*Exercices MP/MP**

Table des matières

1 Algèbre Générale

Exercice 1.1. *Soit $(G, \cdot)$ un groupe tel que $\exists p \in \mathbb{N}$ tel que f_p, f_{p+1}, f_{p+2} soient des morphismes où*

$$\begin{array}{rccc} f_p : & G & \to & G \\ & x & \mapsto & x^p \end{array}$$

Montrer que G est un groupe abélien.

Remarque 1.

— Pour $(\Sigma_3, \circ)$, on a f_0, f_1, f_6 des morphismes mais Σ_3 n'est pas commutatif.

— Si f_2 est un morphisme, pour tout $x, y \in G^2$, on a

$$\begin{aligned} (xy)^2 &= xyxy \\ &= x^2y^2 \end{aligned}$$

d'où $xy = yx$.

Exercice 1.2. *Soit $(G, \cdot)$ un groupe fini. Soit $A = \{x \in G,\ \omega(x) \text{ est impair}\}$ où $\omega(x)$ désigne l'ordre de x. Montrer que A est non vide, et que $x \mapsto x^2$ est une permutation de A.*

Exercice 1.3. *Soit $\sigma \in \Sigma_n$. On note $\theta(\sigma)$ le nombre d'orbite de σ. Montrer que le nombre minimal de transposition dont σ est le produit est $n - \theta(\sigma)$.*

Exercice 1.4. *Soit $(n, m) \in (\mathbb{N}^*)^2$. Combien y a-t-il de morphismes de groupe de $\left(\mathbb{Z}/n\mathbb{Z}, +\right) \to \left(\mathbb{Z}/m\mathbb{Z}, +\right)$?*

Remarque 2. Exemple pour $f : \left(\mathbb{Z}/4\mathbb{Z}, +\right) \to \left(\mathbb{Z}/6\mathbb{Z}, +\right)$. On note $f(\bar{1}) = \tilde{x}$, d'où $4\tilde{x} = \tilde{0}$ et $3 \mid x$, donc $x \in \{0, 3\}$. Ainsi, on a ou bien $f = f_0 : \bar{l} \mapsto \tilde{0}$, ou bien $f = f_1 : \bar{l} \mapsto \tilde{3l}$.

Exercice 1.5. *Soit $(G, \cdot)$ un groupe abélien fini. Soit $P = \prod_{x \in G} x$. Montrer que $P = e_G$ (élément neutre de G) sauf dans un cas très particulier.*

Exercice 1.6. *Soit G un sous-groupe additif de $\mathbb{R}$. On suppose qu'il existe un nombre fini n d'ensembles de la forme $(x + G)_{x \in \mathbb{R}}$ avec $x + G = \{x + y,\ y \in G\}$. Montrer que $G = \mathbb{R}$.*

Exercice 1.7. *Soit $n \in \mathbb{N}^*$. Combien y a-t-il d'automorphismes de $\left(\mathbb{Z}/n\mathbb{Z}, +\right)$?*

Exercice 1.8. *Soit $(G, \cdot)$ un groupe fini et φ un morphisme de $G \to G$. Montrer que $|G| = |\operatorname{Im} \varphi| \times |\ker \varphi|$. En déduire que $\ker \varphi = \ker \varphi^2$ si et seulement si $\operatorname{Im} \varphi = \operatorname{Im} \varphi^2$.*

Exercice 1.9. *Soit $(G, \cdot)$ un groupe fini d'ordre n, et $m \in \mathbb{N}$ tel que $n \wedge m = 1$. Montrer que pour tout $y \in G$, il existe un unique $x \in G$ tel que $x^m = y$.*

Exercice 1.10. *Soit $(G, \cdot)$ un groupe fini. Pour $g \in G$, on note*

$$C(g) = \{hgh^{-1},\ h \in G\}$$

et

$$S_g = \{x \in G,\ xg = gx\}$$

1. *Montrer que S_g est un sous-groupe de G.*
2. *Montrer que $|G| = |S_g| \times |C(g)|$.*
3. *On note $Z(G) = \{x \in G,\ \forall y \in G,\ xy = yx\}$. Montrer que $Z(G)$ est un sous-groupe de G, et que pour tout $g \in G$, $Z(G) \subset S_g$.*
4. *On suppose que $|G| = p^\alpha$ où p est premier et $\alpha \geqslant 1$. Montrer que $|Z(G)| \neq 1$. On pourra utiliser le fait que $x\mathcal{R}y$ si et seulement si il existe $h \in G$ tel que $y = hxh^{-1}$ est une relation d'équivalence.*
5. *On suppose que $|G| = p^2$. Montrer que G est abélien et qu'il est isomorphe à $\mathbb{Z}/p^2\mathbb{Z}$ ou à $\left(\mathbb{Z}/p\mathbb{Z}\right)^2$.*

Remarque 3. Les groupes de cardinal p^3 ne sont pas nécessairement abélien, un exemple est donné par D_4, le groupe des isométries du carré (qui est de cardinal $2^3 = 8$).

