Question de cours. Montrer que $\bigcup_{n\in\mathbb{N}^*}\mathbb{U}_n$ est un groupe pour une loi de composition interne que l'on précisera.

Réponse. On considère la loi $\times$. Montrer que $\bigcup_{n\in\mathbb{N}^*}\mathbb{U}_n$ est un sous-groupe de $\mathbb{C}^*$ pour cette loi.

- Nous avons bien $\bigcup_{n\in\mathbb{N}^*}\mathbb{U}_n \subset \mathbb{C}^*$.
- Nous avons bien $1 \in \bigcup_{n\in\mathbb{N}^*}\mathbb{U}_n$ parce que $1^1 = 1$ par exemple.
- Soient $z, w \in \bigcup_{n\in\mathbb{N}^*}\mathbb{U}_n$. Alors il existe $n, m \in \mathbb{N}^*$ tels que $z^n = 1 = w^m$. En particulier

$$(zw^{-1})^{nm} = (z^n)^m(w^m)^{-n} = 1.$$

  Donc $zw^{-1} \in \mathbb{U}_{nm} \subset \bigcup_{k\in\mathbb{N}^*}\mathbb{U}_k$.

Par conséquent $\bigcup_{n\in\mathbb{N}^*}\mathbb{U}_n$ est un sous-groupe de $\mathbb{C}^*$. En particulier il s'agit d'un groupe.

Exercice. On considère un morphisme d'anneaux $f : \mathbb{C} \longrightarrow \mathbb{C}$ tel que

$$\forall x \in \mathbb{R}, \quad f(x) = x.$$

Montrer que f est l'identité ou la conjugaison complexe.

Réponse. Nous avons

$$f(i)^2 = f(i^2) = f(-1) = -1.$$

Donc $f(i) \in \{i, -i\}$. Si $f(i) = i$ alors

$$\forall x + iy \in \mathbb{C}, \quad f(x + iy) = f(x) + f(i)f(y) = x + iy,$$

d'où f est l'identité. Sinon $f(i) = -i$ et dans ce cas

$$\forall x + iy \in \mathbb{C}, \quad f(x + iy) = f(x) + f(i)f(y) = x - iy = \overline{x + iy},$$

d'où f est la conjugaison complexe.

Exercice. On considère pour $a, b \in \mathbb{R}$,

$$a \perp b = a + b - 1, \quad a \cdot b = ab - a - b + 2.$$

Montrer que $(\mathbb{R}, \perp, \cdot)$ est un corps.

Réponse. On commence par vérifier que $(\mathbb{R}, \perp)$ est un groupe abélien.

- $\perp$ est bien une loi de composition interne.
- $\perp$ est associative : pour tout $a, b, c \in \mathbb{R}$,

$$a \perp (b \perp c) = a \perp (b + c - 1) = a + b + c - 1 - 1 = a + b + c - 2 = (a \perp b) \perp c.$$

- $\perp$ est commutative : pour tout $a, b \in \mathbb{R}$,

$$a \perp b = a + b - 1 = b + a - 1 = b \perp a.$$

- $\perp$ admet 1 comme élément neutre : pour tout $a \in \mathbb{R}$,

$$a \perp 1 = a + 1 - 1 = a.$$

- $\perp$ est inversible : pour tout $a \in \mathbb{R}$,

$$a \perp (-a) = a - a + 1 = 1.$$

On vérifie ensuite que $(\mathbb{R}, \perp, \cdot)$ est un corps.

- $\cdot$ est commutative : pour tout $a, b \in \mathbb{R}$,

$$a \cdot b = ab - a - b + 2 = ba - b - a + 2 = b \cdot a.$$

- $\cdot$ est associative : pour tout $a, b, c \in \mathbb{R}$,

  $a \cdot (b \cdot c) = a \cdot (bc - b - c + 2) = a(bc - b - c + 2) - a - (bc - b - c + 2) + 2 = abc - ab - ac - bc + a + b + c = (a \cdot b) \cdot c.$

- $\cdot$ admet 2 comme élément neutre : pour tout $a \in \mathbb{R}$,

  $$a \cdot 2 = 2a - a - 2 + 2 = a.$$

- $\cdot$ est distributive sur $\perp$: pour tout $a, b, c \in \mathbb{R}$,

  $a \cdot (b \perp c) = a(b \perp c) - a - b \perp c + 2 = a(b + c - 1) - a - b - c + 1 + 2 = ab + ac - 2a - b - c + 3$

  et

  $(a \cdot b) \perp (a \cdot c) = a \cdot b + a \cdot c - 1 = ab - a - b + 2 + ac - a - c + 2 - 1 = ab + ac - 2a - b - c + 3.$

