Chapitre 1 : Groupes, anneaux : Rappels et complèments

Exercice 1 [id=665]

1 Pour tout $(x, y) \in \mathbb{Z}^2$, on pose $x \perp y = x + y + 1$.

(a) Montrer que $(\mathbb{Z}, \perp)$ est un groupe commutatif.

(b) Montrer que les groupes $(\mathbb{Z}, \perp)$ et $(\mathbb{Z}, +)$ sont isomorphes ?

(c) Retrouver l'élément neutre de $(\mathbb{Z}, \perp)$ et le symétrique de 2025 dans $(\mathbb{Z}, \perp)$ en utilisant l'isomorphisme.

2 Pour tout $(x, y) \in \mathbb{Z}^2$, on pose $x \star y = x + (-1)^x y$.

(a) Montrer que $(\mathbb{Z}, \star)$ est un groupe.

(b) Les groupes $(\mathbb{Z}, \star)$ et $(\mathbb{Z}, \perp)$ sont-ils somorphes ?

Exercice 2 [id=501]

Soit $A \in \mathcal{M}_n(\mathbb{R})$. Etablir que les assertions suivantes sont équivalentes :
(i) Il existe une partie $\mathcal{G}$ de $\mathcal{M}_n(\mathbb{R})$ stable par le produit des matrices tel que $(\mathcal{G}, \circ)$ est un groupe et $A \in \mathcal{G}$.
(ii) $\text{rg}\,(A) = \text{rg}\,(A^2)$
(iii) $\ker(A) = \ker(A^2)$
(iv) $\text{Im}(A) \oplus \ker(A) = \mathbb{R}^n$
(v) $\exists B \in \mathcal{M}_n(\mathbb{R}), AB = BA$ et $A^2B = A$ et $B^2A = B$.

Exercice 3 [id=666]

Soit $A = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \in \mathcal{M}_2(\mathbb{R})$ et $G = \{xA / x \in \mathbb{R}^*\}$.

1 Démontrer que G est stable par la multiplication des matrices carrées.

2 Démontrer que $(G, \times)$ est un groupe commutatif. Préciser l'élément neutre E de $(G, \times)$ et pour tout $M = xA \in G$ préciser M' le symétrique de M.

3 Démontrer que les groupes $(G, \times)$ et $(\mathbb{R}^*, \times)$ sont isomorphes.

Exercice 4 [id=11]

Soit G un groupe additif et $f : G \to G'$ un morphisme de groupes.

1 Montrer que pour tout sous-groupe H de G, on a $f^{-1}(f(H)) = H + \ker(f)$

2 Montrer que pour tout sous-groupe H' de G', on a $f(f^{-1}(H')) = H' \cap \text{Im}(f)$

Exercice 5 [id=667]

Pour tout $x \in \mathbb{R}^*$, on note M_x la matrice de $\mathcal{M}_2(\mathbb{R})$ tel que

$$M_x = \begin{pmatrix} 0 & x \\ \frac{1}{x} & 0 \end{pmatrix}.$$

1 Calculer $M_x M_y$ pour tout $x, y \in \mathbb{R}^*$.

2 Démontrer que pour tout $x \in \mathbb{R}^*$, la matrice M_x est d'ordre fini d dans le groupe $\mathbf{GL}_2(\mathbb{R})$, determiner d.

3 Donner un exemple de matrices A et B de $\mathbf{GL}_2(\mathbb{R})$ tel que A et B d'ordres finis et AB n'est pas d'ordre fini.

Exercice 6 [id=19]

1)Soient (G_1, T) et $(G_2, *)$ deux groupe. On note $G = G_1 \times G_2$ et pour tout $x = (x_1, x_2)$ et $y = (y_1, y_2)$ de G, on pose $x \perp y = (x_1 T y_1, x_2 * y_2)$. Démontrer que $(G, \perp)$ est un groupe et préciser eon élément neutre et le symétrique de chaque élément
2) Démontrer que les groupes additifs $G = (\mathbb{Z}/4\mathbb{Z}, +)$ et $G' = ((\mathbb{Z}/2\mathbb{Z})^2, +)$ ne sont pas isomorphes.

Exercice 7 [id=26]

1 Démontrer que le groupe $(\mathbb{Z}^2, +)$ n'est pas monogène.

2 Démontrer que le groupe $(\mathbb{Z}^2, +)$ admet une partie génératrice à deux éléments.

3 Soit $(a, b), (c, d) \in \mathbb{Z}^2$. A quelle condition sur a, b, c, d, on a $\mathbb{Z}^2 = \langle (a, b), (c, d) \rangle$?

Exercice 8 [id=27]

1 Soit $(G, .)$ un groupe et $a, b \in G$ tel que $ab = ba$ et ordre$(a) = m$ et ordre$(b) = n$ et $m \wedge n = 1$. Démontrer que ordre$(ab) = mn$.

