\mathbb{R}/\mathbb{Z} = \{x \,(\mathrm{mod}\, \mathbb{Z}) = x + \mathbb{Z},\ x \in \mathbb{R}\}$$

admet alors une structure de groupe commutatif en posant (et c'est bien defini)

$$x \,(\mathrm{mod}\, \mathbb{Z}) +_{\mathbb{Z}} x' \,(\mathrm{mod}\, \mathbb{Z}) := x + x' \,(\mathrm{mod}\, \mathbb{Z})$$

dont l'element neutre est $0 \,(\mathrm{mod}\, \mathbb{Z}) = \mathbb{Z}$. Voir le resultat analogue pour les anneaux quotients.

Si $[x] \in \mathbb{Z}$ designe la partie entiere de x (le plus grand entier $\leqslant x$) alors

$$x - [x] \,(\mathrm{mod}\, \mathbb{Z}) = x \,(\mathrm{mod}\, \mathbb{Z})$$

et $x - [x] \in [0,1[$. On montre alors que l'application

$$x \in [0,1[\mapsto x \,(\mathrm{mod}\, \mathbb{Z})$$

est une bijection entre ensembles et que pour $x, x' \in [0,1[$ on a

$$x + x' - [x + x'] = x \oplus x'$$

Ainsi dans la bijection precedente $x \oplus x' \in [0,1[$ correspond a la classe $x + x' \,(\mathrm{mod}\, \mathbb{Z}) = x \,(\mathrm{mod}\, \mathbb{Z}) +_{\mathbb{Z}} x'$. Ains le fait que $\oplus$ definisse une lois de groupe provient de la loi de groupe sur le quotient $\mathbb{R}/\mathbb{Z}$.

1 Nouveaux exercices

Exercice 4 (Se reporter a la section 2.2.1 du cours)**.** Soit $n \geqslant 1$ un entier non-nul et

$$\mathfrak{S}_n = \mathrm{Bij}(\{1, 2, \cdots, n\})$$

le groupe des bijections de l'ensemble $\{1, 2, \cdots, n\}$ (ou groupe des permutations de $\{1, 2, \cdots, n\}$). C'est un groupe fini de $n! = 1.2. \cdots .n$ elements.

On peut representer une permutation par un tableau a deux lignes et n colonnes

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}.$$

Ainsi l'identite est ainsi codee par

$$\mathrm{Id}_X = \begin{pmatrix} 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \end{pmatrix},$$

alors que

$$c_n = \begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ 2 & 3 & \cdots & n & 1 \end{pmatrix}$$

est la permutation (dite cylique) qui envoie

$$1 \mapsto 2,\ 2 \mapsto 3, \cdots, n \mapsto n-1,\ n \mapsto 1$$

1. Representer tous les elements de $\mathfrak{S}_2$ et montrer que ce groupe est commutatif.
2. Representer ainsi tous les elements de $\mathfrak{S}_3$ et montrer que ce groupe n'est pas commutatif.

3. Pour $n = 4$, on considere

$$\theta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix},\ \tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}$$

les permutations qui envoient respectivement

$$\theta : 1 \mapsto 4,\ 2 \mapsto 1,\ 3 \mapsto 3,\ 4 \mapsto 2,\ \tau : 1 \mapsto 1,\ 2 \mapsto 4,\ 3 \mapsto 3,\ 4 \mapsto 2.$$

Calculer

$$\theta \circ \tau, \tau \circ \theta,\ \theta^2,\ \theta^3,\ \theta^n,\ \tau^n \text{ pour } n \in \mathbb{Z}.$$

4. On note

$$\mathfrak{S}_{4,3} = \{\sigma \in \mathfrak{S}_4,\ \sigma(3) = 3\}$$

l'ensemble des bijection qui envoie 3 sur 3 ; on appelle cet ensemble le stabilisateur de 3. Donner tous les elements de $\mathfrak{S}_{4,3}$. Montrer que $\mathfrak{S}_{4,3}$ est un sous-groupe de $\mathfrak{S}_4$. Est ce que ce groupe est engendre par θ et τ ?

