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 $(a) \cap (b) = (a \vee b)$.

C'est vrai. Raisonnons par double inclusion :

Si $x \in (a) \cap (b)$, alors x est un multiple de a et un multiple de b, donc c'est par définition un multiple de leur PPCM, et donc $x \in (a \vee b)$.

Si $x \in (a \vee b)$, alors c'est un multiple de $a \vee b$. Or, $a \vee b$ est un multiple de a et un multiple de b, donc par transitivité, x aussi, et donc $x \in (a) \cap (b)$.

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

C'est faux. Soit $A = \mathbb{Z}[X,Y]$ (qui est factoriel), $a = X$ et $b = Y$. Alors $a \wedge b = X \wedge Y = 1$, car si un polynôme divise X et Y, alors il est constant pour des raisons de degré. Mais $(X) + (Y) \neq (1) = A$. En effet, si $P \in (X) + (Y)$, alors $P(0,0) = 0$, donc $1 \notin (X) + (Y)$.

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

C'est vrai. Si $x \in (a) + (b)$, alors il existe $u, v \in A$ tels que $x = au + bv$. Chacun des deux termes de la somme est un multiple du PGCD $a \wedge b$, donc x aussi, et donc $x \in (a \wedge b)$. En d'autres termes, $(a) + (b) \subset (a \wedge b)$.

Réciproquement, comme l'anneau A est principal, il existe un élément $d \in A$ tel que $(a) + (b) = (d)$. En particulier, $a \in (d)$ et $b \in (d)$, donc d divise a et b, et en particulier d divise $a \wedge b$. On en déduit que $(a \wedge b) \subset (d) = (a) + (b)$ comme attendu.

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

C'est faux. Le polynôme constant $P = 2 \in \mathbb{Z}[X]$ est irréductible dans $\mathbb{Z}[X]$, mais il n'est pas irréductible dans $\mathbb{Q}[X]$ (car il y est inversible).

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

C'est vrai. C'est une conséquence du Corollaire II.D.13 : les polynômes irréductibles de $A[X]$ sont les constantes irréductibles et les polynômes primitifs de degré ≥ 1 irréductibles dans $K_A[X]$. Comme on a supposé que le polynôme n'est pas constant, on est donc dans le second cas.

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

C'est faux : il faut que P soit primitif. Par exemple, $P = 2X \in \mathbb{Z}[X]$ est irréductible dans $\mathbb{Q}[X]$ mais pas dans $\mathbb{Z}[X]$.

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 $\jmath = \exp(2i\pi/3)$ l'une des solutions de $1 + \jmath + \jmath^2 = 0$.

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

Il est clair que $A = \mathbb{Z}[\jmath]$ est stable par addition et qu'il contient $0 \in \mathbb{C}$ et $1 \in \mathbb{C}$. Pour la stabilité par multiplication, on note que $\jmath^2 = -\jmath - 1 \in \mathbb{Z}[\jmath]$. Enfin, pour la stabilité par conjugaison complexe, on a que $\bar{\jmath} = \jmath^2 = -\jmath - 1 \in \mathbb{Z}[\jmath]$.

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

On a que $\jmath\bar{\jmath} = |\jmath|^2 = 1$ et $\jmath + \bar{\jmath} = 2\,\mathrm{Re}(\jmath) = 2\cos(2\pi/3) = -1$, d'où :

$$\begin{aligned}\mathrm{N}(x + \jmath y) = (x + \jmath y)(x + \bar{\jmath} y) &= x^2 + (\jmath + \bar{\jmath})xy + \jmath\bar{\jmath} y^2 \\ &= x^2 + 2\,\mathrm{Re}(\jmath)\, xy + y^2 = x^2 - xy + y^2.\end{aligned}$$

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

On a :

$$\mathrm{N}(zz') = zz'\bar{z}\bar{z}' = z\bar{z}z'\bar{z}' = \mathrm{N}(z)\,\mathrm{N}(z').$$

Étant donnés $x, y \in \mathbb{Z}$, on a :

$$(x^2 - xy + y^2) - 3y^2/4 = x^2 - xy + y^2/4 = (x - y/2)^2 \geq 0.$$

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

D'une part, si $\mathrm{N}(z) = 1$, alors $z\bar{z} = 1$ et donc $z^{-1} = \bar{z} \in \mathbb{Z}[\jmath]$ est bien l'inverse de z. Réciproquement, si z est inversible, alors $\mathrm{N}(zz^{-1}) = 1 = \mathrm{N}(z)\,\mathrm{N}(z^{-1})$. Or, $\mathrm{N}(z)$ et $\mathrm{N}(z^{-1})$ sont tous les deux des entiers, donc si leur produit vaut 1, alors ils valent ± 1. Mais comme $\mathrm{N}(z) = |z|^2 \geq 0$, on en déduit que $\mathrm{N}(z) = 1$.