  Donc

  $$a \cdot (b \perp c) = (a \cdot b) \perp (a \cdot c).$$

- $\cdot$ est inversible: pour tout $a \in \mathbb{R} \backslash \{1\}$, on cherche $b \in \mathbb{R}$ tel que

  $$2 = a \cdot b = ab - a - b + 2$$

  i.e. $a = ab - b = b(a - 1)$ i.e., comme $a \neq 1$, $b = \dfrac{a}{a - 1}$. Par conséquent

  $$a \cdot \frac{a}{a-1} = a\frac{a}{a-1} - a - \frac{a}{a-1} + 2 = \frac{a^2 - a(a-1) - a + 2(a-1)}{a-1} = 2.$$

Question de cours. Expliciter les sous-groupes de $(\mathbb{Z}, +)$.

Réponse. Montrons que les sous groupes de $\mathbb{Z}$ sont exactement les $n\mathbb{Z}$ pour $n \in \mathbb{N}$. On procède par double inclusions.

- Soit $n \in \mathbb{N}$. Alors:
  - ⋆ $n\mathbb{Z} \subset \mathbb{Z}$.
  - ⋆ $0 = n \times 0 \in n\mathbb{Z}$.
  - ⋆ Soient $x, y \in n\mathbb{Z}$. Alors il existe $k, \ell \in \mathbb{Z}$ tels que $x = nk$ et $y = n\ell$. En particulier
  $$x - y = n(k - \ell) \in \mathbb{Z}.$$
  Par conséquent $n\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$.
- Réciproquement on considère H un sous-groupe de $\mathbb{Z}$. Si $H = \{0\}$ alors H est un sous-groupe de $\mathbb{Z}$. Sinon il existe $x \in H$ tel que $x \neq 0$. Si $x < 0$ alors, comme H est un sous-groupe, $-x \in H$. Ainsi
  $$\{x \in \mathbb{N}^*, \quad x \in H\}$$
  est un sous-ensemble non vide de $\mathbb{N}$. Donc il admet un plus petit élément
  $$n := \min\{x \in \mathbb{N}^*, \quad x \in H\}.$$
  En particulier $n \in H$. Donc, comme H est un sous-groupe, $n\mathbb{Z} \subset H$. Réciproquement soit $x \in H$. Si $x = 0$ alors $x = n \times 0 \in n\mathbb{Z}$. Si $x > 0$ alors on effectue la division euclidienne de x par n: il existe $q, r \in \mathbb{N}$ tels que
  $$x = qn + r, \quad 0 \leq r < n.$$
  Si $r \neq 0$ alors $0 < r < n$ et $r = x - qn \in H$ ce qui contredit la définition de n. Donc $r = 0$ et $x = qn \in n\mathbb{Z}$. Si $x < 0$ alors $-x > 0$ et ainsi $-x \in n\mathbb{Z}$, d'où $x \in n\mathbb{Z}$. Par conséquent
  $$H = n\mathbb{Z}.$$

Exercice. On considère $A = \mathcal{M}_2(\mathbb{Z})$ l'ensemble des matrices carrées d'ordre 2 à coefficients entiers.

1. Montrer que A est un anneau non commutatif.
2. Montrer que les éléments inversibles de A sont ceux de déterminants ± 1. On pourra commencer par rappeler la formule du déterminant pour les matrices carrées d'ordre 2.
3. Les applications trace et déterminant sont-elles des morphismes d'anneaux de A vers $\mathbb{Z}$?

Réponse.

1. Montrons que A est un sous-anneau de $\mathcal{M}_2(\mathcal{R})$.
   - Nous avons bien $I_2 \in A$.
   - Soient $M, N \in A$. Alors $M - N \in A$ et $MN \in A$.

   Donc A est un sous-anneau de $\mathcal{M}_2(\mathcal{R})$, en particulier un anneau. Il n'est pas commutatif car par exemple
   $$\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \neq \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}.$$
2. Soit $M \in A^\times$. Alors il existe $N \in A$ tel que $MN = I_2$. Ainsi $\det(M)\det(N) = 1$ avec $\det(M), \det(N) \in \mathbb{Z}$. Donc $\det(M) = \pm 1$. Réciproquement soit $M \in A$ tel que $\det(M) = \pm 1$. Ainsi M est inversible et, en notant $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$,
   $$M^{-1} = \frac{1}{\det(M)}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \pm\begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \in A.$$
   Donc $M \in A^\times$.

