Algèbre : Examen

Université Paris Cité – M1 MIC – 21 décembre 2023

Durée : 3h. L'utilisation de documents ou de matériel électronique est interdite. Lisez tout le sujet avant de commencer ; les exercices sont indépendants et il n'est pas nécessaire de résoudre tous les exercices pour obtenir 20/20. Une réponse non justifiée n'obtiendra pas la totalité des points.
English version below.

Exercice 1. Vrai ou faux ? Si l'énoncé est vrai, donner une démonstration ; sinon, donner un contre-exemple. On rappelle que $a \vee b \coloneqq \mathrm{ppcm}(a,b)$, que $a \wedge b \coloneqq \mathrm{pgcd}(a,b)$, et que K_A est le corps des fractions de l'anneau A.

(a) Si A est factoriel et $a, b \in A$, alors $(a) \cap (b) = (a \vee b)$.

(b) Si A est factoriel et $a, b \in A$, alors $(a) + (b) = (a \wedge b)$.

(c) Si A est principal et $a, b \in A$, alors $(a) + (b) = (a \wedge b)$.

(d) Si A est factoriel et $P \in A[X]$ est irréductible dans $A[X]$, alors il est irréductible dans $K_A[X]$.

(e) Si A est factoriel et $P \in A[X]$ est irréductible dans $A[X]$ et non constant, alors il est irréductible dans $K_A[X]$.

(f) Si A est factoriel et $P \in A[X]$ est irréductible dans $K_A[X]$, alors il est irréductible dans $A[X]$.

Exercice 2. On se propose de démontrer un résultat conjecturé par Fermat et démontré par Euler : « si $p \equiv 1 \pmod 3$ est un nombre premier, alors p s'écrit sous la forme $p = a^2 + 3b^2$, où $a, b \in \mathbb{Z}$ ». On note $j = \exp(2i\pi/3)$ l'une des solutions de $1 + j + j^2 = 0$.

(a) Démontrer que $\mathbb{Z}[j] = \{ x + jy \mid x, y \in \mathbb{Z} \}$ est un sous-anneau de $\mathbb{C}$ stable par conjugaison complexe.

(b) Pour $z \in \mathbb{Z}[j]$, on note $N(z) = z\bar{z}$. Démontrer que si $x, y \in \mathbb{Z}$, alors $\mathrm{N}(x + jy) = x^2 - xy + y^2$.

(c) Justifier que $\mathrm{N}(zz') = \mathrm{N}(z)\,\mathrm{N}(z')$ et que, pour $x, y \in \mathbb{Z}$, $x^2 - xy + y^2 \geq 3y^2/4$.

(d) Démontrer que $z \in \mathbb{Z}[j]$ est inversible si et seulement si $\mathrm{N}(z) = 1$. En déduire que $\mathbb{Z}[j]^\times = \{\pm 1, \pm j, \pm j^2\}$.

(e) Démontrer que pour tout $z \in \mathbb{C}$, il existe $w \in \mathbb{Z}[j]$ tel que $|z - w| < 1$. On pourra s'aider d'un dessin. En déduire que $\mathbb{Z}[j]$ est euclidien.

(f) Soit p un nombre premier. Décrire, en fonction de p, la décomposition en produit de facteurs irréductibles dans $\mathbb{F}_p[X]$ du polynôme $X^2 - X + 1$.

(g) Soit p un nombre premier qui est congru à 1 mod 3. Démontrer qu'il existe $x \in \mathbb{Z}$ tel que p divise le produit $(x + j)(x + \bar{j})$ dans $\mathbb{Z}[j]$.

(h) En déduire que p n'est pas irréductible dans $\mathbb{Z}[j]$.

(i) Démontrer qu'il existe $z_0 \in \mathbb{Z}[j]$ tel que $p = \mathrm{N}(z_0)$.

