Exercices 12 – Groupes, Anneaux et Corps – Corrigé

Groupes

Exercice 1. — Montrer que $(\mathbb{R}_+^*, \times)$ est un groupe. Peut-on remplacer $\mathbb{R}_+^*$ par $\mathbb{R}_-^*$?

- ➢ La multiplication est une **LCI sur** $\mathbb{R}_+^*$ (le produit de deux réels strictement positifs est un réel strictement positif).
- ➢ La multiplication est **associative**.
- ➢ Il existe un **élément neutre** pour la multiplication : $1 \in \mathbb{R}_+^*$.
- ➢ Tout réel strictement positif x admet **un inverse dans** $\mathbb{R}_+^*$ pour la multiplication : $\frac{1}{x} \in \mathbb{R}_+^*$ et $x \times \frac{1}{x} = 1 = \frac{1}{x} \times x$.

Conclusion. $(\mathbb{R}_+^*, \times)$ est un groupe.

En revanche, la multiplication n'est pas une LCI dans $(\mathbb{R}_-^*, \times)$, puisque par exemple : $(-2)\times(-3) = 6 \notin \mathbb{R}_-^*$. On ne peut donc pas remplacer $\mathbb{R}_+^*$ par $\mathbb{R}_-^*$ dans ce qui précède.

Exercice 2. — Montrer que $(\mathbb{R}^{\mathbb{R}}, +)$ est un groupe. A-t-on toujours un groupe si on remplace la loi "$+$" par la loi "$\circ$" (composition) ?

- ➢ L'addition est une **LCI sur** $\mathbb{R}^{\mathbb{R}}$ (la somme de deux fonctions à valeurs réelles est encore une fonction à valeurs réelles).
- ➢ L'addition dans $\mathbb{R}^{\mathbb{R}}$ est **associative**.
- ➢ Il existe un **élément neutre** pour l'addition dans $\mathbb{R}^{\mathbb{R}}$: la fonction constante égale à 0, notée $0_{\mathbb{R}^{\mathbb{R}}}$.
- ➢ Toute fonction $f \in \mathbb{R}^{\mathbb{R}}$ admet **un inverse dans** $\mathbb{R}^{\mathbb{R}}$ pour l'addition, qui est son opposée, la fonction $(-f)$: $(-f) \in \mathbb{R}^{\mathbb{R}}$ et $f + (-f) = 0_{\mathbb{R}^{\mathbb{R}}} = (-f) + f$.

Conclusion. $(\mathbb{R}^{\mathbb{R}}, +)$ est un groupe.

Considérons à présent le même ensemble $(\mathbb{R}^{\mathbb{R}})$, en le munissant cette fois la loi "o" au lieu de la loi "$+$". On peut alors affimer que :

- ➢ La composition est une **LCI sur** $\mathbb{R}^{\mathbb{R}}$ (si f et g sont dans $\mathbb{R}^{\mathbb{R}}$, alors $f \circ g \in \mathbb{R}^{\mathbb{R}}$).
- ➢ La composition dans $\mathbb{R}^{\mathbb{R}}$ est **associative** (car plus généralement la composition des applications est associative).
- ➢ Il existe un **élément neutre** pour la composition dans $\mathbb{R}^{\mathbb{R}}$: la fonction $\mathrm{id}_{\mathbb{R}}$ (définie par : $\forall x \in \mathbb{R},\ \mathrm{id}_{\mathbb{R}}(x) = x$).

MAIS toute fonction $f \in \mathbb{R}^{\mathbb{R}}$ n'admet pas nécessairement un inverse dans $\mathbb{R}^{\mathbb{R}}$; en effet, f est inversible dans $\mathbb{R}^{\mathbb{R}}$ SSI f est bijective.

Conclusion. $(\mathbb{R}^{\mathbb{R}}, \circ)$ n'est pas un groupe.

Remarque. Notons Bij($\mathbb{R}$) l'ensemble des fonctions bijectives de $\mathbb{R}$ dans $\mathbb{R}$.[1] Il résulte de ce qui précède que $(\text{Bij}(\mathbb{R}), \circ)$ est un groupe, plus tard appelée **groupe des permutations de** $\mathbb{R}$.

Exercice 3. — On note $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$, et $\mathbb{K}_n[X]$ l'ensemble des polynômes à coefficients dans $\mathbb{K}$ de degré inférieur ou égal à n (n entier naturel). Vérifier que $(\mathbb{K}_n[X], +)$ est un groupe abélien. L'ensemble des polynômes à coefficients dans $\mathbb{K}$ de degré exactement n est-il un groupe ?