3. Il n'agit pas de morphismes d'anneaux car par exemple

$$\mathrm{tr}\left(\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\right) = \mathrm{tr}\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = 1 \neq 0 = \mathrm{tr}\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}\mathrm{tr}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$

et

$$\det\left(\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\right) = \det\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = -1 \neq 0 = \det\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} + \det\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}.$$

Exercice. On considère les corps

$$C_1 = \mathbb{Q}[i\sqrt{2}] = \{a + bi\sqrt{2}, \quad a, b \in \mathbb{Q}\}, \quad C_2 = \mathbb{Q}[i\sqrt{2}] = \{a + b\sqrt{2}, \quad a, b \in \mathbb{Q}\}.$$

1. Déterminer $x, y \in \mathbb{Q}[i\sqrt{2}]$ tels que
$$-1 = x^2 + y^2.$$
2. En déduire que les corps $\mathbb{Q}[i\sqrt{2}]$ et $\mathbb{Q}[\sqrt{2}]$ ne sont pas isomorphes.

Réponse.

1. Nous avons $(i\sqrt{2})^2 = -2$ donc
$$-1 = 1^2 + (i\sqrt{2})^2.$$
2. On suppose par l'absurde qu'il existe une isomorphisme de corps φ de $\mathbb{Q}[i\sqrt{2}]$ vers $\mathbb{Q}[\sqrt{2}]$. Alors
$$-1 = -1\varphi(1) = \varphi(-1) = \varphi(x^2 + y^2) = \varphi(x)^2 + \varphi(y)^2 \geq 0$$
ce qui est absurde. Par conséquent il n'existe pas de morphisme d'anneaux entre les corps $\mathbb{Q}[i\sqrt{2}]$ et $\mathbb{Q}[\sqrt{2}]$.

Question de cours. Montrer que $\mathbb{Q}[\sqrt{3}] = \{a + b\sqrt{3},\ a, b \in \mathbb{Q}\}$ est un sous-corps de $\mathbb{R}$.

Réponse. Montrons tout d'abord que $\mathbb{Q}[\sqrt{3}]$ est un sous-anneau de $(\mathbb{R}, +, \times)$.

- Nous avons bien $\mathbb{Q}[\sqrt{3}] \subset \mathbb{R}$.
- Nous avons bien $0 = 0 + 0 \times \sqrt{3} \in \mathbb{Q}[\sqrt{3}]$.
- Soient $x, y \in \mathbb{Q}[\sqrt{3}]$. Alors il existe $a, b, c, d \in \mathbb{Q}$ tels que $x = a + b\sqrt{3}, y = c + d\sqrt{3}$. Donc

$$x - y = a - c + (b - d)\sqrt{3} \in \mathbb{Q}[\sqrt{3}].$$

- Toujours avec x et y nous avons

$$xy = ac + 3bd + (ad + bc)\sqrt{3} \in \mathbb{Q}[\sqrt{3}].$$

Il ne reste plus qu'à montrer que $\mathbb{Q}[\sqrt{3}]$ est inversible pour $\times$. Soit $x = a + b\sqrt{3} \in \mathbb{Q}[\sqrt{3}]$ différent de 0. Si $b = 0$ alors

$$x^{-1} = \frac{1}{a} \in \mathbb{Q}[\sqrt{3}].$$

Sinon $b \neq 0$ et ainsi $a - b\sqrt{3} \neq 0$ par unicité d'une telle décomposition dans $\mathbb{Q}[\sqrt{3}]$, d'où

$$x^{-1} = \frac{1}{a + b\sqrt{3}} = \frac{a - b\sqrt{3}}{a^2 - 3b^2} = \frac{a}{a^2 - 3b^2} - \frac{b}{a^2 - 3b^2}\sqrt{3} \in \mathbb{Q}[\sqrt{3}].$$

Par conséquent nous avons montré que $\mathbb{Q}[\sqrt{3}]$ est un sous-corps de $\mathbb{R}$.

Exercice. On considère un groupe G noté multiplicativement et deux sous-groupes A et B de G. On définit le sous-ensemble

$$AB = \{ab, \quad a \in A, b \in B\} \subset G.$$

Montrer que AB est un sous-groupe de G si et seulement si $AB = BA$.

Réponse. On procède par double implications.