2 Soient G_1 et G_2 deux groupes cycliques tel que card$(G_1) = m$ et card$(G_2) = n$. Démontrer que si $n \wedge m = 1$ alors $G_1 \times G_2$ est cyclique et si $G_1 = \langle a_1 \rangle$ et $G_2 = \langle a_2 \rangle$ alors $G_1 \times G_2 = \langle (a_1, a_2) \rangle$

Exercice 9 [id=32]

1 Soit $(G, .)$ un groupe tel que

$$(\star) \quad \forall x \in G, x^2 = e.$$

Démontrer que G est commutatif.

2 Donner des exemples de groupe G vérifiant la condition $(\star)$ dans les cas :

(a) G fini.

(b) G infini.

3 Démontrer que si G est un groupe fini qui vérifie la condition $(\star)$ ci-dessus alors il existe $m \in \mathbb{N}$ tel que $\text{card}(G) = 2^m$.

Exercice 10 [id=35]

Démontrer que tout sous-groupe de $(\mathbb{Z}, +)$ est de la forme $n\mathbb{Z}$ avec $n \in \mathbb{N}$.

Exercice 11 [id=38]

Soient H et K deux sous-groupes d'un groupe $(G, \star)$.
A quelle condition l'ensemble $H \cup K$ est-il un sous-groupe de $(G, \star)$?

Exercice 12 [id=39]

Dans chacun des cas ci-dessous, déterminer le nombre de lois de composition internes sur G et le nombre maximale de celles d'entre elles qui fait de G un groupe :

1 $G = \{a\}$ est un singleton

2 $G = \{a, b\}$ est une paire

3 $G = \{a, b, c\}$ est un ensemble à trois éléments.

Exercice 13 [id=40]

G désigne le groupe additif $\mathbb{Z}/12\mathbb{Z}$.

1 Préciser les générateurs de G.

2 Sans faire des calculs, quels sont les ordres possibles des éléments de G ?

3 Dresser le tableau donnant les ordres des éléments de G et expliciter le sous-groupe engendré par chaque élément de G.

4 Monter que si A est l'ensemble des générateurs de G alors $(A, \times)$ est un groupe isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Exercice 14 [id=41]

Pour tout $n \in \mathbb{N}^*$, on pose : $\mathbb{U}_n = \{z \in \mathbb{C}/z^n = 1\}$ et soit $G = \bigcup_{n \in \mathbb{N}^*} \mathbb{U}_n$

1 Prouver que $\mathbb{U}_n$ est un sous-groupe de $(\mathbb{C}^*, \times)$, pour tout $n \in \mathbb{N}^*$.

2 Démontrer que G est un sous-groupe infini de $(\mathbb{C}^*, \times)$, dans lequel tout élément est d'ordre fini.

3 Donner un exemple de groupe G infini dans lequel tout élément différent de l'élément neutre est d'ordre 2.

Exercice 15 [id=42]

Soit n un entier naturel tel que $n \geq 2$.On appelle matrice de transvection de $\mathcal{M}_n(\mathbb{K})$, toute matrice de $\mathcal{M}_n(\mathbb{K})$ de la forme $T_{i,j,a} = I_n + aE_{i,j}$ où $i, j \in [\![1, n]\!]$ et $i \neq j$. On note $\mathscr{T}$ l'ensemble de telles matrices

1 Est ce que $\mathscr{T}$ est un sous-groupe de $GL_n(\mathbb{K})$?

2 Même question pour $\mathscr{T}_{ij} = \{T_{i,j,a} / a \in \mathbb{K}\}$ pour $(i, j) \in [\![1, n]\!]^2$ fixé tel que $i \neq j$

Exercice 16 [id=43]

1 Soit $(G, \perp)$ un groupe et $\top$ la loi de composition interne définie par :

$$\forall (x, y) \in G^2, x \top y = y \perp x$$

Montrer que $(G, \top)$ est un groupe isomorphe au groupe $(G, \perp)$.

2 Determiner tous les morphismes de groupe de $(\mathbb{Z}/4\mathbb{Z}, +)$ vers $(\mathbb{Z}/6\mathbb{Z}, +)$.

3 Soit $n \in \mathbb{N}^*$. Déterminer tous les morphismes de groupe de $(\mathscr{S}_n, \circ)$ vers $(\mathbb{C}^*, \times)$.

Exercice 17 [id=44]

1 Soit $(G, \star)$ un groupe. Démontrer qu'il existe un morphisme injectif Φ, de $(G, \star)$ vers $(\mathscr{S}(G), \circ)$ où $(\mathscr{S}(G), \circ)$ est le groupe des bijections de G vers G pour la composition des applications.

2 Précise les cas où Φ est un isomoprphisme.

Exercice 18 [id=45]

Donner un exemple de groupe(non trivial) où :

1 Tout élément est d'ordre fini.

2 Aucun élément différent de l'élément neutre n'est d'ordre fini.

3 Il y'a en même temps des éléments différents de l'élément neutre, d'ordres finis et d'autres qui ne sont pas d'ordre fini.

4 G est infini et tout élément est d'ordre fini.

5 G est infini et tous les éléments différents de l'élément neutre sont d'ordre fini et ont le même ordre.

Exercice 19 [id=46]

Soit $(G,.)$ un groupe et pour tout $a \in G$, on note φ_a l'application :

$$\varphi_a : G \to G; x \mapsto \varphi_a(x) = axa^{-1}$$

et

$$C_a = \{x \in G / xa = ax\}.$$

On note : $\mathscr{S}(G)$ le groupe des bijections de G vers G, $\mathrm{Aut}(G)$ l'ensemble des automorphismes de G ,

$$\mathrm{Int}(G) = \{\varphi_a / a \in G\}$$

et

$$Z(G) = \{x \in G / \forall g \in G, xg = gx\},$$

appelé le centre de G.