- ➢ L'addition est une **LCI sur** $\mathbb{K}_n[X]$ (la somme de deux polynômes de degré $\leqslant n$ est un polynôme de degré $\leqslant n$.
- ➢ L'addition dans $\mathbb{K}_n[X]$ est **associative**.
- ➢ Il existe un **élément neutre** pour l'addition dans $\mathbb{K}_n[X]$: le polynôme nul, notée $0_{\mathbb{K}_n[X]}$.
- ➢ Tout polynôme $P \in \mathbb{K}_n[X]$ admet **un inverse dans** $\mathbb{K}_n[X]$ pour l'addition, qui est son opposé, le polynôme $(-P)$: $(-P) \in \mathbb{K}_n[X]$ et $P + (-P) = 0_{\mathbb{K}_n[X]} = (-P) + P$.

Conclusion. $(\mathbb{K}_n[X], +)$ est un groupe. De plus, ce groupe est abélien car l'addition dans $\mathbb{K}_n[X]$ est commutative : $\forall\, (P, Q) \in (\mathbb{K}_n[X])^2, \quad P + Q = Q + P$.

En revanche, la somme de deux polynômes de degré exactement n n'est pas nécessairement de degré n. Par exemple, les polynômes $P = X^2 + 1$ et $Q = X - X^2$ sont de degré 2, mais $P + Q = X + 1$ n'est pas de degré 2. En d'autres termes, l'addition n'est pas une LCI dans l'ensemble des polynômes à coefficients dans $\mathbb{K}$ de degré exactement n.

Conclusion. L'ensemble des polynômes à coefficients dans $\mathbb{K}$ de degré exactement n n'est pas un groupe.

Exercice 4. — On note $\mathbb{D}$ l'ensemble des nombres décimaux : $\mathbb{D} = \left\{ \dfrac{n}{10^k} \;\middle|\; n \in \mathbb{Z},\ k \in \mathbb{N} \right\}$. Montrer que $(\mathbb{D}, +)$ est un sous-groupe de $(\mathbb{R}, +)$.

On vérifie les 4 axiomes permettant d'affirmer que $(\mathbb{D}, +)$ est un sous-groupe de $(\mathbb{R}, +)$.

- ➢ **(SG1)**. $\mathbb{D} \subset \mathbb{R}$ (trivial).
- ➢ **(SG2)**. $0 \in \mathbb{D}$ (l'élément neutre pour l'addition appartient à $\mathbb{D}$).
- ➢ **(SG3)**. La somme de deux décimaux est encore un décimal (vérification aisée). L'addition est donc une LCI sur $\mathbb{D}$.
- ➢ **(SG4)**. Tout décimal x admet un inverse pour l'addition, qui est son opposé $(-x)$, et $(-x)$ est encore un décimal.

Conclusion. $(\mathbb{D}, +)$ est un sous-groupe de $(\mathbb{R}, +)$.

1. Une fonction bijective de $\mathbb{R}$ dans $\mathbb{R}$ est appelée une **permutation** de $\mathbb{R}$.

Exercice 5. — Montrer que $(\mathbb{U}, \times)$ est un sous-groupe de $(\mathbb{C}^*, \times)$.

On vérifie les 4 axiomes permettant d'affirmer que $(\mathbb{U}, \times)$ est un sous-groupe de $(\mathbb{C}^*, \times)$.

➢ **(SG1)**. $\mathbb{U} \subset \mathbb{C}^*$ car tout nombre complexe de module 1 est en particulier non nul.

➢ **(SG2)**. $1 \in \mathbb{U}$ (l'élément neutre pour la multiplication appartient à $\mathbb{U}$).

➢ **(SG3)**. Le produit de deux éléments de $\mathbb{U}$ (deux complexes de module 1) est encore un élément de $\mathbb{U}$ (propriété immédiate, déjà vue dans le chapitre sur les complexes). La multiplication est donc une LCI sur $\mathbb{U}$.

➢ **(SG4)**. Tout élément de $\mathbb{U}$ (tout complexe de module 1) z admet un inverse pour la multiplication, qui est $1/z$; et $1/z$ est encore un élément de $\mathbb{U}$ (déjà vu dans le chapitre sur les complexes).

Conclusion. $(\mathbb{U}, \times)$ est un sous-groupe de $(\mathbb{C}^*, \times)$.

Exercice 6. — Soit n un entier naturel non-nul. Montrer que $(\mathbb{U}_n, \times)$ est un sous-groupe de $(\mathbb{U}, \times)$.