Supposons donc que $z = x + \jmath y$ est inversible. D'après la question précédente, on a :

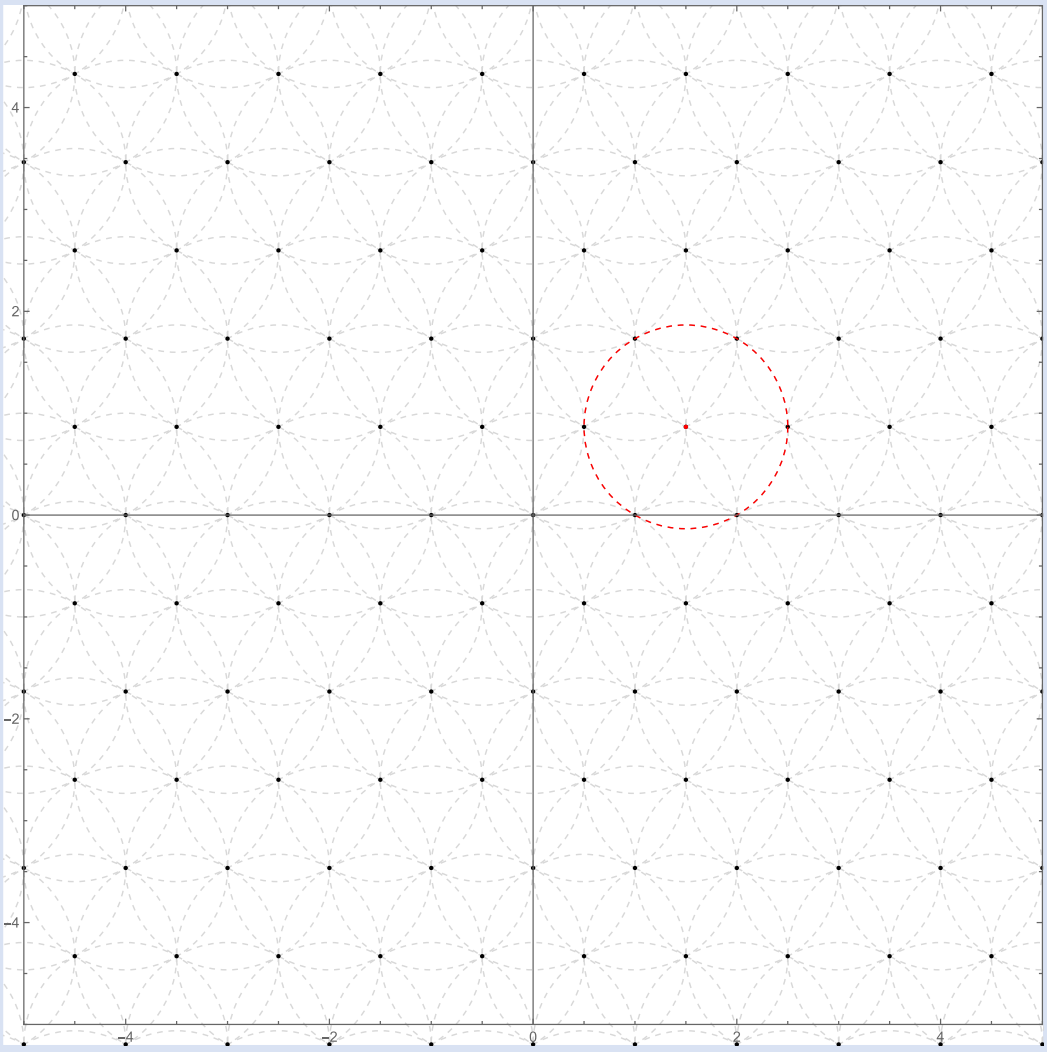
$$1 = \mathrm{N}(z) = x^2 - xy + y^2 \geq 3y^2/4.$$

On en déduit que $y^2 = 0$ ou $y^2 = 1$. Si $y^2 = 0$, alors $z = x$ est un entier dont le carré $z\bar{z} = x^2$ vaut 1, donc $z = \pm 1$. Si au contraire $y^2 = 1$, alors $y = \pm 1$. De manière symétrique, on peut démontrer que x

vaut 0, 1, ou -1. Les possibilités sont donc $z = \jmath$; $z = -\jmath$; $z = 1 + \jmath = -\jmath^2$; $z = -1 + \jmath$; $z = -1 - \jmath = \jmath^2$; $z = 1 - \jmath$. On vérifie que parmi ces possibilités, les seules de module $\mathrm{N}(z) = 1$ sont $\pm\jmath$ et $\pm\jmath^2$ (on a en revanche $\mathrm{N}(1 - \jmath) = \mathrm{N}(-1 + \jmath) = \sqrt{3}$).