1 (a) Montrer que pour tout $a \in G$, C_a est un sous-groupe de G.

(b) En déduire que $Z(G)$ est un sous-groupe de G.

(c) Soit $g \in G$. On pose

$$gZ(G)g^{-1} = \{gxg^{-1} / x \in Z(G)\}.$$

Prouver que $gZ(G)g^{-1} = Z(G)$.

2 Démontrer que $\mathrm{Aut}(G)$ est un sous-groupe de $(\mathscr{S}(G), \circ)$ et que $\mathrm{Int}(G)$ est un sous-groupe de $(\mathrm{Aut}(G), \circ)$.

3 Démontrer que $\Phi : G \to \mathscr{S}(G); x \mapsto \Phi(x) = \varphi_x$ est un morphisme et préciser son image et son noyau.

4 **Exemple de détermination du centre d'un groupe :**
Démontrer que $Z(\mathbf{GL}_2(\mathbb{R})) = \mathbb{R}I_2$.

Exercice 20 [id=47]

Soit G un groupe fini de cardinal n et $k \in \mathbb{N}$. On considère l'application :

$$\varphi_k : G \to G; x \mapsto x^k$$

1 Démontrer que si le groupe G est commutatif alors φ_k est un morphisme, et que φ_k est un isomorphisme si et seulement si $k \wedge n = 1$.

2 Donner un exemple de groupe G de cardinal n et d'entier naturel k tel que $k \wedge n = 1$ et φ_k n'est pas un morphisme.

Exercice 21 [id=48]

1 Soit H un sous-groupe additif de $\mathbb{R}$. Prouver que soit H est de la forme $H = \omega\mathbb{Z}$ avec $\omega \in \mathbb{R}_+$ (on dit que H est discret), soit H est partout dense dans $\mathbb{R}$.

2 Soit $H = a\mathbb{Z} + b\mathbb{Z}$ où $a, b \in \mathbb{R}$ et $b \neq 0$. Montrer que H est discret si et seulement si $\frac{a}{b} \in \mathbb{Q}$.

3 Démontrer que pour tout $(x, y) \in [-1, 1]^2$, tel que $x < y$, il existe au moins un entier

naturel n tel que $x < \cos n < y$.

Exercice 22 [id=49]

G est un groupe multiplicatif. Soient H et K deux sous-groupes de G et on note

$$HK = \{hk/(h,k) \in H \times K\}.$$

1 Démontrer que les assertions suivantes sont équivalentes :
(i) $HK \subset KH$
(ii) $KH \subset HK$
(iii) $HK = KH$
(iv) HK est un sous-groupe de G.

2 En considérant le groupe symétrique $\mathscr{S}_3$, donner un contre exemple où HK n'est pas un sous-groupe.

Exercice 23 [id=50]

Soit $(G, \star)$ un magma tel que G est fini et $\star$ est associative et tout élément est régulier dans $(G, \star)$. Démontrer que $(G, \star)$ est un groupe.

Exercice 24 [id=51]

Soit G un groupe de cardinal p avec p un entier naturel premier. Démontrer que G est cyclique.

Exercice 25 [id=52]

1 Démontrer que les groupes $G_1 = \mathbb{Z}/4\mathbb{Z}$ et $G_2 = (\mathbb{Z}/2\mathbb{Z})^2$ ne sont pas isomorphes.

2 Démontrer que tout groupe H de cardinal 4 est isomorphe à G_1 ou G_2.

Exercice 26 [id=53]

On rappelle que pour tout $n \in \mathbb{N}$ tel que $n \geq 2$, le groupe symétrique $\mathscr{S}_n$ est engendré par les transpositions.

1 Soit $\sigma \in \mathscr{S}_n$. Démontrer que pour toute transposition $\tau_{i,j}$ de $\mathscr{S}_n$, on a

$$\sigma\tau_{i,j}\sigma^{-1} = \tau_{\sigma(i),\sigma(j)}$$

2 (a) Prouver que les transpositions de la forme $\tau_{1,k}, 2 \leq k \leq n$ engendrent $\mathscr{S}_n$.

(b) Même question pour les transpositions de la forme $\tau_{k,k+1}, 1 \leq k \leq n-1$,

(c) Montrer que $\mathscr{S}_n$ est engendré par le cycle : $s = (1, 2, \cdots, n)$ et la transposition $\tau = (1, 2)$.
Indication : Considérer pour tout $k \in [\![1, n]\!]$, le composé : $s^k \tau s^{-k}$.