On vérifie les 4 axiomes permettant d'affirmer que $(\mathbb{U}_n, \times)$ est un sous-groupe de $(\mathbb{U}, \times)$.

➢ **(SG1)**. $\mathbb{U}_n \subset \mathbb{U}$ car toute racine n-ème de l'unité est de module 1 (propriété vus dans le chapitre sur les complexes).

➢ **(SG2)**. $1 \in \mathbb{U}_n$ car $1^n = 1 \ldots$ (l'élément neutre pour la multiplication appartient à $\mathbb{U}_n$).

➢ **(SG3)**. Le produit de deux éléments de $\mathbb{U}_n$ (deux racines n-èmes de l'unité) est encore un élément de $\mathbb{U}_n$ (propriété vue dans le chapitre sur les complexes). La multiplication est donc une LCI sur $\mathbb{U}_n$.

➢ **(SG4)**. Tout élément de $\mathbb{U}_n$ (toute racine n-ème de l'unité) z admet un inverse pour la multiplication, qui est $1/z$; et $1/z$ est encore un élément de $\mathbb{U}_n$ (déjà vu dans le chapitre sur les complexes).

Conclusion. $(\mathbb{U}_n, \times)$ est un sous-groupe de $(\mathbb{U}, \times)$.

Exercice 7. — Soit E un ensemble. L'ensemble $\mathscr{P}(E)$ est-il un groupe muni de la lci $\cup$? De la lci $\cap$?

Dans $\mathscr{P}(E)$, la loi $\cup$ est une LCI associative (et commutative), admettant un élément neutre (l'ensemble vide $\emptyset$).

On distingue alors deux cas, suivant que E est l'ensemble vide ou non.

➢ **Premier cas -** $E \neq \emptyset$. Alors E contient au moins un élément, que nous noterons x. Cette observation faite, le singleton $\{x\}$ est un élément de $\mathscr{P}(E)$, qui n'admet pas d'inverse pour la loi $\cup$. En effet, pour toute partie A de E, on a : $\{x\} \cup A \neq \emptyset$.

Puisqu'il existe dans $\mathscr{P}(E)$ un élément non inversible pour la loi $\cup$, on peut conclure : l'ensemble $\mathscr{P}(E)$ n'est pas un groupe muni de la lci $\cup$.

➢ **Second cas -** $E = \emptyset$. Dans ce cas, $\mathscr{P}(E)$ ne contient qu'un élément : $\mathscr{P}(E) = \{\emptyset\}$. Cet élément étant inversible pour l'union (puisque $\emptyset \cup \emptyset = \emptyset \ldots$), on peut conclure : l'ensemble $\mathscr{P}(\emptyset)$ est un groupe muni de la lci $\cup$.

➢ Des raisonnements analogues permettent d'affirmer que $(\mathscr{P}(E), \cap)$ n'est pas un groupe si $E \neq \emptyset$, et est un groupe lorsque $E = \emptyset$.

Exercice 8. — Décrire tous les groupes possibles possédant 1, 2, 3 ou 4 éléments. Déduire de ces descriptions que tout groupe fini de cardinal inférieur ou égal à 4 est abélien.

Cet exo est l'objet de la propriété 12.4 du pdf, dont la démonstration est située entre les pages 271 et 274. Elle repose essentiellement sur l'écriture des "tables de multiplication" des groupes de cardinal $\leqslant 4$, ce qui est un petit jeu de "sudoku"...

Exercice 9. — **(Groupe des similitudes).** On rappelle que l'on note : $\mathbb{C}^{\mathbb{C}}$ l'ensemble des applications de $\mathbb{C}$ dans $\mathbb{C}$.

1/ Vérifier que la composition usuelle (notée "$\circ$") est une loi de composition interne sur $\mathbb{C}^{\mathbb{C}}$.

La composition de deux applications de $\mathbb{C}$ dans $\mathbb{C}$ est encore une application de $\mathbb{C}$ dans $\mathbb{C}$, d'où la conclusion.

2/ $\left(\mathbb{C}^{\mathbb{C}}, \circ\right)$ est-il un groupe ?

La composition dans $\mathbb{C}^{\mathbb{C}}$ est une LCI (observation faite question précédente), associative (car la composition des applications en général l'est), qui possède un élément neutre ($\mathrm{id}_{\mathbb{C}}$).

Mais toute application de $\mathbb{C}$ dans $\mathbb{C}$ ne possède pas d'inverse pour la composition ; les seuls éléments de $\mathbb{C}^{\mathbb{C}}$ qui sont inversibles pour la loi "$\circ$" étant les bijections de $\mathbb{C}$ dans $\mathbb{C}$. [2]

Conclusion. $\left(\mathbb{C}^{\mathbb{C}}, \circ\right)$ n'est pas un groupe.