Solution 4.

1. Avec la notation de l'exercise on a :

$$\mathfrak{S}_2 = \left\{ \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \right\}.$$

Nous avons montrer precedemment que tout les groupes avec deux elements sont commutatif.

2.

$$\mathfrak{S}_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \right\}.$$

3. $\theta \circ \tau(1) = \theta(1) = 4$, $\theta \circ \tau(2) = \theta(4) = 2$, $\theta \circ \tau(3) = \theta(3) = 3$. Alors on a que

$$\theta \circ \tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 3 & 1 \end{pmatrix}.$$

De meme, on obtient :

$$\tau \circ \theta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix},$$

$$\theta^2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix},$$

$$\theta^3 = \mathrm{Id}.$$

Pour $n \in \mathbb{Z}$ on a $n = 3k + r$ pour un $k \in \mathbb{Z}$ et un $0 \leqslant r < 3 \in \mathbb{Z}$. Alors

$$\theta^n = \theta^{3k} \circ \theta^r = \mathrm{Id} \circ \theta^r = \theta^r.$$

Similairement, $\tau^2 = \mathrm{Id}$, alors on a

$$\tau^n = \begin{cases} \mathrm{Id}, & \text{Si } n \text{ paire} \\ \tau, & \text{Si } n \text{ unpaire} \end{cases}$$

4. $\mathfrak{S}_{4,3}$ n'est pas vide, parceque $\theta \in \mathfrak{S}_{3,4}$. Pour $\sigma, \gamma \in \mathfrak{S}_{3,4}$ on a $\gamma^{-1}(3) = 3$ et alors $\sigma \circ \gamma^{-1}(3) = 3$. Donc $\mathfrak{S}_{4,3}$ est un sous-groupe. On a

$$\begin{aligned} \mathfrak{S}_{4,3} &= \left\{ \mathrm{Id}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} \right\} \\ &= \{\mathrm{Id}, \theta, \theta^2, \tau \circ \theta, \theta \circ \tau, \tau\}. \end{aligned}$$

On note donc que $\mathfrak{S}_{4,3} \subset < \theta, \tau >$. Parce-que $\theta \in \mathfrak{S}_{4,3}$ et $\tau \in \mathfrak{S}_{4,3}$ et $\mathfrak{S}_{4,3}$ c'est un sous-groupe on a d'autre parte que $< \theta, \tau > \subset \mathfrak{S}_{4,3}$ et donc le deux ensembles sont les memes.

Exercice 5. Soit le groupe $(\mathbb{Z}, +)$. On rappelle que tous les sous-groupes de $\mathbb{Z}$ sont de la forme $q.\mathbb{Z}$ pour $q \in \mathbb{Z}$.

1. Montrer que le groupe engendre par 2 et 3 vaut $\langle 2, 3 \rangle = \mathbb{Z}$. (on montrera que ce sous-groupe contient 1).
2. Meme question pour 3 et 73.
3. Montrer (en utilisant Bezout) que pour $m, n \in \mathbb{Z}$, le sous-groupe de $\mathbb{Z}$ engendre par m et n est
$$\langle m, n \rangle = pgcd(m, n).\mathbb{Z}.$$

Solution 5.
1. Comme $\langle 2, 3 \rangle$ est un sous-groupe, il contient $3 - 2 = 1$ et aussi tout multiple de 1, donc tout entier. Donc $\langle 2, 3 \rangle = \mathbb{Z}$.
2. En remarquant que $73 - 24 * 3 = 1$ on peut répéter l'argument précédent pour dire que $\langle 3, 73 \rangle = \mathbb{Z}$.
3. Concrètement, $\langle m, n \rangle = \{am + bn \mid a, b \in \mathbb{Z}\}$. Or par le théorème de Bézout, si $d = pgcd(m, n)$, alors l'équation $am + bn = d$ admet un couple solution (a, b) donc $pgcd(m, n) \in \langle m, n \rangle$ et $pgcd(m, n).\mathbb{Z} \subseteq \langle m, n \rangle$. Comme m et n sont multiples de d, on a également $\langle m, n \rangle \subseteq pgcd(m, n).\mathbb{Z}$ et donc $\langle m, n \rangle = pgcd(m, n).\mathbb{Z}$.

