

*Exercices MP/MP**

Algèbre Générale

Exercice 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

$$\begin{aligned} f_p : G &\rightarrow G \\ x &\mapsto x^p \end{aligned} \tag{1}$$

Montrer que G est un groupe abélien.

Exercice 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 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 4. Soit $(n, m) \in (\mathbb{N}^*)^2$. Combien y a-t-il de morphismes de groupe de $(\mathbb{Z}/n\mathbb{Z}, +) \rightarrow (\mathbb{Z}/m\mathbb{Z}, +)$?

Exercice 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 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 7. Soit $n \in \mathbb{N}^*$. Combien y a-t-il d'automorphismes de $(\mathbb{Z}/n\mathbb{Z}, +)$?

Exercice 8. Soit (G, \cdot) un groupe fini et φ un morphisme de $G \rightarrow G$. Montrer que $|G| = |\text{Im}\varphi| \times |\ker \varphi|$. En déduire que $\ker \varphi = \ker \varphi^2$ si et seulement si $\text{Im}\varphi = \text{Im}\varphi^2$.

Exercice 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 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 $\alpha \geq 1$. 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 $y = h x h^{-1}$ 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 $(\mathbb{Z}/p\mathbb{Z})^2$.

Exercice 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 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 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 , caractérisé 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 $(N \mid k)$. 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 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 $(\mathbb{Z}/13\mathbb{Z}, +, \times)$ (c'est un corps).

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

Exercice 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 $\left((\mathbb{Z}/2\mathbb{Z})^n, +\right)$. On pourra considérer une famille génératrice minimale.

Exercice 16 (Groupe des commutateurs). 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 $n \geq 3$, 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 $D(\Sigma_n)$.

Exercice 17. Soit (G, \cdot) un groupe fini de cardinal n .

1. Soit $g \in G$ et

$$\begin{aligned} \tau_g : G &\rightarrow G \\ x &\mapsto g \cdot x \end{aligned} \tag{2}$$

Montrer que

$$\begin{aligned} \tau : G &\rightarrow \Sigma(G) \\ g &\mapsto \tau_g \end{aligned} \tag{3}$$

(où $\Sigma(G)$ est le groupe des permutations de G) est un morphisme injectif. En déduire que G est isomorphe à un sous-groupe de (Σ_n, \circ) .

2. Montrer que G est isomorphe à un sous-groupe de $(GL_n(\mathbb{C}), \times)$.

Exercice 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 19. Montrer que $10^{10^n} \equiv 4[7]$ pour tout $n \in \mathbb{N}^*$.

Exercice 20. Pour $n \in \mathbb{N}$, on pose $F_n = 2^{2^n} + 1$.

1. Montrer que pour tout $n \geq 1$, $F_n = 2 + \prod_{k=0}^{n-1} F_k$.

2. En déduire qu'il existe une infinité de nombres premiers.

Exercice 21. Soit U le groupe des inversibles de $\mathbb{Z}/32\mathbb{Z}$.

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

Exercice 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

$$\begin{aligned} f \star g : \mathbb{N}^* &\rightarrow \mathbb{C} \\ n &\mapsto (f \star g)(n) = \sum_{d|n} f(d)g(n/d) \end{aligned} \quad (4)$$

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 $n \geq 2$, $\sum_{d|n} \mu(d)$.

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

Exercice 23. Soit p premier. Montrer que

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

Exercice 24.

1. Montrer que les sous-groupes finis de (\mathbb{U}, \times) sont cycliques (où \mathbb{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 $SL_2(\mathbb{R})$. On définit

$$\begin{aligned} \varphi : \mathbb{R}^2 &\rightarrow \mathbb{R} \\ (X, Y) &\mapsto \sum_{M \in G} \langle MX, MY \rangle \end{aligned} \quad (5)$$

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

Exercice 27. Soit p premier plus grand que 5. Soit $a \in \mathbb{N}$ tel que $1 + \frac{1}{2} + \dots + \frac{1}{p-1} = \frac{a}{(p-1)!}$. Montrer que $p^2 \mid a$.