3/ Pour tout $a \in \mathbb{C}^*$, et pour tout $b \in \mathbb{C}$ on définit l'application $f_{a,b} : \mathbb{C} \longrightarrow \mathbb{C}$ par : $f_{a,b}(z) = az + b$.

a) Calculer : $f_{a',b'} \circ f_{a,b}$.

Soit $z \in \mathbb{C}$. On a :

$$\left(f_{a',b'} \circ f_{a,b}\right)(z) = f_{a',b'}\left(f_{a,b}(z)\right) = f_{a',b'}\left(az+b\right) = a'(az+b) + b' = a'az + a'b + b' = f_{a'a,a'b+b'}(z)$$

Conclusion. $\left(f_{a',b'} \circ f_{a,b}\right) = f_{a'a,a'b+b'}$

b) Montrer que $\left(\{f_{a,b};\ a \in \mathbb{C}^*,\ b \in \mathbb{C}\}, \circ\right)$ est un groupe. Ce groupe est-il abélien ?

Notons : $E = \{f_{a,b};\ a \in \mathbb{C}^*,\ b \in \mathbb{C}\}$.

- ➤ D'après ce qui précède, la composition ("$\circ$") est une LCI sur E.
- ➤ Cette LCI est associative (puisque la composition des applications en général est associative).
- ➤ L'identité de $\mathbb{C}$, qui est l'élément neutre pour la composition, est un élément de E puisque : $\mathrm{id}_{\mathbb{C}} = f_{1,0}$.

2. Une remarque analogue a été faite à la fin de l'exercice 2.

➤ Reste à vérifier que tout élément de E est inversible dans E. A cette fin, considérons un élément quelconque $f_{a,b}$ de E, avec $a \in \mathbb{C}^*$ et $b \in \mathbb{C}$.

Par définition, l'application $f_{a,b}$ est inversible si et seulement si :

$$\exists\, f_{a',b'} \in E, \quad f_{a,b} \circ f_{a',b'} = \mathrm{id}_{\mathbb{C}} = f_{a',b'} \circ f_{a,b}$$

Or :

$$[f_{a',b'} \circ f_{a,b} = \mathrm{id}_{\mathbb{C}}] \iff [f_{a'a,a'b+b'} = \mathrm{id}_{\mathbb{C}}] \iff [f_{a'a,a'b+b'} = f_{1,0}] \iff [a'a = 1 \text{ et } a'b + b' = 0]$$

Or :

$$\begin{cases} a'a = 1 \\ a'b + b' = 0 \end{cases} \iff \begin{cases} a' = \dfrac{1}{a} \\ b' = -\dfrac{b}{a} \end{cases}$$

On en déduit que : $f_{1/a,-b/a} \circ f_{a,b} = \mathrm{id}_{\mathbb{C}}$.

On vérifie alors aisément que : $f_{a,b} \circ f_{1/a,-b/a} = \mathrm{id}_{\mathbb{C}}$.

En résumé, tout élément $f_{a,b}$ de E admet un inverse pour la composition, qui est encore un élément de E (puisque c'est : $f_{1/a,-b/a}$).

Conclusion. E est un ensemble muni d'une LCI ("$\circ$") associative, possédant un élément neutre, et dans lequel tout élément admet un inverse pour la composition. A ce titre, $(E, \circ)$ est un groupe.

En outre on a :

$$f_{2,1} \circ f_{1,1} = f_{2,3} \quad \text{et} \quad f_{1,1} \circ f_{2,1} = f_{2,2}$$

Donc : $f_{2,1} \circ f_{1,1} \neq f_{1,1} \circ f_{2,1}$.

On en déduit que E est un groupe non abélien.

Remarque. E est le groupe des similitudes directes du plan complexe, déjà rencontré cette année au chapitre 4.

Exercice 10. — Soient f_1, f_2, f_3 et f_4 les fonctions de $\mathbb{R}^*$ dans $\mathbb{R}^*$ définies par :

$$f_1(x) = x \qquad f_2(x) = \frac{1}{x} \qquad f_3(x) = -x \qquad f_4(x) = -\frac{1}{x}$$

1/ Montrer que $G = \{f_1, f_2, f_3, f_4\}$ muni de la composition $\circ$ est un groupe abélien.

