Sorbonne Université, Algèbre 2, année 2025-2026

Corrigé de la feuille de TD numéro 1

Exercice 1.

- 1 n'a pas d'inverse.
- $(\mathrm{M}_2(\mathbb{R}), \times)$ n'est pas un groupe car il existe des matrices non inversibles, mais $(\mathrm{GL}_2(\mathbb{R}), \times)$ est bien un groupe.
- $(\mathrm{M}_2(\mathbb{R}), +)$ est bien un groupe, mais pas $(\mathrm{GL}_2(\mathbb{R}), +)$ car une somme de matrices inversibles n'est pas toujours inversible (par exemple, $A + (-A)$ n'est pas inversible).

Exercice 2.

(1) On vérifie sans peine que $x * (y * z) = (x * y) * z$ pour tous $x, y, z \in I$, donc la loi est bien associative. Pour tout $x \in I$, on a $x * 0 = 0 * x = x$, donc $*$ admet 0 comme élément neutre. Enfin, on vérifie que pour tout $x \in I$, le réel $y = -x/(1+x)$ (qui appartient bien à I) vérifie $x * y = y * x = 0$.

(2) Soient $x, y \in I$. On a $f(x) * f(y) = (e^x - 1)(e^y - 1) + e^x - 1 + e^y - 1 = e^x e^y - 1 = e^{x+y} - 1 = f(x + y)$, donc f est bien un morphisme de groupes. Si $f(x) = 0$ alors $x = 0$, donc f est injectif. Enfin, pour tout élément $y \in I$, on peut écrire $y = f(\ln(y + 1))$ (le logarithme est bien défini puisque $y + 1 > 0$), donc f est surjectif. Ainsi, f est bien un isomorphisme de groupes.

Exercice 3. Supposons qu'il existe un isomorphisme $\varphi : \mathbb{Q} \to \mathbb{Q}^*$. Soit $x \in \mathbb{Q}$ tel que $\varphi(x) = 2$, et posons $y = x/2$. Alors $2 = \varphi(y + y) = \varphi(y)\varphi(y) = \varphi(y)^2$, or 2 n'a pas de racine carrée rationnelle, contradiction (notons qu'il suffisait de supposer que φ était surjectif).

Exercice 4.

(1) L'ensemble $\{-1, 1\}$ est un sous-groupe de $(\mathbb{Q}^*, \times)$ (contient le neutre 1 et stable par produit et inversion), mais pas un sous-groupe de $(\mathbb{Q}, +)$ puisqu'il ne contient pas le neutre 0.

(2) On vérifie que H contient le neutre 1 et qu'il est stable par produit et inversion.

Exercice 5. La formule bien connue $\exp(x + y) = \exp(x)\exp(y)$ montre qu'il s'agit d'un morphisme de groupes de $(\mathbb{C}, +)$ vers $(\mathbb{C}^*, \times)$. Tout élément z de $\mathbb{C}^*$ s'écrit sous la forme $re^{i\theta}$ avec $r > 0$. On peut écrire $r = e^u$ avec $u \in \mathbb{R}$, donc $z = e^u e^{i\theta} = e^{u+i\theta}$. Ainsi, exp est un morphisme surjectif. Son noyau est l'ensemble des $z = 2i\pi n$ pour $n \in \mathbb{Z}$.

Exercice 6.

On a $(gh)^2 = e$, donc $gh = (gh)^{-1} = h^{-1}g^{-1} = hg$.

Exercice 7.

Soit $y \in E$. Il existe $x \in E$ tel que $x * y = e$. Il existe aussi $z \in E$ tel que $z * x = e$, donc $z * (x * y) = z * e = z = (z * x) * y = e * y = y$. Ainsi $z = y$, donc x est aussi l'inverse à droite de y. Conclusion : $(E, *)$ est un groupe.

Exercice 8.

On peut prendre par exemple pour E l'ensemble des fonctions de $\mathbb{N}$ dans lui-même muni de la composition, avec pour élément neutre la fonction identité notée e, $y : n \mapsto n+1$ et $x : n \mapsto n-1$ si $n \geq 1$ et $x(0) = 0$. On vérifie que $x \circ y(n) = n$ pour tout $n \in \mathbb{N}$, donc $x \circ y = e$. Ainsi, x est inversible à droite et y est inversible à gauche. D'autre part, y n'étant pas surjective, elle ne possède pas d'inverse à droite, et x n'étant pas injective, elle ne possède pas d'inverse à gauche.

Exercice 9. Soit $(G, *)$ un groupe, soit H un sous-ensemble de G.

(1) Soit $h \in H$. L'application $n \in \mathbb{N} \mapsto h^n$ n'est pas injective puisque H est fini, donc il existe $n \neq m$ tels que $h^n = h^m$. On a donc, en posant $k = n - m - 1$: $h^{n-m} = e = hh^k = h^k h$. Ainsi, h est inversible d'inverse h^k.

(2) On peut prendre, par exemple, $G = \mathbb{Z}$ et $H = \mathbb{N}$.