Exercice 28. Soit $P \in \mathbb{R}[X]$ tel que $\forall x \in \mathbb{R}, P(x) \geq 0$. Montrer qu'il existe $(A, B) \in \mathbb{R}[X]^2$ tel que $P = A^2 + B^2$.

Exercice 29.

1. Soit $\alpha \in \mathbb{R}$ tel que $\alpha \notin \mathbb{Q}$. Montrer que $\mathbb{Z} + \alpha\mathbb{Z}$ est dense dans \mathbb{R} . En déduire que $\mathbb{Z} + \alpha\mathbb{N}$ est dense dans \mathbb{R} .
2. 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 $[-1, 1]$.
3. Montrer qu'il y a une infinité de puissance de 2 qui commencent par 7 en base 10.

Exercice 30 (Anneau euclidien). Soit A un anneau commutatif intègre, on dit que A est euclidien si et seulement s'il existe $v : A \setminus \{0\} \rightarrow \mathbb{N}$ 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 31.

1. Soit p premier plus grand que 3. Soit $\bar{x} \in \mathbb{Z}/p\mathbb{Z} \setminus \{\bar{0}\}$. 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 32. Soit $P = \sum_{i=0}^n r_i X^i \in \mathbb{Q}[X] \setminus \{0\}$. On pose

$$c(P) = \prod_{p \in \mathcal{P}} p^{\min_{0 \leq i \leq n} (\nu_p(r_i))}$$

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 $(P, Q) \in \left(\mathbb{Q}[X] \setminus \{0\}\right)^2$. 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 de 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 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 34. Soit $P \in \mathbb{R}[X]$ de degré $n \geq 1$, scindé sur \mathbb{R} . Montrer que pour tout $x \in \mathbb{R}$, $(n - 1)(P'^2)(x) \geq nP(x)P''(x)$.

Exercice 35.

1. Soit $P \in \mathbb{Q}[X]$ irréductible sur $\mathbb{Q}[X]$, montrer que P 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 $\alpha \in \mathbb{Q}$.

Exercice 36. Soit (G, \cdot) un groupe et A une partie finie de G stable pour \cdot . Montrer que A est en fait un sous-groupe de G .

Exercice 37. Soit p premier plus grand que 3. Montrer que pour tout $\alpha \in \mathbb{N}$,

$$(1 + p)^{p^\alpha} \equiv 1 + p^{\alpha+1}[p^{\alpha+2}]$$

Exercice 38. Montrer que pour tout $(x, y) \in \mathbb{Z}^2$, $7 \neq 2x^2 - 5y^2$.

Exercice 39. Résoudre $x^3 = 1$ dans $\mathbb{Z}/19\mathbb{Z}$.

Exercice 40. Soit $n \geq 3$.

1. Combien y a-t-il d'inversibles dans $(\mathbb{Z}/2^n\mathbb{Z}, +, \times)$? On note $(\mathbb{Z}/2^n\mathbb{Z})^\times$ le groupe (multiplicatif) de ses inversibles.
2. Montrer que $5^{2^{n-3}} \equiv 1 + 2^{n-1}[2^n]$.
3. Évaluer l'ordre de 5 dans $(\mathbb{Z}/2^n\mathbb{Z})^\times$.
4. Montrer que $\text{gr}\{-1\} \cap \text{gr}\{5\} = \{1\}$ où gr indique le groupe engendré par l'ensemble. En déduire que $\left((\mathbb{Z}/2^n\mathbb{Z})^\times, \times\right)$ est isomorphe à $(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{n-1}\mathbb{Z}, +)$.