Pour commencer, on prouve que la loi "o" est une LCI sur G en calculant toutes les composées de 2 éléments quelconques de G, càd en dressant la "table de multiplication" du groupe G, que voici :

$*$	f_1	f_2	f_3	f_4
f_1	f_1	f_2	f_3	f_4
f_2	f_2	f_1	f_4	f_3
f_3	f_3	f_4	f_1	f_2
f_4	f_4	f_3	f_2	f_1

On déduit de cette table que la loi "o" est une LCI sur G (la composée de deux éléments quelconques de G étant encore un élément de G).

En outre, la loi "o" est associative (car la composition des applications est associative en général).

De plus, cette LCI possède un élément neutre : $f_1 = \mathrm{id}_{\mathbb{R}^*}$.

Enfin, tout élément de G possède un inverse dans G pour la loi $\circ$, puisque chacun des éléments de G est son propre inverse.

Il s'ensuit que $(G, \circ)$ est un groupe. Il résulte du cours [3] ou de la symétrie de la table ci-dessus par rapport à la diagonale que G est abélien.

Conclusion. $(G, \circ)$ est un groupe abélien.

3. Tout groupe fini de cardinal 4 est abélien.

2/ Déterminer l'ensemble de ses sous-groupes.

Observons qu'un sous-groupe H de G possède au plus 4 éléments, et au moins un élément (l'élément neutre). On distingue donc plusieurs cas suivant le cardinal (càd le nombre d'éléments) de H.

- Cas 1 — $\text{card}(H) = 1$ [4] : il existe un seul sous-groupe de G ayant pour cardinal 1, le **sous-groupe trivial** $(\{f_1\}, \circ)$.
- Cas 2 — $\text{card}(H) = 4$: il existe un seul sous-groupe de G ayant pour cardinal 4, le groupe G lui-même.
- Cas 3 — $\text{card}(H) = 2$: notons $H_1 = \{f_1, f_2\}$. $(H_1, \circ)$ est un sous-groupe de $(G, \circ)$ (essentiellement car f_1 est son propre inverse). De même, $H_2 = \{f_1, f_3\}$ et $H_3 = \{f_1, f_4\}$ sont deux autres sous-groupes de cardinal 2.

  Il n'existe pas d'autre sous-groupe de cardinal 2.
- Cas 4 — $\text{card}(H) = 3$: il n'existe aucun sous-groupe de cardinal 3 de G. En effet, s'il existait, un tel sous-groupe H devrait contenir l'élément neutre (f_1) et deux autres éléments de G ; or la composée de ces deux éléments sera égal au dernier élément de G, et n'appartiendra donc pas à H.

  Pour illustrer ce propos par un exemple, considérons $H = \{f_1, f_2, f_3\}$. On a : $f_2 \circ f_3 = f_4$. Donc $f_2 \circ f_3 \notin H$. Donc la loi "$\circ$" n'est pas une LCI sur H. La conclusion est la même quels que soient les deux éléments que l'on choisit en plus de f_1.

Conclusion. G possède un sous-groupe de cardinal 4 (G lui-même), trois sous-groupes de cardinal 2 (H_1, H_2 et H_3), et un sous-groupe de cardinal 1 (le sous-groupe trivial).

Exercice 11. — Soit G un groupe. On appelle **centre de G** et on note $Z(G)$ l'ensemble des éléments de G qui commutent avec tous les éléments de G, soit : $Z(G) = \{a \in G \mid \forall\, g \in G,\ ag = ga\}$. Montrer que $Z(G)$ est un sous-groupe de G. Que devient $Z(G)$ lorsque G est abélien ?

On montre que $Z(G)$ est un sous-groupe de G en vérifiant les 4 axiomes du cours :

- (SG1) $Z(G) \subset G$ par définition même de $Z(G)$;
- (SG2) Pour tout $g \in G$, on a : $\text{e} * g = g * \text{e}$. Donc : $\text{e} \in Z(G)$.
- (SG3) Soient a et b dans $Z(G)$. Pour tout élément g de G on a :

$$(a * b) * g = a * (b * g) = a\,(g * b) = (a * g) * b = (g * a) * b = g * (a * b)$$

  On en déduit que $(a * b)$ appartient à $Z(G)$. En résumé : $[a \text{ et } b \in Z(G)] \Longrightarrow [a * b \in Z(G)]$.
- (SG4) Soit a dans $Z(G)$. Pour tout élément g de G on a :

$$a^{-1} * g = (g^{-1} * a)^{-1} = (a * g^{-1})^{-1} = g * a^{-1}$$

  On en déduit que a^{-1} appartient à $Z(G)$. En résumé : $[a \in Z(G)] \Longrightarrow [a^{-1} \in Z(G)]$.

