M1 MIC – Algèbre – Examen

Jeudi 18 décembre 2025, 9h–12h

Les documents et le matériel électronique sont interdits. Les exercices sont indépendants les uns des autres. Toutes les réponses doivent être justifiées. Le barème est indicatif. Le sujet compte 7 pages et 6 exercices.

Exercice 1. Système diophantien (2 points)

Résoudre dans $\mathbb{Z}$ le système suivant :

$$\begin{cases} x \equiv 2 \pmod 6 \\ x \equiv 4 \pmod{10} \\ x \equiv 5 \pmod 7 \end{cases}$$

> **Solution:** On note que $6 \wedge 10 = 2$. Comme $2 \equiv 4 \pmod 2$, le système admet des solutions. Il est équivalent à :
>
> $$\begin{cases} x \equiv 2 \pmod 6 \\ x \equiv 4 \pmod 5 \\ x \equiv 5 \pmod 7 \end{cases}$$
>
> On note que $6 - 5 = 1$, et $2 \times 5 \times (-1) + 4 \times 6 \times 1 = 14$, donc le système formé par les deux premières équations est équivalent à $x \equiv 14 \pmod{30}$.
> Ensuite, d'après l'algorithme d'Euclide étendu, on trouve que $13 \times 7 - 3 \times 30 = 1$. De plus, $14 \times 7 \times 13 + 5 \times 30 \times (-3) = 824$. Ainsi, le système initial est équivalent à $x \equiv 824 \pmod{210}$, ou encore $x \equiv 194 \pmod{210}$.

Exercice 2. Arithmétique (3 points)

Soit p un nombre premier impair. On note $Q = X^8 - 16 \in \mathbb{Z}[X]$.

(a) Pourquoi est-ce que le symbole de Legendre $\left(\frac{4}{p}\right)$ vaut 1 ? ½ pt

> **Solution:** Comme p ne divise pas 4 et que 4 est un carré mod p (car c'est déjà un carré dans $\mathbb{Z}$), on a $\left(\frac{4}{p}\right) = 1$.

(b) En déduire que parmi les nombres -1, 2 et -2, au moins un est un carré modulo p. ½ pt

> **Solution:** On a :
>
> $$\left(\frac{4}{p}\right) = \left(\frac{-1}{p}\right) \times \left(\frac{-2}{p}\right) \times \left(\frac{2}{p}\right).$$
>
> Ces trois nombres ne peuvent pas être tous égaux à -1, car sinon leur produit serait -1. Par conséquent, au moins l'un d'entre eux est égal à 1, donc au moins l'un des nombres -1, 2 ou -2 est un carré modulo p.

(c) Décomposer le polynôme Q en produit de polynômes irréductibles dans $\mathbb{Z}[X]$, en démontrant que chaque facteur est effectivement irréductible. 1 pt
On pourra utiliser que $a^4 + 4b^4 = (a^2 - 2ab + 2b^2)(a^2 + 2ab + 2b^2)$.

Solution: On a :

$$Q = X^8 - 16 = (X^4 - 4)(X^4 + 4).$$

De plus,

$$X^4 - 4 = (X^2 - 2)(X^2 + 2),$$

et

$$X^4 + 4 = (X^2 - 2X + 2)(X^2 + 2X + 2).$$

Il reste à vérifier que les polynômes $X^2 - 2$, $X^2 + 2$, $X^2 - 2X + 2$ et $X^2 + 2X + 2$ sont irréductibles dans $\mathbb{Z}[X]$. Chacun de ces polynômes vérifie le critère d'Eisenstein avec le nombre premier 2. Par conséquent, ils sont irréductibles dans $\mathbb{Q}[X]$, et donc aussi dans $\mathbb{Z}[X]$ car ils sont primitifs.

(d) En déduire que Q admet une racine dans $\mathbb{F}_p$. 1 pt

Solution: D'après la partie (b), parmi les nombres -1, 2 et -2, au moins un est un carré modulo p.