3 Déterminer tous les morphismes de groupe de $(\mathscr{S}_n, \circ)$ vers $(\mathbb{C}^*, \times)$.

Exercice 27 [id=54]

On considère les matrices carrées de $\mathbf{GL}_2(\mathbb{R})$ suivantes : $R = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ et $S = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ et soit $G = \langle R, S \rangle$ le sous-groupe de $\mathbf{GL}_2(\mathbb{R})$ engendré par $\{R, S\}$ et $H = \langle A \rangle$ le sous-groupe engendré par R.
1) Démontrer que $\langle R \rangle$ est cyclique de cardinal 4 et que tout élément de G est de la forme $\prod_{k=1}^{m} M_k$ avec $m \in \mathbb{N}^*$ et pour tout $k \in [\![1, m]\!]$, $M_k \in \{R, R^3, S\}$
2) Démontrer que $\forall p \in \mathbb{Z}, \exists q \in \mathbb{Z}, R^p S = S R^q$.
3) En déduire que $\text{card}(G) = 8$ et préciser les éléments de G.
4) Dans le groupe symétrique $\mathscr{S}_4$, on considère le cycle $s = (1, 2, 3, 4)$ et la permutation $t = (1, 2) \circ (3, 4)$ produit des transpositions $(1, 2)$ et $(3, 4)$. Démontrer que $G \simeq \langle s, t \rangle$.

Exercice 28 [id=55]

1 Démontrer que le groupe $(\mathbb{Z}^2, +)$ n'est pas monogène.

2 Soit A une partie finie de $\mathbb{Q}$. Démontrer que le sous-groupe $\langle A \rangle$ du groupe additif $(\mathbb{Q}, +)$ engendré par A est *strictement* inclus dans $\mathbb{Q}$.

Exercice 29 [id=56]

Soit $A = \{m + n\sqrt{2} / m, n \in \mathbb{Z}\}$.

1 Prouver que A est un sous-anneau de $(\mathbb{R}, +, \times)$. On note $U(A)$ le groupe des inversibles de A.

2 Pour tout $x = m + n\sqrt{2} \in A$, on pose $N(x) = |m^2 - 2n^2|$. Démontrer que pour tout $x, y \in A$, on a $N(xy) = N(x)N(y)$.

3 Démontrer que $U(A) = \{\varepsilon(1 + \sqrt{2})^n / \varepsilon \in \{-1, 1\}, n \in \mathbb{Z}\}$.

Exercice 30 [id=57]

Soit A un anneau commutatif non réduit à un singleton et on note $\mathscr{U}(A)$ le groupe des inversibles de A.
1) Démontrer que si I est un idéal de A tel que $I \cap \mathscr{U}(A) \neq \emptyset$ alors $I = A$.
2) Montrer que si les seuls idéaux de A sont A et $\{0_A\}$ alors A est un corps.
3) Montrer que si A est intègre et n'admet qu'un nombre fini d'idéaux alors A est un corps.

Exercice 31 [id=58]

1 Prouver que le groupe additif $\mathbb{Z}^2$ n'est pas monogène.

2 Démontrer que si A est une partie finie de $\mathbb{Q}$ alors le groupe $\langle A\rangle$ engendré par A est strictement inclus dans $\mathbb{Q}$.

3 Soit $A=\left\{\frac{1}{p^\alpha}/p\in\mathbb{P},\alpha\in\mathbb{N}\right\}$ où $\mathbb{P}$ est l'ensemble des nombres premiers positifs. Démontrer que $\langle A\rangle=\mathbb{Q}$.

Exercice 32 [id=59]

Soit G un groupe. On considère deux éléments a et b de G d'ordres respectifs p et q et on suppose de plus que $ab=ba$ et $p\wedge q=1$. Démontrer que ab est d'ordre pq.

Exercice 33 [id=60]

Soit E un ensemble non vide et $\star$ une loi de composition interne associative et admettant un élément neutre e (on dit que $(E,\star)$ est un monoïde). Pour tout élément a de E et tout entier naturel n non nul, on note :

$$a^n=\underbrace{a\star\cdots\star a}_{n\text{ fois}}$$

1 Donner un exemple de monoïde fini qui n'est pas un groupe.

2 Démontrer que si $(G,\star)$ est un groupe fini alors on a :

$$(1):\quad \forall x\in G,\forall\nu\in\mathbb{N},\exists p\in\mathbb{N},\left\{\begin{array}{l}p\geq\nu\\x^p=x\end{array}\right.$$

3 Démontrer que (1) peut ne pas être vrai si on suppose juste que $(G,\star)$ est un monoïde fini(on pourra donner un contre-exemple).

4 Soit M un ensemble non vide et $\star$ une loi de composition interne sur M (On dit que $(M,\star)$ est un magma). On suppose que M est fini et que la loi $\star$ est associative. Démontrer que :

$$(2):\quad \exists x\in M,\forall p\in\mathbb{N}^*,x^p=x$$

Exercice 34 [id=61]

Determiner tous les morphismes du groupe $\mathscr{S}_n$ vers le groupe $\mathbb{C}^*$

Exercice 35 [id=62]

Soit $m,n\in\mathbb{N}^*$. Déterminer tous les morphismes de $(\mathbb{Z}/n\mathbb{Z},+)$ vers $(\mathbb{Z}/m\mathbb{Z},+)$, et notamment leur nombre.