(j) En considérant l'ensemble $\{j^{\pm 1} z_0,\ j^{\pm 1} \bar{z}_0\}$, démontrer qu'on peut supposer que $z_0 = a + bi\sqrt{3}$ avec $a, b \in \mathbb{Z}$. En déduire que $p = a^2 + 3b^2$.

Exercice 3. On considère $P = X^4 - 3 \in \mathbb{Q}[X]$ et on note $\mathbb{K}$ le corps de décomposition de P.

(a) Démontrer que P est irréductible sur $\mathbb{Q}$. Est-il irréductible sur $\mathbb{R}$?

(b) Démontrer que $\mathbb{K} = \mathbb{Q}(\sqrt[4]{3}, i)$.

(c) Déterminer le degré $[\mathbb{K} : \mathbb{Q}]$ et donner une base de $\mathbb{K}$ comme $\mathbb{Q}$-espace vectoriel.

(d) Pourquoi est-ce que $\mathbb{Q} \subset \mathbb{K}$ est galoisienne ? En déduire le cardinal du groupe de Galois $\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$.

(e) Déterminer le groupe $\mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q})$.

(f) Quel sont les liens entre $\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$, $\mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q})$, et $\mathrm{Gal}\big(\mathbb{K}/\mathbb{Q}(i)\big)$?

Exercice 4. On pose $M = \begin{pmatrix} 20 & 8 & 4 \\ -10 & -4 & -2 \\ 8 & 2 & 4 \end{pmatrix} \in M_3(Z)$.

(a) Déterminer la forme normale de Smith $\begin{pmatrix} d_1 & 0 & 0 \\ 0 & d_2 & 0 \\ 0 & 0 & d_3 \end{pmatrix}$ de la matrice M, en faisant bien apparaître les étapes et les opérations élémentaires utilisées.

(b) On note G le sous-groupe de $\mathbb{Z}^3$ engendré par les colonnes de M. Déterminer une base de G.

(c) ★ Décomposer le quotient $Q = \mathbb{Z}^3/G$ sous la forme $\mathbb{Z}^r \times \mathbb{Z}/n_1\mathbb{Z} \times \dots \times \mathbb{Z}/n_s\mathbb{Z}$ avec $r, s \geq 0$ et $n_i \geq 2$. Déterminer des représentants dans $\mathbb{Z}^3$ d'une base de la partie libre et un générateur de chacun des groupes finis dans la décomposition.

English version

Exercice 1. True or false? If the statement is true, give a demonstration; if not, give a counter-example. We recall that $a \vee b \coloneqq \mathrm{lcm}(a, b)$, that $a \wedge b \coloneqq \gcd(a, b)$ and that K_A is the field of fractions of the ring A.

(a) If A is a UFD[1] and $a, b \in A$, then $(a) \cap (b) = (a \vee b)$.

(b) If A is a UFD and $a, b \in A$, then $(a) + (b) = (a \wedge b)$.

(c) If A is a PID[2] and $a, b \in A$, then $(a) + (b) = (a \wedge b)$.

(d) If A is a UFD and $P \in A[X]$ is irreducible in $A[X]$, then it is irreducible in $K_A[X]$.

(e) If A is a UFD and $P \in A[X]$ is irreducible in $A[X]$ and non-constant, then it is irreducible in $K_A[X]$.

(f) If A is a PID and $P \in A[X]$ is irreducible in $K_A[X]$, then it is irreducible in $A[X]$.

[1] Unique Factorization Domain = "*anneau factoriel*" in French.
[2] Principal Ideal Domain = "*anneau principal*" in French.

Exercice 2. We aim at proving a result conjectured by Fermat and proved by Euler : "if $p \equiv 1 \pmod 3$ is prime, then p can be written as $p = a^2 + 3b^2$, where $a, b \in \mathbb{Z}$ ». We let $j = \exp(2i\pi/3)$ be one of the solutions of $1 + j + j^2 = 0$.