— Si 2 est un carré modulo p, alors $X^2 - 2$ admet une racine dans $\mathbb{F}_p$, donc Q aussi.
— Si -2 est un carré modulo p, alors $X^2 + 2$ admet une racine dans $\mathbb{F}_p$, donc Q aussi.
— Enfin, si -1 est un carré modulo p, disons $i^2 = -1$, alors $1 + i$ et $1 - i$ sont des racines de $X^2 - 2X + 2$ dans $\mathbb{F}_p$, donc aussi de Q. (On peut s'aider de la résolution de l'équation $x^2 - 2x + 2 = 0$ dans $\mathbb{C}$ pour déterminer les racines – le discriminant vaut $-4 = (2i)^2$.)

Exercice 3. Anneaux et irréductibilité (4 points)

On considère l'ensemble $A = \{a + ib\sqrt{5} \mid a, b \in \mathbb{Z}\}$.
On munit A de l'application norme $N : A \to \mathbb{N}$ définie par $N(z) = z\bar{z} = a^2 + 5b^2$.

(a) Démontrer que A est un sous-anneau intègre de $\mathbb{C}$. ½ pt

Solution: Il est clair que $0, 1 \in A$. Soient $z = a + ib\sqrt{5}$ et $z' = a' + ib'\sqrt{5}$ dans A. On a :

$$z + z' = (a + a') + i(b + b')\sqrt{5} \in A,$$

et

$$zz' = (aa' - 5bb') + i(ab' + a'b)\sqrt{5} \in A.$$

Ainsi, A est un sous-anneau de $\mathbb{C}$. De plus, comme $\mathbb{C}$ est intègre, A l'est aussi.

(b) Démontrer que $z \in A$ est inversible si et seulement si $N(z) = 1$. 1 pt
En déduire le groupe des unités $A^\times$.

Solution: Soit $z = a + ib\sqrt{5} \in A$. Si z est inversible, il existe $z' = a' + ib'\sqrt{5} \in A$ tel que $zz' = 1$. En prenant les normes, on obtient :

$$N(z)N(z') = N(zz') = N(1) = 1.$$

Comme $N(z), N(z') \in \mathbb{N}$, on en déduit que $N(z) = 1$.
Réciproquement, si $N(z) = 1$, on a :

$$z\bar{z} = 1 \implies z^{-1} = \bar{z} = a - ib\sqrt{5} \in A.$$

Ainsi, z est inversible.
On cherche maintenant les éléments de norme 1. On a :

$$N(a + ib\sqrt{5}) = a^2 + 5b^2 = 1.$$

La seule solution entière est $(a, b) = (\pm 1, 0)$. Ainsi, le groupe des unités est $A^\times = \{1, -1\}$ qui est cyclique d'ordre 2.

(c) Calculer les normes des nombres suivants : 3, $2 + i\sqrt{5}$ et $2 - i\sqrt{5}$. ½ pt

Solution: On a :

$$N(3) = 3^2 + 5 \times 0^2 = 9,$$

$$N(2 + i\sqrt{5}) = 2^2 + 5 \times 1^2 = 4 + 5 = 9,$$

et

$$N(2 - i\sqrt{5}) = 2^2 + 5 \times (-1)^2 = 4 + 5 = 9.$$

(d) Démontrer que 3 est irréductible dans A. 1 pt

Solution: Supposons que 3 n'est pas irréductible. Il existe donc $x, y \in A$, non inversibles, tels que $3 = xy$. En prenant les normes, on obtient :

$$N(3) = N(x)N(y) \implies 9 = N(x)N(y).$$

Comme x et y ne sont pas inversibles, on a $N(x), N(y) \neq 1$. Les seules possibilités sont donc $(N(x), N(y)) = (3, 3)$ ou $(9, 1)$ ou $(1, 9)$. Les deux dernières possibilités sont impossibles car elles impliqueraient que l'un des deux éléments est inversible.
Il reste donc à examiner le cas $(N(x), N(y)) = (3, 3)$. On cherche les éléments de norme 3. On a :

$$N(a + ib\sqrt{5}) = a^2 + 5b^2 = 3.$$

Il n'existe pas de tels entiers. Ainsi, il n'existe pas de tels x, y, et donc 3 est irréductible dans A.

(e) Démontrer que 9 admet deux factorisations en irréductibles distinctes dans A. 1 pt
L'anneau A est-il factoriel ?

