Groupes, Anneaux, Corps

1 Questions de cours

1. Soit $f : G \to H$ un morphisme de groupe, et soit e le neutre de G. Montrer

$$f \text{ est injectif } \textit{si et seulement si } \ker f = \{e\}.$$

2. Soient a et b deux éléments d'un anneau A qui commutent. Soit $n \in \mathbb{N}^*$. Montrer que

$$a^n - b^n = (b-a)\sum_{k=0}^{n-1} a^k b^{n-k-1}.$$

3. Donner un exemple de groupe qui n'est pas un anneau, un exemple d'anneau qui n'est pas un corps, et un exemple de corps.

2 Applications du cours

1. À quelle condition sur un groupe G l'application $x \mapsto x^{-1}$ est-elle un morphisme de G dans lui-même ?
2. Soit $\mathbb{K}$ un corps (commutatif). Trouver tous les éléments a de $\mathbb{K}$ qui vérifient $a = a^{-1}$.
3. Soit $\mathscr{A}$ un anneau, et soit a un élément *nilpotent* (*i.e* vérifiant $\exists n \in \mathbb{N},\ a^n = 0$). Montrer que $1 - a$ est inversible dans $\mathscr{A}$, et calculer son inverse.

3 Exercices

1. Soit $(G, \cdot)$ un groupe. On définit sur G la loi $\star$ par

$$\forall x, y \in G,\ a \star b = b \cdot a.$$

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

2. On appelle *anneau de Boole* un anneau $(\mathscr{B}, +, \times)$ vérifiant

$$\forall x \in \mathscr{B},\ x^2 = x.$$

Montrer que tout anneau de Boole est commutatif.
Soit $\mathscr{B}$ un anneau de Boole intègre. Montrer que $\mathscr{B}$ ne peut avoir que deux éléments.

3. Montrer que les sous-groupes de $\mathbb{Z}$ sont les $n\mathbb{Z} := \{n \times x \mid x \in \mathbb{Z}\}$ pour $n \in \mathbb{N}$.
4. Trouver tous les morphismes de groupe de $(\mathbb{Q}, +)$ dans $(\mathbb{Z}, +)$.
5. Soit $(G, \cdot)$ un groupe, de neutre e. Soit E un ensemble tel qu'il existe $\varphi : G \to E$ bijective.
On définit $\star$ sur E par

$$\forall a, b \in E,\ a \star b = \varphi\left(\varphi^{-1}(a) \cdot \varphi^{-1}(b)\right).$$

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

6. Montrer que tout sous-corps de $(\mathbb{Q}, +, \times)$ est égal à $\mathbb{Q}$ tout entier.
7. On appelle *anneau des entiers de Gauß* l'ensemble

$$\mathbb{Z}[i] = \{a + ib \mid (a, b) \in \mathbb{Z}^2\}.$$

(i) Montrer que $\mathbb{Z}[i]$ est un anneau pour l'addition et la multiplication usuelle de $\mathbb{C}$.
(ii) Déterminer les éléments inversibles de $\mathbb{Z}[i]$.

8. Montrer qu'un anneau intègre fini est toujours un corps.
9. Soit $(\mathscr{A}, +, \times)$ un anneau. On dit que $a \in \mathscr{A}$ est *nilpotent* s'il existe $n \in \mathbb{N}^*$ tel que $x^n = 0$.
(i) Montrer que si a est nilpotent, alors $1 - a$ est inversible, et donner son inverse. Calculer $(1 - a)^k$ pour $k \in \mathbb{N}$.
(ii) Soient a et b dans $\mathscr{A}$. Montrer que si $a \times b$ est nilpotent, alors $b \times a$ aussi.
(iii) Montrer que si a et b sont nilpotents et qui commutent, alors $a + b$ est nilpotent.
En déduire que si $\mathscr{A}$ est commutatif, l'ensemble des éléments nilpotents de $\mathscr{A}$ est un groupe additif.

4 Corrections

4.1 Applications

1. C'est un morphisme si le groupe est abélien.
2. Soit a un tel élément. Alors $a = a^{-1}$, *i.e* $a^2 = 1$.
   Donc $a = \pm 1$.
3. Soit n tel que $a^n = 0$.
   Alors $1 = 1 - a^n = (1-a)\sum_{k=0}^{n-1} a^{n-1-k}$.