Exercice 1.11. *Trouver tous les morphismes de $(\mathbb{Z}, +)$ (respectivement $(\mathbb{Q}, +)$) dans $(\mathbb{Q}_+^*, \times)$. On pourra poser, pour p premier et $n \in \mathbb{Z}$, $\nu_p(n)$ la puissance de p dans la décomposition en produit de facteurs premiers de n.*

Exercice 1.12. *Soit G un groupe engendré par deux éléments $x, y \neq e_G$ tels que $x^5 = e_G$ et $xy = y^2x$. Montrer que $|G| = 155 = 5 \times 31$ et qu'il est unique à un isomorphisme près.*

Exercice 1.13. *Soit $(G, \cdot)$ un groupe abélien fini. On note $N = \vee_{x \in G}\omega(x)$ (ppcm des ordres des éléments de G) appelé exposant de G, caractérise par $\forall k \in \mathbb{Z}, (\forall x \in G, x^k = e)$ si et seulement si $(\forall x \in G,\ \omega(x) \mid k)$ si et seulement si $(N|k)$. En particulier, $N \mid |G|$.*

On pose $N = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ la décomposition en nombres premiers de N.

1. *Soit $i \in \{1, \dots, r\}$. Justifier qu'il existe $y_i \in G$, tel que $p_i^{\alpha_i} \mid \omega(y_i)$.*
2. *Soit $i \in \{1, \dots, r\}$. Justifier qu'il existe $x_i \in G$, tel que $\omega(x_i) = p_i^{\alpha_i}$.*
3. *Montrer qu'il existe $x \in G$ tel que $\omega(x) = N$.*

Exercice 1.14. *Soit $\mathbb{K}$ un corps fini commutatif, $(\mathbb{K}^*, \times)$ est un groupe abélien fini. Soit $N = \vee_{x \in \mathbb{K}^*}\omega(x)$ (ordre multiplicatif). On sait d'après l'exercice précédent qu'il existe $x_0 \in \mathbb{K}^*$ tel que $\omega(x_0) = N$. En étudiant le polynôme $X^N - 1_K$, montrer que $(\mathbb{K}^*, \times)$ est cyclique.*

En exemple, soit $\left(\mathbb{Z}/13\mathbb{Z}, +, \times\right)$ (c'est un corps).

Trouver un générateur du groupe $\left(\mathbb{Z}/13\mathbb{Z}^*, \times\right)$.

Exercice 1.15. *Soit $(G, \cdot)$ un groupe tel que $\forall x \in G,\ x^2 = e_G$.*

1. *Montrer que G est abélien.*
2. *Montrer que si G est fini, il existe $n \in \mathbb{N}$ tel que G soit isomorphe à $\left(\left(\mathbb{Z}/2\mathbb{Z}\right)^n, +\right)$. On pourra considérer une famille génératrice minimale.*

Exercice 1.16. *Soit $(G, \cdot)$ un groupe, on appelle groupe dérivé de G et on note*

$$D(G) = \{xyx^{-1}y^{-1},\ (x, y) \in G^2\}$$

.

1. *Si G est abélien, que vaut $D(G)$?*
2. *Montrer que pour $n \geqslant 3$, les 3-cycles engendrent $\mathcal{A}_n$ (groupe des permutations de signature égale à 1).*
3. *Montrer que deux 3-cycles (a_1, a_2, a_3) et (b_1, b_2, b_3) sont conjugués dans Σ_n (c'est-à-dire qu'il existe $\sigma \in \Sigma_n$ telle que $(b_1, b_2, b_3) = \sigma \circ (a_1, a_2, a_3) \circ \sigma^{-1}$). Est-ce encore vrai dans $\mathcal{A}_n$?*
4. *En déduire $D(\Sigma_n)$.*

Remarque 4. Pour $n \geqslant 5$, on a $D(\mathcal{A}_n) = D(\mathcal{A}_n)$.