Exercice 6 $(\star)$**.** (Groupes produit) Soient $(G, \star)$ et $(H, *)$ deux groupes. On considere le produit cartesien $G \times H$ muni de la loi de composition interne :

$$(g, h) \boxtimes (g', h') := (g \star g', h * h').$$

1. Trouver un element neutre $e_{G \times H}$ et une inversion $(\bullet, \bullet)^{-1}$ de sorte que
$$(G \times H, \boxtimes, e_{G \times H}, (\bullet, \bullet)^{-1})$$
forme un groupe.

2. On suppose dans cette question que $G = H$. Montrer que la diagonale $\Delta G = \{(g, g),\ g \in G\}$ est un sous-groupe de $G \times G$.
3. Soient $G' \subset G$ et $H' \subset H$ des sous-groupes. Montrer que $G' \times H'$ est un sous-groupe de $G \times H$.
4. Est ce que la reciproque est vraie ? C'est a dire est ce que tout sous-groupe de $G \times H$ est de la forme $G' \times H'$?
5. On considere les applications (de projection)

$$\pi_G : \begin{array}{ccc} G \times H & \mapsto & G \\ (g,h) & \mapsto & g \end{array}, \ \pi_H : \begin{array}{ccc} G \times H & \mapsto & H \\ (g,h) & \mapsto & h \end{array}.$$

   Est ce que ce sont des morphismes de groupes ?
6. On suppose que $G = H$. est ce que l'application

$$\star : \begin{array}{ccc} G \times G & \mapsto & G \\ (g,g') & \mapsto & g \star g' \end{array}$$

   est un morphisme de groupes en general ? Sinon donner une condition suffisante pour que cela en soit un.

Solution 6. 1. Le neutre est donne par $e_{G\times H} = (e_G, e_H)$. En effet, comme la loi $\boxtimes$ de $G \times H$ revient a utiliser sur chaque element du couple la loi deson groupe, on a

$$(g,h) \boxtimes (e_G, e_H) = (g \star e_G, h * e_H) = (g,h) = (e_G \star g, e_H * h) = (e_G, e_H) \boxtimes (g,h),$$

pour tout les $(g,h) \in G \times H$.
L'inverse de (g,h) est donne par (g^{-1}, h^{-1}), en fait on a

$$(g,h) \boxtimes (g^{-1}, h^{-1}) = (g \star g^{-1}, h * h^{-1}) = (e_G, e_H)$$

et

$$(g^{-1}, h^{-1}) \boxtimes (g,h) = (g^{-1} \star g, h^{-1} * h) = (e_G, e_H).$$

L'associativite de l'application $\boxtimes$ est un consequence de l'associativite de les applications $\star$ et $*$ dans G et H respectivement.

2. On a que $(e_G, e_G) \in \Delta_G$, i.e. Δ_G n'est pas vide. Soient $x, y \in \Delta_G$. Alors il y a $g, h \in G$ t.q. $x = (g,g)$ et $y = (h,h)$. On a

$$x \otimes y^{-1} = (g,g) \otimes (h^{-1}, h^{-1}) = (g \star h^{-1}, g \star h^{-1}) \in \Delta_G.$$

Donc Δ_G est un sous-groupe de $G \times G$.

3. $e_G \in G'$ et $e_H \in H'$, parce-que ils sont sous-groupes de G et H respectivement. Alors $(e_G, e_H) \in G' \times H'$. Soient $(g_1, h_1), (g_2, h_2) \in G' \times H'$, on a

$$(g_1, h_1) \boxtimes (g_2, h_2)^{-1} = (g_1 \star g_2^{-1}, h_1 * h_2^{-1}) \in G' \times H',$$

parce-que $g_1 g_2^{-1} \in G'$ et $h_1 h_2^{-1} \in H'$ comme G' et H' sont sous-groupes de G et H respectivement.