4. On note $\text{card}(H)$ le cardinal de H, càd le nombre d'éléments de H.

Conclusion. D'après ce qui précède, $Z(G)$ est un sous-groupe de G.

Lorsque G est abélien, on a : $Z(G) = G$.

Exercice 12. — Soient H et K deux sous-groupes d'un groupe $(G, \star)$ tels que $H \cup K$ en soit aussi un sous-groupe. Montrer que $H \subset K$ ou $K \subset H$.

Supposons que H et K sont deux sous-groupes d'un groupe G, tels que $H \cup K$ est un sous-groupe de G.

Par l'absurde, supposons que $K \not\subset H$ et $H \not\subset K$.

Alors il existe un élément h de H tel que $h \notin K$; et il existe un élément k de K tel que $k \notin H$.

Posons : $g = h \star k$. Alors g appartient à $H \cup K$, puisque h et k appartiennent à $H \cup K$, et que $H \cup K$ est un sous-groupe de G par hypothèse.

Donc g appartient à H, ou g appartient à K.

Supposons que g appartienne à H. Alors : $h^{-1} \star g \in H$ (puisque H est un sous-groupe). Donc $k \in H$: contradiction.

De même, si l'on suppose que g appartient à K, on aboutit à une contradiction ($h \in K$).

Par conséquent, l'hypothèse faite au début du raisonnement est fausse. On en déduit que $H \subset K$ ou $K \subset H$.

Anneaux, corps

Exercice 13. — On note $\mathbb{D}$ l'ensemble des nombres décimaux : $\mathbb{D} = \left\{ \dfrac{n}{10^k} \ | n \in \mathbb{Z},\ k \in \mathbb{N} \right\}$. Montrer que $\mathbb{D}$ est un sous-anneau de $(\mathbb{R}, +, \times)$.

$(\mathbb{D}, +, \times)$ est un sous-anneau de $(\mathbb{R}, +, \times)$ car :

- $(\mathbb{D}, +)$ est un sous-groupe de $(\mathbb{R}, +)$ selon l'exercice 4.
- La multiplication est une LCI associative sur $\mathbb{D}$ (il suffit de vérifier que le produit de deux décimaux est encore décimal), et possède un élément neutre (1 est un décimal, puisque $1 = 1/10^0 \ldots$).

On peut observer que l'anneau $\mathbb{D}$ n'est pas un corps, puisque 3 est décimal mais que son inverse pour la multiplication ne l'est pas.

Exercice 14. — Montrer que $(\mathscr{F}(\mathbb{R}, \mathbb{R}), +, \times)$ est un anneau commutatif. Est-il intègre ?

$(\mathscr{F}(\mathbb{R}, \mathbb{R}), +, \times)$ est un anneau commutatif car :

- $(\mathscr{F}(\mathbb{R}, \mathbb{R}), +)$ est un groupe abélien : l'addition est une LCI associative et commutative, possédant un élément neutre (la fonction identiquement nulle sur $\mathbb{R}$), et toute fonction f définie sur $\mathbb{R}$ admet un inverse pour la l'addition (son opposée $-f$).
- La multiplication est une LCI associative sur $\mathscr{F}(\mathbb{R}, \mathbb{R})$, et possède un élément neutre (la fonction constante égale à 1 sur $\mathbb{R}$), et la multiplication est distributive par rapport à l'addition dans $\mathscr{F}(\mathbb{R}, \mathbb{R})$.

On peut observer que l'anneau $\mathscr{F}(\mathbb{R}, \mathbb{R})$ n'est pas un corps, puisque la fonction sin (qui est non nulle) n'est pas inversible pour la multiplication dans $\mathscr{F}(\mathbb{R}, \mathbb{R})$ (la fonction $1/\sin$ n'est pas définie sur $\mathbb{R}$ tout entier).

Exercice 15. — On pose $\mathbb{Z}[\mathrm{i}] = \{a+\mathrm{i}b \,|\, (a,b) \in \mathbb{Z}^2\}$. Montrer que $(\mathbb{Z}[\mathrm{i}], +, \times)$ est un anneau commutatif (*il est appelé anneau des entiers de Gauss*). Est-ce un corps ?

