TD Lois internes et structures algébriques

Groupes et sous-groupes

Exercice 1 Soit $(G, \times)$ un groupe et $g \in G$. Montrer que $\varphi_g : G \to G \quad a \mapsto ag$ est bijective.

Exercice 2 Soit G un groupe, noté multiplicativement. Pour $a \in G$, on note $\langle a \rangle = \{a^n,\ n \in \mathbb{Z}\}$, avec la convention $a^0 = e$. Montrer que $\langle a \rangle$ est un sous-groupe de G, appelé sous-groupe engendré par a.

Exercice 3 Soit G un groupe, noté multiplicativement. On appelle centre de G l'ensemble $Z(G) = \{x \in G \mid \forall y \in G,\ xy = yx\}$. Montrer que $Z(G)$ est un sous-groupe de G.

Exercice 4 Pour $\theta \in \mathbb{R}$, on note $R_\theta = \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix} \in \mathcal{M}_2(\mathbb{R})$.

1. Pour $\theta, \theta' \in \mathbb{R}$, calculer et simplifier le produit $R_\theta R_{\theta'}$. En déduire que R_θ est inversible.
2. Montrer que $\mathcal{R} = \{R_\theta,\ \theta \in \mathbb{R}\}$ forme un groupe pour la multiplication matricielle.

Exercice 5 Soit G un groupe et $(H_n)_{n\in\mathbb{N}}$ une suite de sous-groupes de G.

1. Montrer que
$$H = \bigcap_{n\in\mathbb{N}} H_n$$
est un sous-groupe de G.
2. On suppose que la suite $(H_n)_{n\in\mathbb{N}}$ est croissante pour l'inclusion. Montrer que
$$H = \bigcup_{n\in\mathbb{N}} H_n$$
est un sous-groupe de G.

Exercice 6 Soit $f : \mathbb{R} \to \mathbb{R}$ une fonction périodique.

1. Montrer que l'ensemble des périodes de f est un sous-groupe de $(\mathbb{R}, +)$.
2. ★ Si H est un sous-groupe de $(\mathbb{R}, +)$, construire une fonction dont c'est l'ensemble des périodes

Exercice 7 On dit que $\omega \in \mathbb{U}_n$ est une racine primitive n-ième de l'unité si ω engendre $\mathbb{U}_n$, c'est-à-dire si $\{\omega^k,\ k \in \mathbb{N}\} = \mathbb{U}_n$. Montrer que $\omega = e^{\frac{2ik\pi}{n}}$ est une racine primitive n-ième de l'unité si et seulement si k est premier avec n.

Arithmétique

Exercice 8 Montrer que $7 \mid 2^{333} + 3^{333}$.
Indication : *Que dire des puissances successives de* 2, *et* 3 *modulo* 7 *?*

Exercice 9 Petit théorème de Fermat

1. Soit p un nombre premier et $a \in [\![1, p-1]\!]$.
   (a) Montrer l'existence d'un inverse de a modulo p, c'est-à-dire d'un élément $a^{-1} \in [\![1, p-1]\!]$ tel que $aa^{-1} \equiv 1[p]$.
   (b) Justifier l'existence d'un entier $d \in [\![1, p-1]\!]$ tel que $a^d \equiv 1[p]$.
   Dans la suite, on note d le plus petit tel entier, appelé l'ordre de a modulo p.
   (c) On définit une relation $\sim$ sur $[\![1, p-1]\!]$ en posant
   $$\forall x, y \in [\![1, p-1]\!], \quad x \sim y \Leftrightarrow \exists k \in \mathbb{Z},\ a^k x \equiv y[p].$$
   Montrer que $\sim$ est une relation d'équivalence.
   (d) Pour $x \in [\![1, p-1]\!]$, on note C_x la classe d'équivalence de x. Montrer que $|C_x| = d$.
   (e) En déduire que $a^{p-1} \equiv 1[p]$.
2. ★ Énoncer un analogue du résultat précédent modulo n quelconque.
3. ★ Soit n un entier premier avec 10. Montrer qu'il existe un multiple de n qui ne s'écrit qu'avec le chiffre 1.

Exercice 10 Soit p premier impair.

1. Donner une CNS sur $a \in \mathbb{Z}$ pour que $a \not\equiv -a[p]$. Justifier précisément.
2. On dit que $a \in \mathbb{Z}$ est un carré modulo p si et seulement s'il existe $u \in \mathbb{Z}$ tel que $u^2 \equiv a[p]$. Justifier que si a est un carré modulo p et que $a \not\equiv 0[p]$, alors a admet exactement deux racines carrées.
3. ★ Soit $a \in \mathbb{Z}$ premier avec p et $\overline{a} \in (\mathbb{Z}/p\mathbb{Z})^*$ sa classe et $m = \overline{(p-1)!} \in \mathbb{Z}/p\mathbb{Z}$. En regroupant les termes x et $\frac{\overline{a}}{x}$. Montrer que
$$m = \begin{cases} -\overline{a}^{(p-1)/2} \text{ si } a \text{ est un carré} \\ \overline{a}^{(p-1)/2} \text{ sinon} \end{cases}$$
4. En déduire le théorème de Fermat.