4. Si $|G| \geqslant 2$, alors c'est faux, plus precisement dans ce cas Δ_G n'est jamais le produit de deux sous-groupes de G.

5. Oui, les deux sont des morphismes de groupes. Nous le montrons seulment pour π_G, l'autre cas est analogue. On a que

$$\pi_G((g_1, h_1) \boxtimes (g_2, h_2)) = \pi_G((g_1 \star g_2, h_1 * h_2) = g_1 \star g_2 = \pi_G(g_1, h_1) \star \pi_G(g_2, h_2).$$

6. Soient (g_1, g_1') et $(g_2, g_2'$ deux elements de $G \times G$. On a

$$\star((g_1, g_1'), (g_2, g_2')) = \star(g_1 \star g_2, g_1' \star g_2') = (g_1 \star g_2) \star (g_1' \star g_2').$$

D'autre part on a

$$(\star(g_1, g_1')) \star (\star(g_2, g_2')) = (g_1 \star g_1') \star (g_2 \star g_2').$$

Si G est commutatif, on voit que $\star$ definit un morphisme de groupes, ceci n'est pas seulment un condition sufficient, mais aussi necessaire. En effet, si on fixe $g_1 = e_G$ et $g_2' = e_G$, on note que si $\star$ est un morphisme de groupes alors $g_1' \star g_2 = g_2 \star g_1'$ pour tous les $g_1', g_2 \in G$.

Exercice 7. Soit le groupe produit $(\mathbb{Z}^2, +)$ forme des paires d'entiers et equipe de l'addition provenant de $(\mathbb{Z}, +)$:

$$\mathbb{Z}^2 = \mathbb{Z} \times \mathbb{Z} = \{(x, y),\ x, y \in \mathbb{Z}\}$$

$$(x, y) + (x', y') = (x + x', y + y').$$

(comme la notation le suggere on utilisera -sauf pour la deuxieme question et preuve du Lemme ci-dessous- ici la notation additive/multiple : en particulier on notera pour $n \geqslant 1$ un entier

$$n.(x, y) = (n.x, n.y) = (x, y) + (x, y) + \cdots + (x, y)\ n \text{ fois.})$$

1. Montrer que le groupe $\mathbb{Z}^2$ est engendre par les elements $(1, 0)$ et $(0, 1)$:

$$\langle \{(1, 0), (0, 1)\} \rangle = \mathbb{Z}^2.$$

2. Soit $(H, \star)$ un autre groupe (note multiplicativement) et $\varphi : \mathbb{Z}^2 \mapsto H$ un morphisme de groupes. Montrer que pour tout $x, y \in \mathbb{Z}$ on a

$$\varphi((x, y)) = h_1^x \star h_2^y$$

avec $h_1 = \varphi((1, 0)),\ h_2 = \varphi((0, 1))$.

3. Soient $(a, b), (c, d) \in \mathbb{Z}^2$ deux paires d'entiers tels que

$$ad - bc = \pm 1.$$

Montrer que ces deux elements engendrent $\mathbb{Z}^2$:

$$\mathbb{Z}^2 = \langle \{(a, b), (c, d)\} \rangle.$$

On pourra commencer par remarquer que

$$\langle \{(a, b), (c, d)\} \rangle = \{m.(a, b) + n.(c.d),\ m, n \in \mathbb{Z}\} =: \mathbb{Z}.(a, b) + \mathbb{Z}(c, d),$$

montrer que

$$(1, 0), (0, 1) \in \langle \{(a, b), (c, d)\} \rangle$$

et utiliser le Lemme suivant (qu'on demontrera) :

Lemme 1. *Soit $(G, *)$ un groupe et $A \subset G$ un sous-ensemble. On suppose que $\langle A \rangle = G$ (ie. le groupe G est engendre par A). Soit $B \subset G$ un autre sous-ensemble. On a alors*

$$A \subset \langle B \rangle \Longrightarrow G = \langle B \rangle$$

(si le sous-groupe engendre par B contient A alors c'est G tout entier).