Exercice 1.17. *Soit $(G, \cdot)$ un groupe fini de cardinal n.*

1. *Soit $g \in G$ et*
$$\begin{array}{rccc} \tau_g : & G & \to & G \\ & x & \mapsto & g \cdot x \end{array}$$
Montrer que
$$\begin{array}{rccc} \tau : & G & \to & \Sigma(G) \\ & g & \mapsto & \tau_g \end{array}$$
(où $\Sigma(G)$ est le groupe des permutations de G) est un morphisme injection. En déduire que G est isomorphe à un sous-groupe de $(\Sigma_n, \circ)$.
2. *Montrer que G est isomorphe) un sous-groupe de $(GL_n(\mathbb{C}), \times)$.*

Exercice 1.18. *Montrer qu'il n'existe pas $(x, y, z, t, n) \in \mathbb{N}^5$ tel que $x^2 + y^2 + z^2 = (8t + 7) \times 4^n$.*

Exercice 1.19. *Montrer que $10^{10^n} \equiv 4[7]$ pour tout $n \in \mathbb{N}^*$.*

Exercice 1.20. *Pour $n \in \mathbb{N}$, on pose $F_n = 2^{2^n} + 1$.*

1. *Montrer que pour tout $n \geqslant 1$, $F_n = 2 + \prod_{k=0}^{n-1} F_k$.*
2. *En déduire qu'il existe une infinité de nombres premiers.*

Remarque 5. Si $n \neq m$, alors $F_n \wedge F_m = 1$.

Exercice 1.21. *Soit U le groupe des inversibles de $\mathbb{Z}/32\mathbb{Z}$.*

1. *Quel est l'ordre de $\bar{5}$?*
2. *Montrer que $U = gr\{\bar{-}1, \bar{5}\}$ (groupe engendré) et qu'il est isomorphe à un groupe produit.*

Exercice 1.22. *On note, pour $n \in \mathbb{N}^*$, $G_n = \{e^{\frac{2ik\pi}{n}},\ k \wedge n = 1\}$ l'ensemble des racines n-ièmes de l'unité, on définit $\mu(n) = \sum_{\xi \in G_n} \xi$.*

1. *Montrer que si $n \wedge m = 1$, alors $\mu(nm) = \mu(m)\mu(n)$.*
2. *Calculer $\mu(1)$. Que vaut $\mu(n)$ si $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ (décomposition en nombres premiers) ?*
3. *Soit $\mathbb{C}^{\mathbb{N}^*}$ muni de*
$$\begin{array}{rccc} f \star g : & \mathbb{N}^* & \to & \mathbb{C} \\ & n & \mapsto & (f \star g)(n) = \sum_{d|n} f(d) g(n/d) \end{array}$$
Montrer que $\star$ est une loi associative et commutative, qu'elle admet un élément neutre noté e. Déterminer l'inverse de μ pour $\star$. On pourra calculer, pour $n \geqslant 2$, $\sum_{d|n} \mu(d)$.

4. *Que vaut pour $n \in \mathbb{N}^*$, $\sum_{d|n} d\mu(d/n)$?*

Exercice 1.23. *Soit p premier. Montrer que*

$$\sum_{k=0}^{p} \binom{p}{k}\binom{p+k}{k} \equiv 2^p + 1[p^2]$$

Exercice 1.24.

1. *Montrer que les sous-groupes finis de $(U, \times)$ sont cycliques (où U est le cercle unité).*
2. *Quels sont les sous-groupes finis de $SO_2(\mathbb{R})$?*
3. *Soit G un sous-groupe fini de $SL_2(\mathbb{R})$. Montrer que*

$$\begin{array}{rccc} \varphi : & \mathbb{R}^2 & \to & \mathbb{R} \\ & (X,Y) & \mapsto & \sum_{M\in G}\langle MX, MY\rangle \end{array}$$

où $\langle\cdot,\cdot\rangle$ est le produit scalaire canonique de $\mathbb{R}$. Montrer que φ est un produit scalaire pour lequel les matrices de M sont des isométries. En déduire que G est cyclique.

Exercice 1.25. *Soit $E = \{x + y\sqrt{2},\ x \in \mathbb{N}^*,\ y \in \mathbb{Z},\ \text{et } x^2 - 2y = 1\}$.*

1. *Montrer que E est un sous-groupe de $(\mathbb{R}_+^*, \times)$.*
2. *Montrer que $E = \{(x_0 + y_0\sqrt{2})^n,\ n \in \mathbb{Z}\}$ où $x_0 + y_0\sqrt{2} = \min E \cap]1, +\infty[$.*

Exercice 1.26. *Déterminer les entiers $n \in \mathbb{N}^*$ tels que $7 \mid n^n - 3$.*

Exercice 1.27. *Soit p premier plus grand que 5. Soit $a \in \mathbb{N}$ tel que $1+\frac{1}{2}+\cdots+\frac{1}{p-1} = \frac{a}{(p-1)!}$. Montrer que $p^2 \mid a$.*

Exercice 1.28. *Soit $P \in \mathbb{R}[X]$ tel que $\forall x \in \mathbb{R}$, $P(x) \geqslant 0$. Montrer qu'il existe $(A, B) \in \mathbb{R}[X]^2$ tel que $P = A^2 + B^2$.*

Exercice 1.29.