Anneaux

Exercice 11 Montrer que l'ensemble des inversibles d'un anneau forme un groupe.

Exercice 12 🍃 Entiers de Gauss On considère $\mathbb{Z}[i] = \{a + bi,\ a, b \in \mathbb{Z}\} \subset \mathbb{C}$.

1. Montrer que $\mathbb{Z}[i]$ est un sous-anneau de $\mathbb{C}$.
2. Montrer que $\mathbb{Z}[i]^\times = \mathbb{Z}[i] \cap \mathbb{U}$, où $\mathbb{Z}[i]^\times$ est l'ensemble des éléments inversibles de $\mathbb{Z}[i]$.

Exercice 13 Pour $a \in \mathbb{R}_+$, on note $\mathbb{Q}(\sqrt{a}) = \{x + y\sqrt{a},\ x, y \in \mathbb{Q}\}$.

1. Montrer que $\mathbb{Q}(\sqrt{a})$ est un sous-corps de $\mathbb{R}$.
2. Si $\sqrt{a} \notin \mathbb{Q}$, expliciter un isomorphisme d'anneaux de $\mathbb{Q}(\sqrt{a})$ dans lui-même non trivial.
3. Montrer que $\mathbb{Q}(\sqrt{2})$ n'est pas isomorphe à $\mathbb{Q}(\sqrt{3})$.

Exercice 14 ♣ Inversion de Möbius On munit $\mathcal{F}(\mathbb{N}^*, \mathbb{C})$ de l'addition usuelle des fonctions et du produit $f \star g \colon n \mapsto \sum_{d|n} f(d)g(\frac{n}{d})$.

1. Montrer que cela en fait un anneau commutatif.
2. En caractériser les éléments inversibles.
3. Soit μ la fonction associant 0 aux multiples de carrés et $(-1)^r$ à tout entier qui s'écrit $p_1 \dots p_r$, où les p_i sont premiers distincts. Calculer $\mu \star (n \mapsto 1)$ et en déduire que si $\forall n \in \mathbb{N}^*,\ f(n) = \sum_{d|n} g(d)$, alors $\forall n \in \mathbb{N}^*,\ g(n) = \sum_{d|n} \mu(\frac{n}{d}) f(d)$.

Morphismes

Exercice 15 🍃 Soient $(G_1, \times_1)$, $(G_2, \times_2)$ et $(G_3, \times_3)$ trois groupes et $\varphi_1 \colon G_1 \to G_2$ et $\varphi_2 \colon G_2 \to G_3$ deux morphismes de groupes. Montrer que $\varphi_2 \circ \varphi_1$ est un morphisme de groupes.

Exercice 16 Soit $\varphi \colon G \to G'$ un isomorphisme de groupes. Montrer que φ^{-1} est un isomorphisme.

Exercice 17 🍃 Soit $(G_1, \times_1)$, $(G_2, \times_2)$ deux groupes, dont on note e_1 et e_2 les éléments neutres. Soit $f \colon G_1 \to G_2$ un morphisme de groupes.

1. Montrer que si $H_2 \subset G_2$ est un sous-groupe de G_2, $f^{-1}(H_2)$ est un sous-groupe de G_1.
2. Montrer que si $H_1 \subset G_1$ est un sous-groupe de G_1, $f(H_1)$ est un sous-groupe de G_2.

Exercice 18 [Mines 2021] Montrer que les groupes $(\mathbb{Z}, +)$ et $(\mathbb{Q}, +)$ ne sont pas isomorphes.

Sous-groupes de $\mathbb{R}$

Exercice 19 Montrer que $\{2^a 3^b,\ a, b \in \mathbb{Z}\}$ est dense dans $\mathbb{R}_+$.

Exercice 20 ★ Soit $\theta \in \mathbb{R}$. Montrer que $\{e^{in\theta},\ n \in \mathbb{N}\}$ est soit fini, soit dense dans $\mathbb{U}$.

Exercice 21 ★★ Soit $A \subset \mathbb{R}_+$ stable par addition. Montrer l'alternative

(*i*) $\exists a \geq 0,\ A \subset a\mathbb{N}$.

(*ii*) $\forall \varepsilon > 0, \exists M > 0, \forall x \geq M,\ A \cap [x - \varepsilon, x + \varepsilon] \neq \emptyset$.