Solution: On a déjà vu que $N(3) = 9$ et que 3 est irréductible dans A. De plus, on a :

$$9 = (2 + i\sqrt{5})(2 - i\sqrt{5}).$$

Il reste à vérifier que $2 + i\sqrt{5}$ et $2 - i\sqrt{5}$ sont irréductibles dans A. Comme avant, vu que $N(2 + i\sqrt{5}) = 9$ et $N(2 - i\sqrt{5}) = 9$, les seules possibilités pour une éventuelle factorisation en éléments non inversibles seraient que les deux facteurs aient chacun une norme égale à 3. Or, on a déjà vu qu'il n'existe pas d'éléments de norme 3 dans A. Ainsi, $2 + i\sqrt{5}$ et $2 - i\sqrt{5}$ sont irréductibles dans A. On a donc deux factorisations distinctes de 9 en irréductibles dans A :

$$9 = 3 \times 3 = (2 + i\sqrt{5})(2 - i\sqrt{5}).$$

Comme $A^\times$ est réduit à $\{1, -1\}$, ces deux factorisations ne diffèrent pas seulement par des unités. Par conséquent, l'anneau A n'est pas factoriel.

Exercice 4. Corps finis (5 points)

Soit $P = X^3 + 2X + 1 \in \mathbb{F}_3[X]$.

(a) Démontrer que P est irréductible sur $\mathbb{F}_3$. 1 pt

> **Solution:** Il n'admet pas de racine dans $\mathbb{F}_3$ car :
>
> $$P(0) = 1, \quad P(1) = 1 + 2 + 1 = 1, \quad P(2) = 8 + 4 + 1 = 13 \equiv 1 \pmod 3.$$
>
> Comme P est de degré 3, il est irréductible dans $\mathbb{F}_3[X]$.

(b) On note $\mathbb{K} = \mathbb{F}_3[X]/(P)$. Justifier que $\mathbb{K}$ est un corps et préciser sa caractéristique. 1 pt

> **Solution:** L'anneau $\mathbb{F}_3[X]$ est un anneau principal car $\mathbb{F}_3$ est un corps. Comme P est irréductible dans $\mathbb{F}_3[X]$, l'idéal (P) est maximal. Par conséquent, le quotient $\mathbb{K} = \mathbb{F}_3[X]/(P)$ est un corps. La caractéristique de $\mathbb{K}$ est la même que celle de $\mathbb{F}_3$, c'est-à-dire 3.

(c) On note α la classe de X dans $\mathbb{K}$. Donner une base de $\mathbb{K}$ comme espace vectoriel sur $\mathbb{F}_3$. Quel est le cardinal de $\mathbb{K}$? 1/2 pt

> **Solution:** Une base est donnée par $(1, \alpha, \alpha^2)$. En effet, comme P est de degré 3, les classes des polynômes de degré inférieur à 3 forment un système de représentants des classes dans le quotient. Le cardinal de $\mathbb{K}$ est donc $3^3 = 27$.

(d) Calculer l'inverse de $\alpha + 1$ dans $\mathbb{K}$ dans la base précédente. 1 pt

> **Solution:** Dans le quotient, on a $\alpha^3 + 2\alpha + 1 = 0$, donc $\alpha^3 = -2\alpha - 1 = \alpha - 1$ (car $-2 \equiv 1 \pmod 3$). On en déduit que $\alpha(1 - \alpha^2) = 1$, donc l'inverse de $\alpha + 1$ est $\alpha - \alpha^2$.

(e) Le groupe multiplicatif $\mathbb{K}^\times$ est-il cyclique ? 1/2 pt
Quel est l'ordre possible d'un élément de ce groupe ?

> **Solution:** Oui, le groupe multiplicatif d'un corps fini est cyclique. Le cardinal de $\mathbb{K}^\times$ est $27 - 1 = 26$. Les diviseurs de 26 sont 1, 2, 13 et 26. Les ordres possibles d'un élément de $\mathbb{K}^\times$ sont donc 1, 2, 13 ou 26.