Exercice 41. Soit (G, \cdot) un ensemble non vide muni d'une loi interne associative. On suppose que

- (i) $\exists e \in G, \forall x \in G, x \cdot e = x,$
- (ii) $\forall x \in G, \exists x' \in G, x \cdot x' = e.$

Montrer que (G, \cdot) est un groupe.

Exercice 42. Montrer qu'il existe une infinité de multiples de 21 qui s'écrivent avec uniquement des 1 en base 10.

Exercice 43. Soit \mathbb{K} un corps commutatif fini. Soit $n = |\mathbb{K}^*|$.

1. Soit d un diviseur de n , on suppose qu'il existe $x_0 \in \mathbb{K}^*$ d'ordre (multiplicatif) d dans le groupe (\mathbb{K}^*, \times) . Montrer qu'il existe exactement $\varphi(d)$ éléments d'ordre d dans (\mathbb{K}^*, \times) (φ indique la fonction d'Euler). On pourra s'intéresser au polynôme $X^d - 1_{\mathbb{K}}$.
2. En utilisant $n = \sum_{d|n} \varphi(d)$, montrer que (\mathbb{K}^*, \times) est cyclique.

Exercice 44. Soit p premier plus grand que 5. et $M = \mathbb{Z}/p\mathbb{Z} \setminus \{0, 1\}$.

1. Montrer que

$$\begin{aligned} f : M &\rightarrow M \\ x &\mapsto 1 - x^{-1} \end{aligned} \tag{6}$$

est bien définie et calculer f^3 .

2. Montrer que -3 est un carré dans $\mathbb{Z}/p\mathbb{Z}$ si et seulement si f admet un point fixe.
3. Montrer que -3 est un carré dans $\mathbb{Z}/p\mathbb{Z}$ si et seulement si $p \equiv 1[3]$ (on pourra décomposer f en produit de cycles de supports disjoints).

Exercice 45. Soit $x \in \mathbb{R}$ avec $x = \pm b_m b_{m-1} \dots b_0, a_1 a_2 \dots a_n \dots$ (écriture décimale). Montrer que $x \in \mathbb{Q}$ si et seulement si $\exists n_0 \in \mathbb{N}, \exists T \in \mathbb{N}^*, \forall n \geq n_0, a_{n+T} = a_n$ (la suite des décimales est périodique à partir du rang n_0).

Exercice 46. On définit $H_0 = 1$ et pour tout $n \geq 1$, $H_n = \frac{X(X-1)\dots(X-n+1)}{n!}$.

1. Montrer que $H_n(\mathbb{Z}) \subset \mathbb{Z}$.
2. Soit $P \in \mathbb{C}[X]$. Montrer que $P(\mathbb{Z}) \subset \mathbb{Z}$ et seulement si $\exists n \in \mathbb{N}, \exists (a_0, \dots, a_n) \in \mathbb{Z}^{n+1}$ avec $P = \sum_{k=0}^n a_k H_k$.

Exercice 47. Soit $P \in \mathbb{Q}[X]$ irréductible sur $\mathbb{Q}[X]$, $\alpha \in \mathbb{C} \setminus \mathbb{Q}$ racine de P . Montrer que α est racine simple de P . On pourra se demander, si le degré de P est n et $P = (X - \alpha)(a_0 + a_1 X + \dots + a_{n-1} X^{n-1})$, quels sont les coefficients a_k tels que $a_k \in \mathbb{Q}$.

Exercice 48. Soit $P \in \mathbb{Q}[X]$ de degré 5 tel que P admette une racine complexe α d'ordre plus grand que 2. Montrer que P admet au moins une racine rationnelle.

Exercice 49. On définit $\mathbb{Z}[i] = \{a + ib \mid (a, b) \in \mathbb{Z}^2\}$.