Exercice 36 [id=63]

$\mathcal{M}_2(\mathbb{R})$ designe l'ensemble des matrices carrées à coefficients réels. On rappelle que $\mathbf{GL}_2(\mathbb{R}) = \{A \in \mathcal{M}_2(\mathbb{R}) / \det(A) \neq 0\}$ et on note $\mathbf{SL}_2(\mathbb{R}) = \{A \in \mathbf{GL}_2(\mathbb{R}) / \det(A) = 1\}$. Pour tout nombre réel α, on note $\Gamma_\alpha = \begin{pmatrix} 1 & 0 \\ \alpha & 1 \end{pmatrix}$ et $\Lambda_\alpha = \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}$. On appelle matrice de transvection de $\mathcal{M}_2(\mathbb{R})$, toute matrice de la forme Γ_α ou Λ_α avec $\alpha \in \mathbb{R}$.

1 Soit $\gamma \in \mathbb{R}$ tel que $\gamma(\gamma - 1) \neq 0$. On pose $M_\gamma = \begin{pmatrix} \gamma^{-1} & 0 \\ 0 & \gamma \end{pmatrix}$.

(a) Démontrer que M_γ ne peut être produit de m matrices de transvection pour tout $m \in \mathbb{N}^*$ tel que $m \leq 3$.

(b) Démontrer que M_γ est un produit de matrices de transvections.

2 Soit $A = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$ une matrice de $\mathbf{GL}_2(\mathbb{R})$ tel que $a \neq 0$ et $ad - bc = 1$.

(a) Soit $A_1 = \begin{pmatrix} a_1 & c_1 \\ b_1 & d_1 \end{pmatrix}$ la matrice obtenue à partir de A par l'opération élémentaire $L_2 \leftarrow L_2 - \frac{b}{a} L_1$. Démontrer qu'il existe une matrice de transvection T_1 à préciser tel que $A_1 = T_1 A$.

(b) Démontrer que si la matrice A_2 est celle obtenue à partir de A_1 par l'opération élémentaire $C_2 \leftarrow C_2 - \frac{c}{a} C_1$ alors il existe une matrice de transvection T_2 tel que $A_2 = A_1 T_1$.

3 Déduire de tout ce qui précéde que toute matrice $A \in \mathbf{SL}_2(\mathbb{R})$ est un produit de matrices de transvections.

Exercice 37 [id=64]

Si X est une partie de $\mathbb{Q}$, on note $\langle X \rangle$, le sous-groupe de $(\mathbb{Q}, +)$ engendré par X.
Soit A une partie de $\mathbb{Q}$ tel que

$$\langle A \rangle = \mathbb{Q}.$$

Démontrer que :

$$\forall a \in A, \quad \langle A \backslash \{a\} \rangle = \mathbb{Q}.$$

Exercice 38 [id=65]

n est un entier naturel tel que $n \geq 2$ et $\mathfrak{S}_n$ le groupe symetrique. On considère deux transpositions t et τ éléments de $\mathfrak{S}_n$ et soit $\sigma = t \circ \tau$. Quelles sont les valeurs possibles de l'ordre de la permutation σ ?

Exercice 39 [id=66]

Soit G un groupe et H un sous-groupe de G tel que H est strictement inclus dans G. On pose $A = G \backslash H$. Démontrer que $\langle A \rangle = G$

Exercice 40 [id=67]

Soit $(A,+,\times)$ un anneau. On note 0_A et 1_A respectivement, l'élément neutre de la première et la deuxiéme loi de A. Un élément x de A est dit nilpotent s'il existe $k \in \mathbb{N}^*$ tel que $x^k = 0_A$. On appelle indice de nilpotence de x, l'entier naturel $\nu = \min\{k \in \mathbb{N}^* / x^k = 0_A\}$.

1 Démontrer que pour tout élément nilpotent x de A, d'indice de nilpotence ν, on a $1-x$ est inversible et exprimer son inverse $(1-x)^{-1}$ en fonction de x et ν.

2 Démontrer que si a et b sont deux éléments nilpotents de A tel que $ab = ba$, il en est de même de $a+b$ et ab.

3 Démontrer que si A est commutatif l'ensemble $\mathscr{N}(A)$ des éléments nilpotents de A est un idéal de A.

Exercice 41 [id=68]

Soit $(A,+,\times)$ un ensemble non vide tel que tous les axiomes d'un anneau sont satisfait sauf celui de la commutativité de la première loi $+$. Démontrer que $(A,+,\times)$ est tout de même un anneau.

Exercice 42 [id=69]

Soit A un anneau et x un élément de A.

1 Démontrer que si x est inversible à gauche et régulier à droite. Démontrer que x est inversible.

2 Démontrer que s'il existe $n \in \mathbb{N}^*$ tel que x^n est inversible alors x est inversible.

Exercice 43 [id=70]

1 Démontrer qu'il existe au moins un corps $\mathbb{K}$ ayant quatre éléments.

2 Pour tout $x = (x_1, x_2) \in (\mathbb{Z}/2\mathbb{Z})^2$ et $y = (y_1, y_2) \in (\mathbb{Z}/2\mathbb{Z})^2$, on pose $x \otimes y = (x_1y_1, x_1y_2 + x_2y_1)$. Démontrer que $((\mathbb{Z}/2\mathbb{Z})^2, +, \otimes)$ est un anneau.