Démonstration. Il faut se rappeler que pour un sous-ensemble $S \subset G$ on a

$$\langle S \rangle = \bigcap_{\substack{S \subset H \\ H \text{ sous-group de } G}} H.$$

Dans le notre cas on a que $\langle B \rangle$ est un sous-groupe de G, qui contient A, et alors $\langle A \rangle \subset \langle B \rangle$. On a

$$G = \langle A \rangle \subset \langle B \rangle \subset G,$$

donc $\langle B \rangle = G$.

□

Solution 7. Etendre la notation de l'exercice aux cas suivants : si $n = 0$ on pose $n.(x, y) = (0, 0)$, si $n < 0$ on pose $n.(x, y) = (-n).(-x, -y)) = (-x, -y) + \cdots + (-x, -y)$ pour $|n|$-fois.

1. Avec la notation de l'exercise on a :

$$(n, m) = n.(1, 0) + m.(0, 1).$$

Dans tous les cas, c'est un element de $\langle\{(1, 0), (0, 1)\}\rangle$. Et alors $\mathbb{Z}^2 = \langle\{(1, 0), (0, 1)\}\rangle$.

2. Pour $x = 0 = y$ on a, comme φ est un morphisme des groupes, que $\varphi((0, 0)) = 1 = h_1^0 h_2^0$. Par induction on peut montrer que pour des entiers positifs x, y on a $\varphi(x.(1, 0)) = \varphi((1, 0))^x = h_1^x$ et $\varphi(y.(0, 1)) = h_2^y$. Pour un entier *negatif* x (resp. y), comme $x.(1, 0)$ (resp. $y.(0, 1)$) est l'inverse de $(-x, 0)$ (resp. $((0, -y))$ on a $\varphi(x.(1, 0)) = \varphi(-x, 0))^{-1} = (h_1^{-x})^{-1} = h_1^x$ (resp. $\varphi(y.(0, 1)) = h_2^y$). En conclusion

$$\varphi(x, y) = \varphi(x.(1, 0) + y.(0, 1)) = \varphi(x.(1, 0)) \star \varphi(y.(0, 1)) = h_1^x \star h_2^y.$$

3. On veut montrer que $(1, 0)$ et $(0, 1)$ sont contenus dans $\mathbb{Z}.(a, b) + \mathbb{Z}.(c, d)$, i.e. on doit trouver $n_1, m_1, n_2, m_2 \in \mathbb{Z}$ t.q.

$$m_1(a, b) + n_1(c, d) = (1, 0),\ m_2(a, b) + n_2(c, d) = (0, 1).$$

Si $ad - bc = 1$ on a que $m_1 = d, n_1 = -b$ et $m_2 = -c, n_2 = a$ est une solutione. Si $ad - bc = -1$ en peut choisir $m_1 = -d, n_1 = b$ et $m_2 = c, n_2 = -a$. Dans tous le cas on a que $(1, 0), (0, 1) \in \langle\{(a, b), (c, d)\}\rangle$. Nous pouvons maintenant utiliser le lemme et la point (1) pour conclure l'exercice.

Exercice 8 (Groupes de fonctions)**.** Soit X un ensemble et $(G, \star)$ un groupe. Soit

$$\mathcal{F}(X, G) = \{f : X \mapsto G\}$$

l'ensemble des fonctions de X a valeurs dans G (les applications de X vers G).

On muni $\mathcal{F}(X, G)$ de la loi de composition interne suivante : etant donne $f_1, f_2 \in \mathcal{F}(X, G)$ on defini la fonction $f_1 \star f_2$ par

$$\forall x \in X,\ f_1 \star f_2(x) := f_1(x) \star f_2(x).$$

(ici on abuse les notations en notant la loi de composition sur $\mathcal{F}(X, G)$ de la meme maniere que celle sur G).