On peut montrer que $(\mathbb{Z}[\mathrm{i}], +, \times)$ est un anneau commutatif directement (voir plan des exos 15 et 17), ou en prouvant que c'est un sous-anneau de $(\mathbb{C}, +, \times)$. On utilise ici cette seconde méthode, pour changer :

➤ $(\mathbb{Z}[\mathrm{i}], +)$ est un sous-groupe de $(\mathbb{C}, +)$ car $\mathbb{Z}[\mathrm{i}] \subset \mathbb{C}$, $0 \in \mathbb{Z}[\mathrm{i}]$ (car $0 = 0 + \mathrm{i}0$, pas d'applaudissements...), la somme de deux éléments de $\mathbb{Z}[\mathrm{i}]$ est encore dans $\mathbb{Z}[\mathrm{i}]$, et si tout élément $a + \mathrm{i}b$ de $\mathbb{Z}[\mathrm{i}]$ admet un inverse pour la loi $+$ dans $\mathbb{Z}[\mathrm{i}]$ (son opposé $-a - \mathrm{i}b$).

➤ La multiplication est une LCI associative sur $\mathbb{Z}[\mathrm{i}]$ (il suffit de vérifier que le produit de deux entiers de Gauss en est encore un), et possède un élément neutre (1 est un décimal, puisque $1 = 1 + \mathrm{i}0\ldots$).

On en déduit que $\mathbb{Z}[\mathrm{i}]$ est un sous-anneau de l'anneau des nombres complexes. A ce titre, $\mathbb{Z}[\mathrm{i}]$ est un anneau.

En revanche, l'anneau $\mathbb{Z}[\mathrm{i}]$ des entiers de Gauss n'est pas un corps : 2 est un entier de Gauss, mais son inverse $1/2$ n'est pas dans $\mathbb{Z}[\mathrm{i}]$.

Exercice 16. — On pose $\mathbb{Q}[\mathrm{i}] = \{a + \mathrm{i}b \,|\, (a,b) \in \mathbb{Q}^2\}$. Montrer que $(\mathbb{Q}[\mathrm{i}], +, \times)$ est un corps.

On peut montrer comme dans l'exercice précédent que $(\mathbb{Q}[\mathrm{i}], +, \times)$ est un anneau commutatif en prouvant que c'est un sous-anneau de $(\mathbb{C}, +, \times)$.

Pour prouver que c'est un corps, il suffit de prouver que tout élément non nul de $\mathbb{Q}[\mathrm{i}]$ est inversible pour la multiplication dans $\mathbb{Q}[\mathrm{i}]$.

Soit $a+\mathrm{i}b \neq 0$ dans $\mathbb{Q}[\mathrm{i}]$ (a et b sont donc rationnels). Alors :

$$\frac{1}{a+\mathrm{i}b} = \frac{a-\mathrm{i}b}{a^2+b^2} = \frac{a}{a^2+b^2} + \frac{-b}{a^2+b^2}\,\mathrm{i}$$

Puisque $\dfrac{a}{a^2+b^2}$ et $\dfrac{-b}{a^2+b^2}$ sont rationnels (a et b le sont, $a^2+b^2 \neq 0$, et $\mathbb{Q}$ est un corps), on en déduit que $\dfrac{1}{a+\mathrm{i}b} \in \mathbb{Q}[\mathrm{i}]$. Donc tout élément non nul de $\mathbb{Q}[\mathrm{i}]$ est inversible pour la multiplication dans $\mathbb{Q}[\mathrm{i}]$.

On en déduit que $(\mathbb{Q}[\mathrm{i}], +, \times)$ est un corps (c'est d'ailleurs un sous-corps de $\mathbb{C}$).

Groupes, anneaux, corps (pour aller un peu plus loin)

Exercice 17. — Soient n et p deux entiers naturels non nuls. A quelle condition sur n et p le groupe $(\mathbb{U}_n, \times)$ est-il un sous-groupe de $(\mathbb{U}_p, \times)$?

La première condition à vérifier doit être l'inclusion : $\mathbb{U}_n \subset \mathbb{U}_p$. Cette assertion est vraie dès que n divise p.

Sous cette hypothèse, la vérication des autres assertions (SG2, SG3 et SG4) est immédiate (puisque l'on a déjà établi dans le cours que $(\mathbb{U}_n, \times)$ est un groupe).

Conclusion. Si n divise p, alors $(\mathbb{U}_n, \times)$ est un sous-groupe de $(\mathbb{U}_p, \times)$.

Exercice 18. — **(Anneau des entiers de Gauss)**. On pose $\mathbb{Z}[i] = \{a+ib \,|\, (a,b) \in \mathbb{Z}^2\}$ et $\mathbb{Q}[i] = \{a+ib \,|\, (a,b) \in \mathbb{Q}^2\}$. Il a déjà été établi au cours des exercices précédents que le premier est un anneau commutatif, et le second un corps.