1. Montrer que c'est le plus petit sous-anneau de \mathbb{C} contenant i .
2. On définit, pour $z = a + ib \in \mathbb{Z}[i]$, $|z|^2 = a^2 + b^2$. Montrer que z est inverse dans $\mathbb{Z}[i]$ si et seulement si $|z|^2 = 1$. En déduire l'ensemble U des inversibles.
3. (a) Montrer que pour tout $z_0 = x_0 + iy_0 \in \mathbb{C}$, il existe $z = a + ib \in \mathbb{Z}[i]$, $|z - z_0|^2 \leq \frac{1}{2}$.
 (b) Soit $(z_1, z_2) \in \mathbb{Z}[i]^2$ avec $z_2 \neq 0$. Montrer qu'il existe $(q, r) \in \mathbb{Z}[i]^2$ tel que $z_1 = qz_2 + r$ et $|r| < |z_1|$. A-t-on unicité ?
 (c) En déduire que $\mathbb{Z}[i]$ est principal.
4. Montrer que tout élément $z \in \mathbb{Z}[i] \setminus \{0\}$ peut se décomposer en $z = u \times \prod_{\rho \in \mathcal{P}_0} \rho^{\nu_\rho(z)}$ où $u \in U$ et \mathcal{P}_0 est un ensemble d'irréductibles tel que tout élément de \mathcal{P} (irréductibles de $\mathbb{Z}[i]$) est associé à un unique élément de \mathcal{P}_0 (on pourra raisonner par récurrence sur $|z|^2 \in \mathbb{N}$). Montrer l'unicité de cette décomposition.

Exercice 50. Soit p premier plus grand que 3. On note \mathbb{F}_p le corps $(\mathbb{Z}/p\mathbb{Z}, +, \times)$. On dit que $\bar{x} \in \mathbb{F}_p^*$ est un résidu quadratique si et seulement si il existe $\bar{y} \in \mathbb{F}_p^*$ tel que $\bar{x} = \bar{y}^2$. On note R l'ensemble des résidus quadratiques.

1. Montrer que R est un sous-groupe de (\mathbb{F}_p, \times) de cardinal $\frac{p-1}{2}$ et $a \in R$ si et seulement si $a^{\frac{p-1}{2}} = 1$.
2. Montrer que si $p = a^2 + b^2$ avec $(a, b) \in \mathbb{N}^2$, alors $p \equiv 1[4]$. On pourra montrer que $\overline{-1} \in R$.
3. Montrer que, pour $k \in \{1, \dots, p-1\}$,

$$\begin{aligned} f : \{0, \dots, E(\sqrt{p})\}^2 &\rightarrow \mathbb{F}_p \\ (a, b) &\mapsto a - kb \end{aligned} \tag{7}$$

n'est pas injective. En déduire qu'il existe $(a_0, b_0) \in \{1, \dots, E(\sqrt{p})\}^2$ tel que $k = a_0 \times b_0^{-1}$.

4. Soit p premier tel que $p \equiv 1[4]$. Montrer que p est somme de deux carrés.

Exercice 51 (Fermat). Soit p premier. On sait, d'après l'exercice précédent, que p est somme de deux carrés si et seulement si $p = 2$ ou $p \equiv 1[4]$. On note $A = \{n \in \mathbb{N}^* \mid \exists (a, b) \in \mathbb{N}^2, n = a^2 + b^2\}$.

1. Montrer que A est stable par produit. On note alors $P_1 = \{p \text{ premier} \mid p = 2 \text{ ou } p \equiv 1[4]\}$ et $P_2 = \{p \text{ premier} \mid p \equiv 3[4]\}$.
2. Soit $n \in \mathbb{N}^*$. On suppose que pour tout $p \in P_2$, $\nu_p(n)$ est pair (où $\nu_p(n)$ la puissance de p dans la décomposition en produit de facteurs premiers de n). Montrer que $n \in A$.
3. Montrer la réciproque (pour $n \in A$, pour $p \in P_1 \cup P_2$ tel que $\nu_p(n)$ est impair, on montrera que -1 est un carré dans \mathbb{F}_p).