

TD Lois internes et structures algébriques

K11 Exercice 1 Pour $x, y \in]-1, 1[$, on pose $x \oplus y = \frac{x+y}{1+xy}$. Montrer que $\oplus$ définit une loi interne sur $]-1, 1[$, associative et commutative.

Groupes et sous-groupes

OTL Exercice 2 Soit $(G, \times)$ un groupe et $g \in G$. Montrer que $\varphi_g: G \rightarrow G \quad a \mapsto ag$ est bijective.

BG1 Exercice 3 On travaille dans le groupe $(\mathbb{Z}, +)$.

1. Soit $\alpha \in \mathbb{Z}$. Montrer que $\alpha\mathbb{Z} = \{\alpha k, k \in \mathbb{Z}\}$ est un sous-groupe de $\mathbb{Z}$.
2. Montrer brièvement que si $H \subset (\mathbb{Z}, +)$ est un sous-groupe de $\mathbb{Z}$ et $\alpha \in H$, alors $\alpha\mathbb{Z} \subset H$.
3. On note $\mathcal{H}$ l'ensemble des sous-groupes de $\mathbb{Z}$ qui contiennent α . Montrer que $\bigcap_{H \in \mathcal{H}} H = \alpha\mathbb{Z}$.

5G1 Exercice 4 Soit G un groupe, noté multiplicativement. On appelle centre de G l'ensemble $\mathcal{Z}(G) = \{x \in G \mid \forall y \in G, xy = yx\}$. Montrer que $\mathcal{Z}(G)$ est un sous-groupe de G .

JXU Exercice 5 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.

K61 Exercice 6 Soit $(G, \times)$ un groupe noté multiplicativement 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, c'est-à-dire $\forall n \in \mathbb{N}, H_n \subset H_{n+1}$. Montrer que $H = \bigcup_{n \in \mathbb{N}} H_n$ est un sous-groupe de G .

YMV Exercice 7 Soit $f: \mathbb{R} \rightarrow \mathbb{R}$ 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.

OPK Exercice 8 Soit $A = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, B = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}, X = \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{R}^2 \mid |x| > |y| \right\}, Y = \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{R}^2 \mid |y| > |x| \right\}$ et $E = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$.

1. Montrer que, pour $k \in \mathbb{N}^*$, $A^k Y \subset X$ et que $B^k X \subset Y$.
2. On pose $M_1 = A$ et $M_2 = B$. Pour $\omega \in \{1, 2\}^n$, on pose $\varphi(\omega) = \prod_{k=1}^n M_{\omega_k}$. Montrer que φ est injective. **Ind :** Utiliser E .
3. Plus généralement, montrer que tout produit de n matrices valant chacune soit A , soit B , soit A^{-1} , soit B^{-1} mais sans facteurs A et A^{-1} consécutifs, ni B et B^{-1} , est différent de l'identité. *On dit que le groupe engendré par A et B est libre.*

Arithmétique

BSY Exercice 9 Montrer que $7 \mid 2^{333} + 3^{333}$.

Indication : Que dire des puissances successives de 2, et 3 modulo 7 ?

XVJ Exercice 10 Soit $N = 4444^{4444}$.

1. Pour $n \in \mathbb{N}^*$, on note $s(n)$ la somme des chiffres de n . Montrer que $n \equiv s(n)[9]$.
2. On note A la somme des chiffres de N , B celle de A et C celle de B . Que vaut C ?

5Z0 Exercice 11 PETIT THÉORÈME DE FERMAT

1. Soit p un nombre premier et $a \in \llbracket 1, p-1 \rrbracket$.
 - a) Montrer l'existence d'un inverse de a modulo p , c'est-à-dire d'un élément $a^{-1} \in \llbracket 1, p-1 \rrbracket$ tel que $aa^{-1} \equiv 1[p]$.
 - b) Justifier l'existence de deux entiers distincts $k, \ell \in \mathbb{N}$ tels que $a^k \equiv a^\ell[p]$. En déduire l'existence d'un entier plus petit $d \in \llbracket 1, p-1 \rrbracket$ tel que $a^d \equiv 1[p]$ et que $\{a^k[p], k \in \mathbb{Z}\} = \{a^k[p], k \in \llbracket 0, d-1 \rrbracket\}$.
 - c) On définit une relation $\sim$ sur $\llbracket 1, p-1 \rrbracket$ en posant

$$\forall x, y \in \llbracket 1, p-1 \rrbracket, \quad x \sim y \Leftrightarrow \exists k \in \mathbb{Z}, a^k x \equiv y[p].$$

Montrer que $\sim$ est une relation d'équivalence.

- d) Pour $x \in \llbracket 1, p-1 \rrbracket$, on note C_x la classe d'équivalence de x . Montrer que $|C_x| = d$.
 - e) En déduire que $a^{p-1} \equiv 1[p]$. **Ind :** L'ensemble des classes d'équivalences forme une partition.
2. On note $\varphi(n)$ le nombre d'entiers de $\llbracket 1, n \rrbracket$ qui sont premiers avec n . 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.