(f) Démontrer que α n'est ni d'ordre 2, ni 13. En déduire que α est un générateur de $\mathbb{K}^\times$. 1 pt

> **Solution:** Comme $(1, \alpha, \alpha^2)$ est une base de $\mathbb{K}$ sur $\mathbb{F}_3$, on a $\alpha \neq 1$ et $\alpha^2 \neq 1$. Ainsi, α n'est pas d'ordre 2.
> De plus, $\alpha^3 = \alpha - 1$, donc $\alpha^9 = (\alpha - 1)^3 = \alpha^3 - 1 = (\alpha - 1) - 1 = \alpha - 2 = \alpha + 1$. On a donc :
>
> $$\alpha^{13} = \alpha^9\alpha^3\alpha = (\alpha + 1)(\alpha - 1)\alpha = (\alpha^2 - 1)\alpha = \alpha^3 - \alpha = (\alpha - 1) - \alpha = -1.$$
>
> Ainsi, α n'est pas d'ordre 13. Par conséquent, l'ordre de α dans $\mathbb{K}^\times$ est 26, et donc α est un générateur de $\mathbb{K}^\times$.

Exercice 5. Théorie de Galois (4 points)

Soit $\mathbb{K} = \mathbb{Q}(\alpha, j)$ où $j = e^{2i\pi/3}$ et $\alpha = \sqrt[3]{2}$. On note $P(X) = X^3 - 2 \in \mathbb{Q}[X]$.

(a) Démontrer que $\mathbb{K}$ est le corps de décomposition de P sur $\mathbb{Q}$. 1/2 pt

Solution: Les racines de P dans $\mathbb{C}$ sont α, $j\alpha$ et $j^2\alpha$. Le corps de décomposition de P est donc $\mathbb{Q}(\alpha, j\alpha, j^2\alpha)$. Or, on a $j\alpha = j \cdot \alpha$ et $j^2\alpha = j^2 \cdot \alpha$. Ainsi, $\mathbb{Q}(\alpha, j\alpha, j^2\alpha) = \mathbb{Q}(\alpha, j)$. Par conséquent, $\mathbb{K}$ est le corps de décomposition de P sur $\mathbb{Q}$.

(b) Déterminer le degré de l'extension $[\mathbb{K} : \mathbb{Q}]$. 1 pt
En déduire l'ordre du groupe de Galois $G = \mathrm{Gal}(\mathbb{K}/\mathbb{Q})$.

Solution: Le polynôme $P(X) = X^3 - 2$ est irréductible dans $\mathbb{Q}[X]$ par le critère d'Eisenstein avec le nombre premier 2. Ainsi, $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$.
De plus, le polynôme minimal de j sur $\mathbb{Q}$ est $X^2 + X + 1$, qui est irréductible dans $\mathbb{Q}[X]$. Donc, $[\mathbb{Q}(j) : \mathbb{Q}] = 2$.
Comme $j \notin \mathbb{Q}(\alpha)$ (car $\mathbb{Q}(\alpha) \subset \mathbb{R}$), on a :

$$[\mathbb{K} : \mathbb{Q}] = [\mathbb{Q}(\alpha, j) : \mathbb{Q}] = [\mathbb{Q}(\alpha, j) : \mathbb{Q}(\alpha)] \cdot [\mathbb{Q}(\alpha) : \mathbb{Q}] = 2 \times 3 = 6.$$

L'extension $\mathbb{K}/\mathbb{Q}$ est donc de degré 6. Elle est de plus galoisienne car $\mathbb{K}$ est le corps de décomposition d'un polynôme sur $\mathbb{Q}$, donc normale, et séparable car $\mathbb{Q}$ est de caractéristique 0. Par le théorème fondamental de la théorie de Galois, l'ordre du groupe de Galois $G = \mathrm{Gal}(\mathbb{K}/\mathbb{Q})$ est égal au degré de l'extension, donc $|G| = 6$.

(c) On considère les automorphismes σ et τ de $\mathbb{K}$ définis par leur action sur les générateurs : ½ pt

$$\begin{cases} \sigma : \alpha \mapsto j\alpha, \quad j \mapsto j \\ \tau : \alpha \mapsto \alpha, \quad j \mapsto j^2 \end{cases}$$

Vérifier que σ et τ sont bien des éléments de G.

Solution: Pour vérifier que σ est un automorphisme de $\mathbb{K}$, il suffit de vérifier que σ préserve les relations algébriques des générateurs. On a :

$$\sigma(P(\alpha)) = \sigma(\alpha^3 - 2) = (j\alpha)^3 - 2 = j^3\alpha^3 - 2 = \alpha^3 - 2 = 0,$$

et

$$\sigma(j^2 + j + 1) = j^2 + j + 1 = 0.$$

Ainsi, σ est bien un automorphisme de $\mathbb{K}$.
De même, pour τ, on a :

$$\tau(P(\alpha)) = P(\alpha) = 0,$$

et

$$\tau(j^2 + j + 1) = (j^2)^2 + j^2 + 1 = j + j^2 + 1 = 0.$$

Ainsi, τ est aussi un automorphisme de $\mathbb{K}$.
Par conséquent, σ et τ sont bien des éléments de G.