Exercice 10. Si H est contenu dans K ou K est contenu dans H alors $H \cup K$ est évidemment un sous-groupe de G car il est égal à H ou K. Réciproquement, supposons que $H \cup K$ est un sous-groupe et que H n'est pas contenu dans K. Il existe alors un élément $h \in H$ qui n'est pas dans K. Pour tout $k \in K$, le produit hk appartient à $H \cup K$. On distingue deux cas : soit hk appartient à H, auquel cas k appartient à H, soit hk appartient à K, auquel cas h appartient à K, ce qui contredit notre hypothèse. Donc K est contenu dans H.

Exercice 11.

(1) On vérifie les trois axiomes de la définition d'un sous-groupe : H contient le neutre (qui est d'ordre 1), H est stable par inversion car $(h^{-1})^n = (h^n)^{-1}$, et H est stable par produit car, G étant commutatif, $(hh')^n = h^n h'^n$.

(2) La stabilité par produit de l'ensemble H n'est pas assurée en général ; on vérifie en effet que $A^4 = I_2$ et que $B^6 = I_2$ tandis que AB est d'ordre infini car

$$AB = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \quad \text{et} \quad (AB)^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}.$$

Exercice 12.

(1) L'ensemble des parties de G est fini si G est fini, donc l'ensemble des sous-groupes de G est fini.

(2) On distingue deux cas.
Premier cas : si G possède un élément d'ordre infini g, alors les sous-groupes $\langle g^n \rangle$ pour $n \in \mathbb{N}$ sont distincts deux à deux, donc G a une infinité de sous-groupes.
Second cas : supposons maintenant que G ne possède que des éléments d'ordre fini. Par l'absurde, si G n'avait qu'un nombre fini de sous-groupes, il existerait un nombre fini d'éléments $g_1, \ldots, g_n \in G$ tels que $G = \cup_{1 \leq i \leq n} \langle g_i \rangle$. Or, une réunion finie d'ensembles finis est un ensemble fini, ce qui contredit l'infinitude de G.

Exercice 13.

(1) On vérifie les trois axiomes : réflexivité, symétrie, transitivité.

(2) On a donc une partition $G = g_1 H \cup \cdots \cup g_n H$, d'où $|G| = n|H|$.

Exercice 14.

(1) Soit G un sous-groupe fini de $\mathbb{C}^*$ de cardinal n. Pour tout $g \in G$, on a $g^n = 1$ en vertu de l'exercice 13, donc G est contenu dans l'ensemble $\mathrm{Rac}(P)$ des racines dans $\mathbb{C}$ du polynôme $P(X) = X^n - 1$. Or $\mathrm{Rac}(P)$ est de cardinal au plus n (en fait, exactement n), donc $G = \mathrm{Rac}(P)$. Enfin, $\mathrm{Rac}(P)$ est précisément l'ensemble $\mathbb{U}_n$ des racines $n$ièmes de l'unité.

(2) L'ensemble $\{z \in \mathbb{C}^* \mid \exists n \geq 1,\ z^n = 1\}$ est un sous-groupe de $\mathbb{C}^*$ dont tous les éléments sont d'ordre fini.

Exercice 15. Tout élément non trivial de $(\mathbb{C}, +)$ est d'ordre infini, donc le seul morphisme de groupes de $(\mathbb{Z}/n\mathbb{Z}, +)$ vers $(\mathbb{C}, +)$ est le morphisme trivial, et il n'existe donc pas de morphisme injectif dès que n est au moins égal à 2. Soit maintenant un morphisme injectif φ de $(\mathbb{Z}/n\mathbb{Z}, +)$ vers $(\mathbb{C}^*, \times)$. Son image est un sous-groupe de $\mathbb{C}^*$ d'ordre n, donc coïncide avec $\mathbb{U}_n$. Comme $\mathbb{U}_n$ est isomorphe à $\mathbb{Z}/n\mathbb{Z}$, la question revient à décrire les automorphismes de $(\mathbb{Z}/n\mathbb{Z}, +)$: ce sont les endomorphismes qui envoient $\bar{1}$ sur $\bar{k}$ avec $1 \leq k \leq n$ tel que $\mathrm{PGCD}(k, n) = 1$. Les morphismes cherchés sont donc de la forme $\varphi : \bar{1} \mapsto e^{2ik\pi/n}$ avec $1 \leq k \leq n$ tel que $\mathrm{PGCD}(k, n) = 1$.

Exercice 16. Soit $h \in G$ tel que $\varphi(h) \neq 1$ (qui existe par hypothèse). Alors $\sum_{g \in G} \varphi(gh) = \sum_{g \in G} \varphi(g)$ (renumérotation des éléments). D'autre part, $\sum_{g \in G} \varphi(gh) = \varphi(h) \sum_{g \in G} \varphi(g)$, donc $\varphi(h) \sum_{g \in G} \varphi(g) = \sum_{g \in G} \varphi(g)$, d'où $\sum_{g \in G} \varphi(g) = 0$ puisque $\varphi(h) \neq 1$.