C5E Exercice 12 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 $\bar{a} \in (\mathbb{Z}/p\mathbb{Z})^*$ sa classe et $m = \overline{(p-1)!} \in \mathbb{Z}/p\mathbb{Z}$. En regroupant les termes x et $\frac{\bar{a}}{x}$. Montrer que

$$m = \begin{cases} -\bar{a}^{(p-1)/2} & \text{si } a \text{ est un carré} \\ \bar{a}^{(p-1)/2} & \text{sinon} \end{cases}$$

4. En déduire le théorème de Fermat.

Groupes de racines n -ième

P11 Exercice 13 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 $\{\omega^k, k \in \mathbb{N}\} = \mathbb{U}_n$.

1. 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 .
2. Montrer que si n_1, n_2 sont premiers entre eux, le produit d'une racine primitive n_1 -ième et d'une racine primitive n_2 -ième est une racine primitive $n_1 n_2$ -ième de l'unité.
3. ★ Soit H un sous-groupe de $\mathbb{U}_n$.
 - a) Montrer que si H contient une racine primitive n_1 -ième et une racine primitive n_2 -ième, H contient $\mathbb{U}_{\text{ppcm}(n_1, n_2)}$.
 - b) Montrer qu'il existe m tel que $H = \mathbb{U}_m$.

6F1 Exercice 14 ★ Soit p un nombre premier, et $G = \bigcup_{n \in \mathbb{N}} \mathbb{U}_{p^n}$.

1. Montrer que G est sous-groupe de $(\mathbb{C}^*, \times)$.
2. Soit H un sous-groupe propre de G , c'est-à-dire un sous-groupe différent de G . Montrer qu'il existe $n \in \mathbb{N}$ tel que $H = \mathbb{U}_{p^n}$.

Indication : Considérer un élément $z_0 \in G \setminus H$. En déduire qu'il existe $n_0 \in \mathbb{N}$ tel que $H \subset \mathbb{U}_{p^{n_0}}$.

Anneaux

5CS Exercice 15 Montrer que l'ensemble des inversibles d'un anneau forme un groupe.

JTL Exercice 16 ✂ **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 $\mathbb{Z}[i]$.

HZN Exercice 17 ✂ Soit $(A, +, \times)$ un anneau, et $x, y \in A$ deux éléments nilpotents qui commutent.

1. Montrer que le produit xy est nilpotent.
2. Montrer que $x + y$ est nilpotent.

ETL Exercice 18 Pour $a \in \mathbb{Q}_+$, 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-anneau de $\mathbb{R}$, et un sous-corps si $\sqrt{a} \notin \mathbb{Q}$.
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 $\mathbb{Q}(\sqrt{3})$.

XTT Exercice 19 ♣ **INVERSION DE MÖBIUS** On munit $\mathcal{F}(\mathbb{N}^*, \mathbb{C})$ de l'addition usuelle des fonctions et du produit $f \star g : n \mapsto \sum_{d|n} f(d)g(\frac{n}{d})$.

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 $\forall n \in \mathbb{N}^*, g(n) = \sum_{d|n} \mu(\frac{n}{d})f(d)$.

Ind : La partie la plus subtile est l'associativité.

Morphismes

ADS Exercice 20 ✂

1. Soient $(G_1, \times_1), (G_2, \times_2)$ et $(G_3, \times_3)$ trois groupes et $\varphi_1 : G_1 \rightarrow G_2$ et $\varphi_2 : G_2 \rightarrow G_3$ deux morphismes de groupes. Montrer que $\varphi_2 \circ \varphi_1$ est un morphisme de groupes.
2. Soit $\varphi : G \rightarrow G'$ un isomorphisme de groupes. Montrer que φ^{-1} est un isomorphisme de groupes.

9ZB Exercice 21 ✂ Soit $(G_1, \times_1), (G_2, \times_2)$ deux groupes, dont on note e_1 et e_2 les éléments neutres. Soit $f : G_1 \rightarrow G_2$ 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 .

FDS Exercice 22 [ORAL MINES]

1. Montrer que les groupes $(\mathbb{Z}, +)$ et $(\mathbb{Q}, +)$ ne sont pas isomorphes.
2. ★ Montrer que les groupes $(\mathbb{Q}, +)$ et $(\mathbb{Q}^*, \times)$ ne sont pas isomorphes.

Sous-groupes de $\mathbb{R}$

P61 Exercice 23 Montrer que $\{2^a 3^b, a, b \in \mathbb{Z}\}$ est dense dans $\mathbb{R}_+$.

IG5 Exercice 24 ★ Soit $\theta \in \mathbb{R}$. Montrer que $\{e^{in\theta}, n \in \mathbb{N}\}$ est soit fini, soit dense dans $\mathbb{U}$.

Indication : Introduire un certain sous-groupe de $\mathbb{R}$, engendré par θ et 2π .

BQ8 Exercice 25 ★ ★ Soit $A \subset \mathbb{R}_+$ stable par addition. Montrer l'alternative

- (i) $\exists a \geq 0, A \subset a\mathbb{N}$.
- (ii) $\forall \varepsilon > 0, \exists M > 0, \forall x \geq M, A \cap [x - \varepsilon, x + \varepsilon] \neq \emptyset$.