On définit l'application $N : \mathbb{Z}[i] \longrightarrow \mathbb{N}$ par : $\forall z \in \mathbb{Z}[i]$, $N(z) = z\bar{z}$.

1/ Montrer que pour tout $(z, z') \in \mathbb{Z}[i]^2$, $N(zz') = N(z)N(z')$.

Soient z et z' dans $\mathbb{Z}[i]$. On a : $N(zz') = zz'\overline{zz'} = z\bar{z}z'\overline{z'} = N(z)N(z')$.

2/ En déduire l'équivalence suivante : z est inversible dans $\mathbb{Z}[i] \iff N(z) = 1$

Soit $z \in \mathbb{Z}[i]$. Si z est inversible dans $\mathbb{Z}[i]$, alors il existe $z' \in \mathbb{Z}[i]$ tel que : $zz' = 1$.

On en déduit que : $N(zz') = N(1)$. D'après la question précédente, on a donc : $N(z)N(z') = 1$. Or $N(z)$ $N(z')$ sont des entiers naturels ; il s'ensuit que $N(z) = N(z') = 1$.

Ce qui prouve l'implication : z est inversible dans $\mathbb{Z}[i] \Longrightarrow N(z) = 1$.

Réciproquement, supposons que $N(z) = 1$. Alors $z = a + \mathrm{i}b$ avec a et b entiers naturels tels que : $a^2+b^2 = 1$. Ceci implique que ($a = \pm 1$ et $b = 0$) ou ($a = 0$ et $b = \pm 1$). D'où $z = \pm 1$ ou $z = \pm \mathrm{i}$. Chacun de ces 4 entiers de Gauss étant inversible pour la multiplication dans $\mathbb{Z}[i]$ (1 et -1 sont leurs propres inverses, i et $-\mathrm{i}$ sont inverses l'un de l'autre), on a prouvé l'implication réciproque.

Conclusion. z est inversible dans $\mathbb{Z}[i] \iff N(z) = 1$

3/ Reconnaître alors l'ensemble des éléments inversibles de $\mathbb{Z}[i]$ et vérifier qu'il s'agit bien d'un groupe.

D'après les calculs de la question précédente, l'ensemble des éléments inversibles (pour la multiplication) de $\mathbb{Z}[i]$ est :

$$(\mathbb{Z}\,[\mathrm{i}])^* = \{1, -1, \mathrm{i}, -\mathrm{i}\}$$

En d'autres termes : $(\mathbb{Z}\,[\mathrm{i}])^* = \mathbb{U}_4$. D'après le cours [5], $(\mathbb{Z}\,[\mathrm{i}])^*$ est un groupe (abélien).

Exercice 19. — Soit F un sous-corps de $(\mathbb{Q}, +, \times)$. Montrer que $F = \mathbb{Q}$.

Plan de la preuve, pour ce qui est une question à la limite du programme (et plus que rarissime à l'écrit) :

- ➤ $1 \in F$ par définition de sous-corps.
- ➤ Donc $\mathbb{N} \subset F$ par récurrence, et en utilisant le fait que l'addition est une LCI sur F.
- ➤ Donc $\mathbb{Z} \subset F$ en utilisant le fait précédent, et le fait que l'opposé de tout élément de F est encore dans F, puisque $(F, +)$ est un sous-groupe de $(\mathbb{Q}, +)$.
- ➤ Soit $\frac{a}{b}$ un rationnel, avec $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$. Alors $a \in F$ (cf second point) ; et $1/b \in F$, puisque b est un élément non nul de $\mathbb{N}$ donc de F, et que tout élément non nul de F est inversible dans F (puisque F est un sous-corps de $\mathbb{Q}$ par hypothèse). On en déduit que $a \times (1/b)$ est un élément de F (la multiplication étant une LCI sur F, toujours par hypothèse). Donc : $\frac{a}{b} \in F$.
- ➤ Ce qui précède prouve que : $\mathbb{Q} \subset F$. Or $F \subset \mathbb{Q}$ par hypothèse. D'après la régle de double inclusion, on en déduit que $F = \mathbb{Q}$.

Conclusion. $\mathbb{Q}$ n'admet pas d'autre sous-corps que $\mathbb{Q}$ lui-même.

5. Vous pouvez utiliser sans justification le résultat du cours affirmant que $(\mathbb{U}_n, \times)$ est un groupe (abélien), car c'est un sous-groupe de $(\mathbb{U}, \times)$, qui est lui-même un sous-groupe de $(\mathbb{C}^*, \times)$.