1. Trouver un element neutre $e_{\mathcal{F}(X,G)}$ et une inversion $\bullet^{-1}$ de sorte que $(\mathcal{F}(X, G), \star, e_{\mathcal{F}(X,G)}, \bullet^{-1})$ forme un groupe.
2. Soit $U \subset G$ un sous-ensemble de G. Donner une condition necessaire et suffisante pour que le sous-ensemble des fonctions a valeurs dans U

$$\mathcal{F}(X, U) \subset \mathcal{F}(X, G)$$

forme un sous-groupe de $\mathcal{F}(X, G)$.

Solution 8. L'idee sera vraiment tout au long de l'exercice de puiser autant de choses que possibles dans la structure de groupe de G pour en deduire des choses sur celle de $\mathcal{F}(X,G)$.

1. On pose le neutre
$$e_{\mathcal{F}(X,G)}\colon X \to G,\ x \mapsto e_G$$
et pour $f \in \mathcal{F}(X,G)$,
$$f^{-1}\colon X \to G,\ x \mapsto (f(x))^{-1}.$$
En effet, $\forall f \in \mathcal{F}(X,G), \forall x \in X$:
   - $f \star e_{\mathcal{F}(X,G)}(x) = f(x) \star e_{\mathcal{F}(X,G)}(x) = f(x) \star e_G = f(x)$, et donc $e_{\mathcal{F}(X,G)}$ est neutre a droite. On montre la neutralite a gauche de la meme maniere.
   - $f \star f^{-1}(x) = f(x) \star (f(x))^{-1} = e_G = e_{\mathcal{F}(X,G)}(x)$, et donc f^{-1} est bien l'inverse de f

   On peut se convaincre facilement que l'associativite de la loi de $\mathcal{F}(X,G)$ decoule de celle de la loi de G par un argument similaire.

   Remarque. : On a fait ici un petit abus de notations en ecrivant f^{-1} sans avoir encore verifie que c'etait bien l'inverse (mais on s'en remettra). Notez cependant que f^{-1} ne designe pas la reciproque de f (au sens reciproque d'une bijection).

2. On veut montrer que U est un sous-groupe de G si et seulment si $\mathcal{F}(X,U)$ est un sous-groupe de $\mathcal{F}(X,G)$.
   - ($\Rightarrow$) : Soit U un sous-groupe de G on vas montrer que $\mathcal{F}(X,U)$ est un sous-groupe de $\mathcal{F}(X,G)$. On a $e_G \in U$, alors la fonction $e_{\mathcal{F}(X,G)}$ a valeurs dans U, i.e. $e_{\mathcal{F}(X,G)} \in \mathcal{F}(X,U)$. Si $f_1, f_2 \in \mathcal{F}(X,U)$, alors on a que $\forall x\colon f_1(x), f_2(x) \in U$. Donc $f_1(x) \star f_2^{-1}(x) = f_1(x) \star (f_2(x))^{-1} \in U$ pour tous les $x \in X$. Donc $f_1 \star f_2^{-1} \in \mathcal{F}(X,U)$.
   - ($\Leftarrow$) : Soit $\mathcal{F}(X,U) \subset \mathcal{F}(X,G)$ un sous-groupe. On vas montrer que $U \subset G$ est un sous-groupe. La fonction $e_{\mathcal{F}(X,G)}$ est dans $\mathcal{F}(X,U)$, i.e. elle a valeurs dans U, i.e. $e_G \in U$. Soient $g_1, g_2 \in U$. On considere les fonctions constantes $f_i\colon X \to G;\ x \mapsto g_i$, $i = 1,2$. On a $f_1, f_2 \in \mathcal{F}(X,U)$, et alors $f_2^{-1} \in \mathcal{F}(X,U)$. Donc
$$g_1 \star g_2^{-1} = f_1(x) \star f_2(x)^{-1} = f_1 \star f_2^{-1}(x) \in U.$$