(d) Calculer σ^3 et τ^2. Calculer $\tau\sigma\tau^{-1}$ et le comparer à σ^2. 1½ pts

Solution: On a :

$$\sigma^3 : \alpha \mapsto j^3\alpha = \alpha, \quad j \mapsto j,$$

donc $\sigma^3 = \mathrm{id}$.
De plus,

$$\tau^2 : \alpha \mapsto \alpha, \quad j \mapsto (j^2)^2 = j^4 = j,$$

donc $\tau^2 = \mathrm{id}$.
Ensuite,
$$\tau\sigma\tau^{-1} : \alpha \mapsto \tau(\sigma(\tau^{-1}(\alpha))) = \tau(\sigma(\alpha)) = \tau(j\alpha) = j^2\alpha,$$
et
$$j \mapsto \tau(\sigma(\tau^{-1}(j))) = \tau(\sigma(j^2)) = \tau(j^2) = j.$$
Ainsi, $\tau\sigma\tau^{-1} : \alpha \mapsto j^2\alpha, j \mapsto j$.
Par ailleurs,
$$\sigma^2 : \alpha \mapsto j^2\alpha, \quad j \mapsto j.$$
On en déduit que $\tau\sigma\tau^{-1} = \sigma^2$.

(e) À quel groupe connu G est-il isomorphe ? ½ pt

Solution: Le groupe G est engendré par σ et τ avec les relations $\sigma^3 = \mathrm{id}$, $\tau^2 = \mathrm{id}$ et $\tau\sigma\tau^{-1} = \sigma^2$. Ces relations sont exactement celles du groupe symétrique S_3, qui est le groupe des permutations de trois éléments. Par conséquent, G est isomorphe à S_3.

Exercice 6. Forme normale de Smith (2 points)

Soit la matrice
$$M = \begin{pmatrix} 2 & 6 & 4 \\ 4 & 6 & 2 \end{pmatrix} \in \mathcal{M}_{2,3}(\mathbb{Z}).$$

(a) En calculant $\Delta_1(M)$ et $\Delta_2(M)$, déterminer les facteurs invariants de M. ½ pt

Solution: On a :
$$\Delta_1(M) = \gcd(2, 6, 4, 4, 6, 2) = 2,$$
et
$$\Delta_2(M) = \gcd(\begin{vmatrix} 2 & 6 \\ 4 & 6 \end{vmatrix}, \begin{vmatrix} 2 & 4 \\ 4 & 2 \end{vmatrix}, \begin{vmatrix} 6 & 4 \\ 6 & 2 \end{vmatrix}) = \gcd(-12, -12, -24) = 12.$$
Ainsi, $\Delta_2(M) = 12$.
Les facteurs invariants sont donc $d_1 = \Delta_1(M) = 2$ et $d_2 = \frac{\Delta_2(M)}{\Delta_1(M)} = \frac{12}{2} = 6$.

(b) Déterminer la forme normale de Smith de la matrice M. On donnera les matrices inversibles U, V telles que UMV est la forme normale de Smith de M. 1 pt

Solution: L'application de l'algorithme donne :
$$U = \begin{pmatrix} -1 & 1 \\ 2 & -1 \end{pmatrix}, \quad V = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix}, \quad D = UMV = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 6 & 0 \end{pmatrix}.$$

(c) Soit $f : \mathbb{Z}^3 \to \mathbb{Z}^2$ l'application linéaire dont la matrice dans les bases canoniques est M. En déduire la structure du groupe abélien quotient $G = \mathbb{Z}^2/\mathrm{Im}(f)$ et un générateur de chaque facteur direct. ½ pt

Solution: D'après ce qui précède, on a :
$$G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}.$$

Les générateurs respectifs sont les colonnes de la matrice :

$$U^{-1} = \begin{pmatrix} 1 & 1 \\ 2 & 1 \end{pmatrix}$$