1. *Soit $\alpha \in \mathbb{R}$ tel que $\frac{\alpha}{\pi} \notin \mathbb{Q}$. Montrer que $(\sin(n\alpha))_{n\in\mathbb{N}}$ est dense dans $[-1, 1]$.*
2. *Montrer qu'il y a une infinité de puissance de 2 qui commencent par 7 en base 10.*

Exercice 1.30. *Soit A un anneau commutatif intègre, on dit que A est euclidien si et seulement s'il existe $v : A \setminus \{0\} \to \mathbb{N}$ tels que pour tout $(a, b) \in A \times A \setminus \{0\}$, il existe $(q, r) \in A^2$ tels que $a = bq + r$ et $v(r) < v(b)$ ou $r = 0$.*

1. *Montrer que $\mathbb{Z}[i] = \{a + ib,\ (a, b) \in \mathbb{Z}^2\}$ est euclidien.*
2. *Montrer que tout anneau euclidien est principal.*

Exercice 1.31.

1. *Soit p premier plus grand que 3. Soit $\bar{x} \in \mathbb{Z}/Z \setminus \{\bar{0}\}$. Montrer que $\bar{x}$ est un carré dans $\mathbb{Z}/p\mathbb{Z}$ si et seulement $\bar{x}^{\frac{p-1}{2}} = \bar{1}$.*
2. *En déduire qu'il existe une infinité de nombres premiers congrus à 1 modulo 4.*

Exercice 1.32. *Soit* $P = \sum_{i=0}^{n} r_i X^i \in \mathbb{Q}[X] \setminus \{0\}$. *On pose*

$$c(P) = \prod_{p \in \mathcal{P}} p^{\min\limits_{0 \leqslant i \leqslant n} (\nu_p(r_i))}$$

où $\mathcal{P}$ *est l'ensemble des nombres premiers. On écrit* $P = c(P) \times P_1$.

1. *Montrer que* $P_1 \in \mathbb{Z}[X]$, *que ses coefficients sont premiers entre eux dans leur ensemble et qu'une telle écriture est unique.*
2. *Soit* $(P, Q) \in \Big(\mathbb{Q}[X] \setminus \{0\}\Big)^2$. *Montrer que* $c(PQ) = c(P)c(Q)$. *On justifiera en passant dans* $\mathbb{Z}/p\mathbb{Z}[X]$ *que si* p *premier divise tous les coefficients de* $P_1 \times Q_1$, *alors il divise tous les coefficients de* P_1 *ou tous ceux que* Q_1 *[Lemme de Gauss].*
3. *En déduire que si* $P \in \mathbb{Z}[X]$ *est irréductible sur* $\mathbb{Z}[X]$, *alors il l'est aussi sur* $\mathbb{Q}[X]$. *La réciproque est-elle vraie ?*
4. *Trouver tous les* $\theta \in [0, 2\pi[$ *tels que* $\frac{\theta}{\pi} \in \mathbb{Q}$ *et* $\cos(\theta) \in \mathbb{Q}$. *Si* $\theta \not\equiv 0[\pi]$ *et si* $\theta = 2\pi p/q$ *avec* $p \wedge q = 1$, *on appliquera ce qui précède à* $A = X^q - 1$ *et* $P = X^2 - (2\cos(\theta))X + 1$.

Exercice 1.33. *Soit* $P \in \mathbb{R}[X]$ *scindé sur* $\mathbb{R}$.

1. *Montrer que pour tout* $\alpha \in \mathbb{R}$, $P + \alpha P'$ *est scindé sur* $\mathbb{R}$.
2. *Soit* $R = \sum_{i=0}^{r} a_i X^i$ *scindé sur* $\mathbb{R}$. *Montrer que* $\sum_{i=0}^{r} a_i P^{(i)}$ *l'est aussi.*

Exercice 1.34. *Soit* $P \in \mathbb{R}[X]$ *de degré* $n \geqslant 1$, *scindé sur* $\mathbb{R}$. *Montrer que pour tout* $x \in \mathbb{R}$, $(n-1)(P'^2)(x) \geqslant nP(x)P''(x)$.

Exercice 1.35.

1. *Soit* $P \in \mathbb{Q}[X]$ *irréductible sur* $\mathbb{Q}[X]$, *montrer que* R *n'a que des racines simples sur* $\mathbb{C}$. *On pourra évaluer* $P \wedge P'$ *sur* $\mathbb{Q}[X]$.
2. *Soit* $A \in \mathbb{Q}[X]$ *et* $\alpha \in \mathbb{C}$ *une racine de* A *de multiplicité* $m(\alpha) > d(A)/2$ *où* $d(A)$ *est le degré de* A. *Montrer que* $\alpha \in \mathbb{Q}$.
3. *Soit* $A \in \mathbb{Q}[X]$ *de degré* $2m+1$. *On suppose que* A *admet une racine complexe de multiplicité plus grande que* m. *Montrer que* A *possède une racine rationnelle.*