3 Démontrer qu'il y'a au moins quatre anneaux non isomorphes à quatre éléments.

Exercice 44 [id=71]

On note :

$$\mathcal{A} = \left\{ \begin{pmatrix} a & c \\ b & d \end{pmatrix} \in \mathcal{M}_2(\mathbb{R}) / a+b = c+d \right\}.$$

Démontrer que $\mathcal{A}$ est un sous-anneau de $\mathcal{M}_2(\mathbb{R})$ isomorphe au sous-anneau $\mathcal{T}(\mathbb{R})$ des matrices triangulaires inférieures de $\mathcal{M}_2(\mathbb{R})$.

Exercice 45 [id=72]

Soit A un anneau et u et v deux éléments de A tel que $Au = Av$. Démontrer qu'il existe une et une seule application $f : uA \to vA$ telle que :

$$\begin{cases} f(u) = v \\ \forall (x,y) \in (uA)^2, \forall (\lambda,\mu) \in A^2, \quad f(x\lambda + y\mu) = f(x)\lambda + f(y)\mu \end{cases}.$$

Exercice 46 [id=73]

Soit $\mathbb{Z}(i) = \left\{a + ib \mid (a,b) \in \mathbb{Z}^2\right\} \cdot \mathbb{Z}(i)$ est un anneau. On pose :

$$N(a+ib) = a^2 + b^2$$

1 Montrer que :

$$\forall (x,y) \in \mathbb{Z}(i)^2, \quad N(xy) = N(x)N(y).$$

En déduire les éléments inversibles de $\mathbb{Z}(i)$.

2 Si $x \in \mathbb{Z}(i)$ et si $N(x)$ est un entier premier, montrer que x est irréductible (i.e. $x = \alpha.\beta \Rightarrow \alpha$ ou β inversible). La réciproque est-elle vraie ?

3 **Division euclidienne dans $\mathbb{Z}(i)$:**
Soient $x \in \mathbb{Z}(i), y \in \mathbb{Z}(i)^*$. On pose $\frac{x}{y} = u + iv$, où $(u,v) \in \mathbb{Q}^2$. On prend $(u_0, v_0) \in \mathbb{Z}^2$ tel que $|u - u_0| \leqslant \frac{1}{2}$ et $|v - v_0| \leqslant \frac{1}{2}$. Montrer qu'on a : $x = y\,(u_0 + iv_0) + r$ avec $N(r) < N(y)$. Dans quel cas $u_0 + iv_0$ et r sont-ils uniques ?

4 En déduire que $\mathbb{Z}(i)$ est principal.

5 Soit p un nombre premier dans $\mathbb{Z}$. Montrer que p est irréductible ssi il n'existe pas $(a,b) \in \mathbb{N}^2$ tel que $p = a^2 + b^2$

6 Montrer que si p est un nombre premier tel que $p \equiv 3 (\mathrm{mod} 4)$, alors

$$a^2 + b^2 \equiv 0 (\mathrm{mod} p) \Rightarrow a \equiv 0 (\mathrm{mod} p) \text{ et } b \equiv 0 (\mathrm{mod} p)$$

En déduire que tout nombre premier $\geqslant 3$ est irréductible dans $\mathbb{Z}(i)$ ssi $p \equiv 3 (\mathrm{mod} 4)$.

7 Montrer q'un entier n peut se mettre sous la forme d'une somme de 2 carrés ssi il est de la forme :

$$n = \left(\prod_j p_j^{\alpha_j}\right)\left(\prod_{4k+3 \text{ premier}} (4k+3)^{2\beta_k}\right)$$

où p_j est un nombre premier tel que $p_j \not\equiv 3 (\mathrm{mod} 4)$, i.e. les exposants des facteurs premiers de la forme $4k+3$ sont pairs.

8 Donner une C.N.S. pour que $x \in \mathbb{Z}(i)$ soit irréductible.

Exercice 47 [id=74]

Soit $G = \langle \omega \rangle$ un groupe cyclique de cardinal n. Pour tout diviseur d de n on note $\tilde{d}$ l'unique entier naturel tel que $d\tilde{d} = n$ et on note $\omega_d = \omega^{\tilde{d}}$ et $G_d = \{x \in G / x^d = e\}$.

1 Démontrer que pour tout diviseur d de n, l'ordre de ω_d est égal à d et que G admet au moins un sous-groupe H de cardinal d.

2 Démontrer que si H est un sous-groupe de G alors H est cyclique et $d = |H|$ divise n.

3 Démontrer que pour tout diviseur d de n, on a G_d est un sous-groupe de G, et en déduire qu' il existe un seul sous-groupe H de G de cardinal d et expliciter un générateur de H en fonction de a, n et d.

Exercice 48 [id=75]

On considère deux groupes monogènes G_1 et G_2 dont les lois sont notées multiplicativement et les éléments neutres respectifs sont notés e_1 et e_2.

1 On suppose de plus que $G_1 \neq \{e_1\}$ et $G_2 \neq \{e_2\}$. Démontrer que si $G_1 \times G_2$ est monogène alors G_1 et G_2 sont cycliques.