- On suppose que $AB = BA$. Vérifions les propriétés d'un sous-groupe.
  - ⋆ $1 = 1 \times 1 \in AB$ car A et B sont des sous-groupes de G.
  - ⋆ Soient $a_1b_1, a_2b_2 \in AB$ avec $a_1, a_2 \in A$ et $b_1, b_2 \in B$. Alors

$$a_1b_1(a_2b_2)^{-1} = a_1b_1b_2^{-1}a_2^{-1}$$

    avec $b_2^{-1}a_2^{-1} \in BA = AB$. Donc il existe $a_3 \in A$ et $b_3 \in B$ tels que $b_2^{-1}a_2^{-1} = a_3b_3$. Ainsi

$$a_1b_1(a_2b_2)^{-1} = a_1b_1a_3b_3$$

    avec $b_1a_3 \in BA = AB$. Ainsi il existe $a_4 \in A$ et $b_4 \in B$ tels que $b_1a_3 = a_4b_4$. Ainsi

$$a_1b_1(a_2b_2)^{-1} = a_1a_4b_4b_3 \in AB.$$

  Donc AB est un sous-groupe de G.

- Réciproquement on suppose que AB est un sous-groupe de G. Procédons par double inclusions.
  - ⋆ Soit $ab \in AB$. Alors $(ab)^{-1} \in AB$. Donc il existe $a_1 \in A$ et $b_1 \in B$ tels que $(ab)^{-1} = a_1b_1$ i.e.

$$ab = (a_1b_1)^{-1} = b_1^{-1}a_1^{-1} \in BA.$$

  - ⋆ L'autre inclusion s'obtient de la même manière par symétrie des rôles.

  Par conséquent $AB = BA$.

Exercice. Soit $(G, \times)$ un groupe noté multiplicativement et $a \in G$ d'inverse a^{-1}. On considère la loi de composition interne $*$ défini par

$$\forall x, y \in G, \quad x * y = xay.$$

1. Montrer que $(G, *)$ est un groupe. On notera x^{-*} l'inverse de $x \in G$ pour cette loi.
2. Soient H un sous groupe de $(G, \times)$ et $K = a^{-1}H = \{a^{-1}x,\ x \in H\}$. Montrer que K est un sous-groupe de $(G, *)$.
3. Montrer que l'application $f : x \in G \longmapsto x * a^{-1}$ est un isomorphisme de $(G, \times)$ vers $(G, *)$.

Réponse.

1. On vérifie les axiomes d'un groupe.
   - $*$ est associative : pour tout $x, y, z \in G$,
   $$x * (y * z) = xa(y * z) = xayaz = (x * y) * z.$$
   - $*$ admet a^{-1} comme élément neutre : pour tout $x \in G$,
   $$x * a^{-1} = xaa^{-1} = x = a^{-1}ax = a^{-1} * x.$$
   - $*$ est inversible : pour tout $x \in G$,
   $$x * (a^{-1}x^{-1}a^{-1}) = xaa^{-1}x^{-1}a^{-1} = a^{-1}.$$
   Donc
   $$x^{-*} = a^{-1}x^{-1}a^{-1}.$$
2. On vérifie les propriétés des sous-groupes.
   - $a^{-1} = a^{-1}1 \in a^{-1}H = K$.
   - Soient $a^{-1}x, a^{-1}y \in K$ avec $x, y \in H$. Alors $xy \in H$ et
   $$(a^{-1}x) * (a^{-1}y) = a^{-1}xaa^{-1}y = a^{-1}xy \in a^{-1}H = K.$$
   - Soit $a^{-1}x \in K$ avec $x \in H$. Alors $x^{-1} \in H$ et
   $$(a^{-1}x)^{-*} = a^{-1}(a^{-1}x)^{-1}a^{-1} = a^{-1}x^{-1}aa^{-1} = a^{-1}x^{-1} \in a^{-1}H = K.$$
3. On vérifie les propriétés d'un isomorphisme d'un groupes.
   - Nous avons bien le neutre de $\times$ qui est envoyé sur le neutre de $*$:
   $$f(1) = a^{-1}.$$
   - Soient $x, y \in G$. Alors
   $$f(xy^{-1}) = xy^{-1}a^{-1} = xa^{-1}ay^{-1}a^{-1} = f(x)af(y)^{-1} = f(x) * f(y)^{-1}.$$
   - Soient $x, y \in G$ tels que $f(x) = f(y)$ i.e. $xa^{-1} = ya^{-1}$ i.e. $x = y$. Donc f est injective.
   - Soit $z \in G$. Alors $z = zaa^{-1} = f(za)$. Donc f est surjective.

   Par conséquent f est un isomorphisme de $(G, \times)$ vers $(G, *)$.