4.2 Exercices

1. $\star$ est associative car $\cdot$ l'est.
   $\star$ possède un élément neutre qui est le même que celui de $\cdot$.
   Si $x \in G$, et si y est l'inverse de x pour $\cdot$, alors
   $$\begin{aligned} x \star y &= y \cdot x \\ &= 1 \\ &= y \star x \end{aligned}$$
2. On commence par montrer que pour tous x, y de $\mathscr{B}$, $xy = -yx$:
   $$\begin{aligned} (x+y)^2 &= x^2 + y^2 + xy + yx \\ &= x + y + xy + yx \\ &= x + y \end{aligned}$$
   On en déduit $(y = 1)$ que $x = -x$, et donc que $\mathscr{B}$ est commutatif.
   Si $\mathscr{B}$ est intègre, on a :
   $$\begin{aligned} xy(x+y) &= x^2 y + xy^2 \\ &= -xy + xy \\ &= 0, \end{aligned}$$
   et donc $x = 0$ ou $y = 0$ ou $x = y$.
3. Les $n\mathbb{Z}$ sont clairement des sous-groupes de $\mathbb{Z}$.
   Soit H un sous-groupe non trivial de $\mathbb{Z}$. On note $H^+ = H \cap \mathbb{Z}^+$.
   Alors H^+ admet un plus petit élément, soit n.
   On a alors $n\mathbb{Z} \subseteq H$.
   Pour l'inclusion réciproque, soit $x \in H$. On écrit la division euclidienne de x par n :
   $$x = np + r,\ 0 \leqslant r < n.$$
   Alors, comme $x - np \in H$, on a $r \in H$, ce qui est impossible si $r \neq 0$.

4. Soit φ un morphisme de groupe de $(\mathbb{Q},+)$ dans $(\mathbb{Z},+)$.
   On a alors, pour $n \in \mathbb{N}^*$:
   $$n\varphi\left(\frac{1}{n}\right) = \varphi(1).$$
   Donc $\varphi(1)$ est divisible par tous les entiers, et donc $\varphi(1) = 0$.
   On en déduit $\varphi = 0$.
5. $\star$ est associative car $\cdot$ l'est, et $\varphi \cdot \varphi^{-1} = \mathrm{id}$.
   $\star$ admet un élément neutre : si e est le neutre de G, $\varphi(e)$ est celui de E.
   Si $x \in E$, soit y l'inverse de $\varphi^{-1}(x)$ dans G. Alors
   $$\begin{aligned} x \star \varphi(y) &= \varphi(\varphi^{-1}(x) \cdot \varphi^{-1}(\varphi(y))) \\ &= \varphi(\varphi^{-1}(x) \cdot y) \\ &= \varphi(e) \\ &= \varphi(y) \star x \end{aligned}$$
6. Soit $\mathbb{K}$ un sous-corps de $\mathbb{Q}$.
   Alors $0, 1 \in \mathbb{K}$, et par stabilité par addition, $\mathbb{Z} \subset \mathbb{K}$.
   Par stabilité par division, $\mathbb{Q} \subset \mathbb{K}$, d'où $\mathbb{Q} = \mathbb{K}$.
7. (i) On vérifie que $\mathbb{Z}[i]$ est un sous-anneau de $\mathbb{C}$.
   (ii) Soit $x = a + ib \in \mathbb{Z}[i]$. Si x est inversible dans $\mathbb{Z}[i]$, alors il l'est aussi dans $\mathbb{C}$, et les inverses sont les mêmes :
   $$\begin{aligned} x^{-1} &= \frac{1}{a+ib} \\ &= \frac{a-ib}{a^+b^2} \\ &\in \mathbb{Z}[i] \end{aligned}$$
   D'où
   $$\frac{a}{a^2+b^2} \in \mathbb{Z} \text{ et } \frac{b}{a^2+b^2} \in \mathbb{Z}.$$
   On a donc
   $$\frac{ab}{a^2+b^2}, \text{ or } \left|\frac{ab}{a^2+b^2}\right| \leqslant \frac{1}{2}, \text{ donc } ab = 0.$$
   Si $a = 0$, alors $b = \pm 1$ et si $b = 0$ alors $a = \pm 1$.
   Donc $x = 1, i, -1$ ou $-i$.
   Réciproquement, ces x sont inversibles.
8. Soit $a \in A$ non nul. On pose
   $$\varphi_a : \begin{array}{ccc} A & \longrightarrow & A \\ x & \longmapsto & ax \end{array}.$$
   Alors φ_a est injective, et donc comme A est fini, elle est bijective.

9. (i) Cf. application 3. On a

$$(1-a)^k = \sum_{p=0}^{k} C_k^p (-1)^p a^p$$

Si $k \geqslant n$, alors la somme se limite à $n-1$.

(ii) Supposons que ab est nilpotent : $(ab)^n = 0$.
Alors $b(ab)^n a = 0$ et donc $(ba)^{n+1} = 0$.
Donc ba est nilpotent.

(iii) Soient a et b nilpotents qui commutent : $a^n = b^m = 0$.
Alors

$$\begin{aligned}(a+b)^{n+m} &= \sum_{k=0}^{n+m} C_{n+m}^k a^k b^{n+m-k} \\ &= 0\end{aligned}$$

car pour k de 0 à $n-1$, $b^{n+m-k} = 0$ et pour k de n à m, $a^k = 0$.
Donc, comme la nilpotence passe aussi à l'inverse, l'ensemble des nilpotents de $\mathscr{A}$ est bien un groupe additif.