2 On suppose que G_1 et G_2 sont cycliques de cardinaux respectifs n_1 et n_2. Démontrer que $G_1 \times G_2$ est cyclique si et seulement si $n_1 \wedge n_2 = 1$.

Exercice 49 [id=76]

1 Soit x un entier relatif impair. Démontrer que :

$$\forall n \in \mathbb{N} \quad n \geq 3 \Rightarrow x^{2^{n-2}} \equiv 1\ [2^n]$$

2 Démontrer que pour tout $n \in \mathbb{N}$ tel que $n \geq 3$, le groupe $\mathscr{U}(\mathbb{Z}/2^n\mathbb{Z})$ des inversibles de l'anneau $\mathbb{Z}/2^n\mathbb{Z}$ n'est pas cyclique.

Exercice 50 [id=77]

Pour toute partie A de $\mathbb{C}$, et tout sous-corps $\mathbb{K}$ de $\mathbb{C}$, on note $\mathbb{K}(A)$ le plus petit sous-corps $\mathbb{L}$ de $\mathbb{C}$ tel que $A \subset \mathbb{L}$ et $\mathbb{K} \subset \mathbb{L}$. Si A est finie non vide, $A = \{x_1, \ldots, x_n\}$ on notera $\mathbb{K}(x_1, \ldots, x_n)$ au lieu de $\mathbb{K}(A)$.

1 Démontrer que $\mathbb{Q}(\sqrt{2}) = \mathbb{Q} + \mathbb{Q}\sqrt{2}$ et que $\mathbb{Q}(\sqrt{2})(\sqrt{3}) = \mathbb{Q}(\sqrt{2}) + \mathbb{Q}(\sqrt{2})\sqrt{3}$.

2 Démontrer que $\mathbb{Q}(\sqrt{2})(\sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.

3 Démontrer que $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q} + \mathbb{Q}\sqrt{2} + \mathbb{Q}\sqrt{3} + \mathbb{Q}\sqrt{6}$

4 Soit $\theta = \sqrt{2} + \sqrt{3}$.

(a) Démontrer que $\mathfrak{I}_\theta = \{P \in \mathbb{Q}[X] / P(\theta) = 0\}$ est un idéal non nul de $\mathbb{Q}[X]$. En déduire qu'il existe un unique polynôme unitaire $\pi_\theta \in \mathbb{Q}[X]$ tel que $\mathfrak{I}_\theta = \pi_\theta \mathbb{Q}[X]$.

(b) Démontrer que π_θ est irréductible dans $\mathbb{Q}[X]$. En déduire que la famille $(1, \theta, \theta^2, \theta^3)$ est libre dans le $\mathbb{Q}-$ espace vectoriel $\mathbb{R}$

(c) Démontrer que :

$$\mathbb{Q}(\theta) = \mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q} + \mathbb{Q}\theta + \mathbb{Q}\theta^2 + \mathbb{Q}\theta^3.$$

Exercice 51 [id=466]

Trouver tous les sous-groupes de $\mathbb{Z}/12\mathbb{Z}$. Soignez vos réponses

Exercice 52 [id=472]

Soit $f : \mathbb{R} \to \mathbb{R}$ un morphisme d'anneaux non nul.

1 Calculer $f(0), f(1), f(n)$ pour tout $n \in \mathbb{N}$, puis $\mathbb{Z}$, puis $\mathbb{Q}$.

2 Montrer que $x \geqslant 0$ entraîne $f(x) \geqslant 0$ (dans $\mathbb{R}$, tout positif est un carré).

3 En déduire f croissante, puis $f = \mathrm{id}_{\mathbb{R}}$.

Exercice 53 [id=491]

Soit G une partie de $\mathcal{M}_n(\mathbb{R})$ non réduite à la matrice nulle. On suppose que $(G, \times)$ est un groupe. Montrer qu'il existe $r \in \mathbb{N}^*$ tel que le groupe $(G, \times)$ soit isomorphe à un sous-groupe de $(\mathrm{GL}_r(\mathbb{R}), \times)$

Exercice 54 [id=504]

Soient $\mathbb{K}$ un corps et

$$f(X) = \frac{(1+X)\left(1+X^{15}\right)}{(1+X^3)(1+X^5)}$$

1 Montrer que $f(X) \in \mathbb{K}[X]$.

2 En calculant modulo X^9, montrer que

$$f(X) = X^8 + X^7 - X^5 - X^4 - X^3 + X + 1$$

Exercice 55 [id=505]

1 Démontrer que si $\mathbb{K}$ est un sous-corps de $\mathbb{C}$ alors $\mathbb{K}$ est un $\mathbb{Q}$ espace vectoriel pour l'addition naturelle et la loi externe induite par la multiplication naturelle.

2 Donner des exemple de sous-corps $\mathbb{K}$ de $\mathbb{C}$ pour lesquels :

(a) $\mathbb{K}$ est un $\mathbb{Q}-$ espace vectoriel de dimension finie .

(b) $\mathbb{K}$ est un $\mathbb{Q}-$ espace vectoriel de dimension infinie .