(a) Prove that $\mathbb{Z}[j] = \{ x + jy \mid x, y \in \mathbb{Z} \}$ is a subring of $\mathbb{C}$ stable by complex conjugation.

(b) For $z \in \mathbb{Z}[j]$, we let $N(z) = z\bar{z}$. Prove that if $x, y \in \mathbb{Z}$, then $\mathrm{N}(x + jy) = x^2 - xy + y^2$.

(c) Justify that $\mathrm{N}(zz') = \mathrm{N}(z)\,\mathrm{N}(z')$ and that, for $x, y \in \mathbb{Z}$, $x^2 - xy + y^2 \geq 3y^2/4$.

(d) Prove that $z \in \mathbb{Z}[j]$ is invertible if and only if $\mathrm{N}(z) = 1$. Deduce that $\mathbb{Z}[j]^\times = \{\pm 1, \pm j, \pm j^2\}$.

(e) Prove that for all $z \in \mathbb{C}$, there exists $w \in \mathbb{Z}[j]$ such that $|z - w| < 1$. A drawing can help. Deduce that $\mathbb{Z}[j]$ is Euclidean.

(f) Let p be a prime number. Describe, in terms of p, the decomposition in irreducible factors in $\mathbb{F}_p[X]$ of the polynomial $X^2 - X + 1$.

(g) Let p be a prime number congruent to 1 mod 3. Prove that there exists $x \in \mathbb{Z}$ such that p divides the product $(x + j)(x + \bar{j})$ in $\mathbb{Z}[j]$.

(h) Deduce that p is not irreducible in $\mathbb{Z}[j]$.

(i) Prove that there exists $z_0 \in \mathbb{Z}[j]$ such that $p = \mathrm{N}(z_0)$.

(j) By considering the set $\{j^{\pm 1} z_0,\ j^{\pm 1}\bar{z}_0\}$, prove that we can assume that $z_0 = a + bi\sqrt{3}$ with $a, b \in \mathbb{Z}$. Deduce that $p = a^2 + 3b^2$.

Exercice 3. We consider $P = X^4 - 3 \in \mathbb{Q}[X]$ and we let $\mathbb{K}$ be the decomposition field of P.

(a) Prove that P is irreducible over $\mathbb{Q}$. Is it irreducible over $\mathbb{R}$?

(b) Prove that $\mathbb{K} = \mathbb{Q}\left(\sqrt[4]{3}, i\right)$.

(c) Determine the degree $[\mathbb{K} \colon \mathbb{Q}]$ and give a basis of $\mathbb{K}$ as a $\mathbb{Q}$-vector space.

(d) Why is $\mathbb{Q} \subset \mathbb{K}$ Galoisian? Deduce from that the cardinal of the Galois group $\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$.

(e) Determine the group $\mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q})$.

(f) What are the relationships between $\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$, $\mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q})$, and $\mathrm{Gal}\big(\mathbb{K}/\mathbb{Q}(i)\big)$?

Exercice 4. We let $M = \begin{pmatrix} 20 & 8 & 4 \\ -10 & -4 & -2 \\ 8 & 2 & 4 \end{pmatrix} \in M_3(Z)$.

(a) Give the Smith normal form $\begin{pmatrix} d_1 & 0 & 0 \\ 0 & d_2 & 0 \\ 0 & 0 & d_3 \end{pmatrix}$ of the matrix M, making explicit the steps and elementary operations used.

(b) We let G be the subgroup of $\mathbb{Z}^3$ generated by the columns of M. Determine a basis of G.

(c) ★ Decompose the quotient $Q = \mathbb{Z}^3/G$ under the form $\mathbb{Z}^r \times \mathbb{Z}/n_1\mathbb{Z} \times \ldots \times \mathbb{Z}/n_s\mathbb{Z}$ with $r, s \geq 0$ and $n_i \geq 2$. Give representatives in $\mathbb{Z}^3$ of a basis of the free part and generators for each of the cyclic groups in the decomposition.