Exercice I. On définit sur $\mathbb{R}^2\backslash\{(0,0)\}$ la loi de composition interne $\star$:

$$(x,y)\star(x',y') = (xx'-yy', xy'+x'y)$$

1. Montrer que $(\mathbb{R}^2\backslash\{(0,0)\},\star)$ est un groupe commutatif.

2. Montrer que ce groupe est isomorphe à $(\mathbb{C}\backslash\{0\},.)$.

Exercice II.

1. Soient $(G,.)$ un groupe et a,b deux éléments de G. Vérifier que les équations $a.x=b$ et $y.a=b$ ont une unique solution.

2. Soit E un ensemble non vide muni d'une loi de composition interne associative $\star$ telle que

$$\forall (a,b)\in E^2, \exists (x,y)\in E^2 \; a\star x = y\star a = b$$

Montrer que $(E,\star)$ est un groupe.

Exercice III. Soit $(G,.)$ un groupe dans lequel chaque élément est son propre inverse. Montrer que ce groupe est abélien.

Exercice IV. Soit $(G,.)$ un groupe, H et K deux sous-groupes de G. Montrer que $H\cup K$ est un sous-groupe de G si et seulement si $H\subset K$ ou $K\subset H$.

Exercice V. **1.** Soit G un groupe et $g\in G$. On note $C_G(g)=\{x\in G | gx=xg\}$ le **centralisateur de** g.

a. Montrer que $C_G(g)$ est un sous-groupe de G.

b. Calculer $C_{S_3}((123))$ et $C_{S_4}((12)(34))$.

2. On note $Z(G)=\{x\in G \mid \forall g\in G \; gx=xg\} = \cap_{g\in G} C_G(g)$ le **centre de** G.

a. Montrer que $Z(G)$ est un sous-groupe de G.

b. Déterminer $Z(S_3)$ et $Z(GL_2(\mathbb{R}))$.

Exercice VI. Soit n un entier et $\mathbb{Z}/n\mathbb{Z}^\times$ le groupe multiplicatif de $\mathbb{Z}/n\mathbb{Z}$.

1. Donner le cardinal de $\mathbb{Z}/n\mathbb{Z}^\times$.

2. Montrer que pour tout $x\in\mathbb{Z}$ premier avec n on a $x^{\varphi(n)}\equiv 1 \mod n$.

3. Calculer l'ordre des éléments de $\mathbb{Z}/3\mathbb{Z}^\times$, $\mathbb{Z}/5\mathbb{Z}^\times$ et $\mathbb{Z}/8\mathbb{Z}^\times$.

4. Montrer que $\mathbb{Z}/3\mathbb{Z}^\times \simeq \mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/5\mathbb{Z}^\times \simeq \mathbb{Z}/4\mathbb{Z}$ et $\mathbb{Z}/8\mathbb{Z}^\times \simeq \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$.

5. Déterminer tous les automorphismes de $\mathbb{Z}/n\mathbb{Z}$.

Exercice VII. **1.** Écrire la table de multiplication d'un groupe $(G, .)$ de cardinal 2, puis d'un groupe de cardinal 3.

Montrer que ces groupes sont uniques à isomorphismes près.

2. Quelles sont les tables de multiplication possibles pour un groupe de cardinal 4 ?

Donner l'ordre des éléments dans chacun des cas.

3. Montrer que si $\varphi : G \to G'$ est un homomorphisme de groupes et que g est un élément de G d'ordre fini, alors l'ordre de $\varphi(g)$ est fini et divise l'ordre de g.

Exercice VIII. Soit U l'ensemble des **racines de l'unité de** $\mathbb{C}$:

$$U = \{z \in \mathbb{C} \mid \exists n \in \mathbb{N}, z^n = 1\}$$

Pour tout $n \in \mathbb{N}$, on considère

$$U_n = \{z \in \mathbb{C} / z^n = 1\}$$

1. Montrer que U et U_n sont des sous-groupes multiplicatifs de $\mathbb{C}$.

2. Déterminer les éléments de U_n, pour tout n.

3. **a.** Soit $\omega = \mathrm{e}^{2i\pi/n}$. Quel est l'ordre de ω dans $(U_n, .)$?

b. En déduire que $< \omega >= U_n \simeq \mathbb{Z}/n\mathbb{Z}$.

4. Soit z un élément de U_n, $z = \mathrm{e}^{2ik\pi/n}$ pour $k \in \mathbb{Z}$. Démontrer que l'ordre de z est égal à $\frac{n}{pgcd(n,k)}$.

5. Citer les éléments de U_4 en précisant leurs ordres respectifs.

Exercice IX. On considère $C(\mathbb{R}) = \{\begin{pmatrix} a & -b \\ b & a \end{pmatrix} \mid a, b \in \mathbb{R}\}$ et $J = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$.

1. Montrer que $C(\mathbb{R})$ est un sous-anneau commutatif de $M_2(\mathbb{R})$.

2. Montrer que $C(\mathbb{R})$ est un corps.

3. Calculer J^2.

4. Montrer que $C(\mathbb{R})$ est isomorphe à $\mathbb{C}$ et préciser l'isomorphisme.

Exercice X. **Extensions quadratiques**. On considère $\mathbb{Z}[\sqrt{3}] = \{a + b\sqrt{3} \mid a, b \in \mathbb{Z}\}$.

1. Montrer que $\mathbb{Z}[\sqrt{3}]$ est un anneau commutatif intègre et unitaire.

2. On considère $N : \mathbb{Z}[\sqrt{3}] \to \mathbb{Z}$ tel que $N(a + b\sqrt{3}) = |a^2 - 3b^2|$.

a. Montrer que $\forall z, z' \in \mathbb{Z}[\sqrt{3}]$, $N(zz') = N(z)N(z')$.

b. En déduire que $\mathbb{Z}[\sqrt{3}]$ n'est pas un corps.

c. N est-il un homomorphisme d'anneau ?

d. Montrer que $U = \{z \in \mathbb{Z}[\sqrt{3}] \mid N(z) = 1\}$ est le groupe des unités de $\mathbb{Z}[\sqrt{3}]$. Donner quelques éléments de U.

3. Montrer que si z divise z' alors $N(z)$ divise $N(z')$. La réciproque est-elle vraie ?