Si $\mathbb{K}$ est un sous-corps de $\mathbb{C}$ tel que $\dim_{\mathbb{Q}}(\mathbb{K})$ est finie, on notera $[\mathbb{K} : \mathbb{Q}] = \dim_{\mathbb{Q}}(\mathbb{K})$. Pour tout $\theta \in \mathbb{C}$, on notera $\mathbb{Q}(\theta)$ le plus petits sous corps de $\mathbb{C}$ contenant $\{\theta\}$. On dit que θ est algébrique sur $\mathbb{Q}$ si et seulement si $\mathbb{Q}(\theta)$ est de dimension finie. Dans ce cas on dira que $[\mathbb{Q}(\theta) : \mathbb{Q}]$ est le degré de l'extension $\mathbb{Q}(\theta)$.

3 Soit $\theta \in \mathbb{C}$ et $\mathfrak{I}_\theta = \{P \in \mathbb{Q}[X]/P(\theta) = 0\}$. Montrer que $\mathfrak{I}_\theta$ est un idéal de l'anneau $\mathbb{Q}[X]$ et que $\mathfrak{I}_\theta \neq \{0\}$ si et seulement si θ est algébrique sur $\mathbb{Q}$.

4 Démontrer que si $\theta \in \mathbb{C}$ est algébrique alors il existe un et unseul polynôme unitaire π_θ tel que $\mathfrak{I}_\theta = \pi_\theta\mathbb{Q}[X]$. Démontrer alors que π_θ est irréductible dans $\mathbb{Q}[X]$ et que $\deg(\pi_\theta) = [\mathbb{Q}(\theta) : \mathbb{Q}]$.

5 Démontrer que $\mathbb{Q}(\sqrt{2})$ et $\mathbb{Q}(i\sqrt{2})$ sont isomorphes en tant que $\mathbb{Q}-$espaces vectoriels mais ne sont pas isomorphes en tant que corps.

Exercice 56 [id=506]

Soit $\alpha \in \mathbb{C}$ une racine de

$$f(X) = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$$

avec $a_0, a_1, \ldots a_n \in \mathbb{Z}$ premiers dans leur ensemble, $n \geq 1$ et $a_n \neq 0$.

1 On suppose que $\alpha \in \mathbb{Z}$, montrer que α divise a_0.

2 On suppose que $\alpha = p/q \in \mathbb{Q}$, la fraction p/q étant irréductible, démontrer que p divise a_0 et que q divise a_n. Démontrer que pour tout entier m, l'entier $p-mq$ divise $f(m)$. (En particulier $p-q$ divise $f(1)$ et $p+q$ divise $f(-1)$). Enoncer le résultat obtenu lorsque $a_n = 1$.

3 Soit

$$\varphi(Y) = Y^n + a_{n-1}Y^{n-1} + a_na_{n-2}Y^{n-2} + \cdots + a_n^{n-2}a_1Y + a_n^{n-1}a_0$$

Montrer que $a_n^{n-1}f(X) = \varphi(Y)$ avec $Y = a_nX$. En déduire le lien entre les racines rationnelles de $f(X)$ et celles de $\varphi(Y)$.

4 Déterminer les racines rationnelles de $f_1(X) = 2X^3 - 12X^2 + 13X - 15$ et de $f_2(X) = 4X^3 - 8X^2 + 15X - 3$.

Exercice 57 [id=507]

Soit $f(X) \in \mathbb{Q}[X]$ un polynôme irréductible de degré ≥ 3.

1 On suppose que $f(X)$ admet exactement deux racines non réelles $z_1 = \alpha + i\beta$ et $z_2 = \overline{z}_1$ avec $\alpha, \beta \in \mathbb{R}$. Montrer que $\beta \notin \mathbb{Q}$.

2 On suppose que $f(X)$ admet une seule racine réelle r. Soit $z = \alpha + i\beta$ avec α, $\beta \in \mathbb{R}$ une autre racine de f. Montrer que $\alpha \notin \mathbb{Q}$.

Exercice 58 [id=512]

Soit $(G, \star)$ un groupe et $\omega \in G$.

1 Démontrer que les assertions suivantes sont équivalentes :

(i) $\forall A \subset G, \langle A\rangle = G \Rightarrow \langle A\backslash\{\omega\}\rangle = G$.

(ii) $\forall A \subset G, \langle A \cup \{\omega\}\rangle = G \Rightarrow \langle A\rangle = G$.

(iii) $\forall A \subset G, \langle A\rangle = G \Rightarrow \langle \omega A\rangle = \langle \omega^{-1}A\rangle = G$.

Si ω satisfait l'une des conditions $(i), (ii), (iii)$ on dit que ω est *superflu*.

2 On note $\mathfrak{T}_G$ l'ensemble des éléments superflus de G. Démontrer que $\mathfrak{T}_G$ est un sous groupe de $(G, \star)$.

3 Determiner $\mathfrak{T}_G$ dans chacun des cas suivants :

a $G = \mathbb{Z}$ muni de l'addition.

b $G = \mathbb{Q}$ muni de l'addition.

c $G = \mathbb{Z}/6\mathbb{Z}$ muni de l'addition.