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

On peut illustrer la situation par le dessin suivant, où les points noirs sont les points de $\mathbb{Z}[\jmath]$ et les cercles sont centrés en ces points et de rayon 1. Pour aider à la compréhension de l'illustration, un des points de $\mathbb{Z}[\jmath]$ et le cercle centré en ce point est dessiné en rouge.



Soit $B(w, 1) \subset \mathbb{C}$ le disque ouvert centré en $w \in \mathbb{C}$ de rayon 1. On pose :

$$A = \{\, z \in \mathbb{C} \mid \exists w \in \mathbb{Z}[\jmath] \text{ t.q. } |z - w| < 1 \,\} = \bigcup_{w \in \mathbb{Z}[\jmath]} B(w, 1).$$

Notre objectif est de démontrer que $A = \mathbb{C}$. On constate que $i\sqrt{3} \in \mathbb{Z}[\jmath]$, car on a $i\sqrt{3} = 1 + 2\jmath$. Donc, comme $\mathbb{Z}[\jmath]$ est un sous-anneau, pour tout $m, n \in \mathbb{Z}$, on a $w := m + ni\sqrt{3} \in \mathbb{Z}[\jmath]$. De plus, si $|x| < 1/2$ et $|y| < \sqrt{3}/2$, alors $|x + iy| < 1$. On en déduit que la boule $B(w, 1)$ contient le rectangle :

$$\left]m-\frac{1}{2},m+\frac{1}{2}\right[\times\left]n\sqrt{3}-\frac{\sqrt{3}}{2},n\sqrt{3}+\frac{\sqrt{3}}{2}\right[.$$

Elle contient de plus le bord de ce rectangle, sauf ses quatre coins ; mais les coins du rectangles $\left(m\pm 1/2,\sqrt{3}(n\pm 1/2)\right)$ sont des points de $\mathbb{Z}[j]$. On en déduit donc que le rectangle fermé est contenu dans A. La réunion de tous ces rectangles est égale à $\mathbb{C}$, CQFD.

(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.

Soit $P=X^2-X+1$. Comme $\deg(P)=2$, ce polynôme est irréductible si et seulement s'il n'a pas de racines.

Traitons à part le cas $p=2$. Si $p=2$, alors le polynôme $P:=X^2-X+1$ n'a pas de racine (il n'y a que deux éléments à vérifier).

Supposons maintenant $p\neq 2$. L'élément $2\in\mathbb{F}_p$ est donc inversible, et P est irréductible si et seulement si $4P$ est irréductible. On peut alors « compléter le carré » :

$$(2X-1)^2=4X^2-4X+1\Longrightarrow 4P=4(X^2-X+1)=(2X-1)^2+3.$$

Donc si $P(\alpha)=0$, alors $(2\alpha-1)^2+3\equiv 0\pmod p$ et donc -3 est un carré mod p. Réciproquement, si -3 est un carré mod p, disons $\beta^2\equiv -3\pmod p$, alors $\alpha=(\beta+1)/2$ est une racine de P modulo p. En conclusion, P admet une racine si et seulement si -3 est un carré mod p, ou encore si et seulement si le symbole de Legendre $\left(\frac{-3}{p}\right)$ vaut 1.

C'est bien sûr le cas si $p=3$ (et on a alors $X^2-X+1=(X+1)^2$) donc supposons $p\neq 3$. D'après la loi de réciprocité quadratique, on a toujours $\left(\frac{-3}{p}\right)=\left(\frac{p}{3}\right)$ (on peut procéder par disjonction des cas suivant si p est congru à 1 ou -1 mod 4). Ce symbole ne dépend que de p mod 3, et on a $\left(\frac{1}{3}\right)=1$ et $\left(\frac{2}{3}\right)=-1$.

Donc finalement, le polynôme P admet une racine si et seulement si $p=3$ ou $p\equiv 1\pmod 3$; il est irréductible si et seulement si $p\equiv 2\pmod 3$.

(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 $\mathbb{Z}[j]$.

Si on développe, on a :

$$(x+j)(x+\bar{j})=x^2-2\,\mathrm{Re}(j)\,x+j\bar{j}=x^2-x+1.$$

D'après la question précédente, si $p\equiv 1\pmod 3$, le polynôme X^2-X+1 admet une racine mod p. Cette racine est représentée par un nombre entier $x\in\mathbb{Z}$ tel qu'il existe $k\in\mathbb{Z}\subset\mathbb{Z}[j]$ avec $x^2-x+1=pk$. On a donc bien que p divise $x^2-x+1=(x+j)(x+\bar{j})$ dans $\mathbb{Z}[j]$.

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

Supposons au contraire que p est irréductible dans $\mathbb{Z}[\jmath]$. Alors d'après le lemme de Gauss, p divise $x+\jmath$ ou $x+\bar{\jmath}$ dans $\mathbb{Z}[\jmath]$, c'est-à-dire qu'il existe des entiers $a, b \in \mathbb{Z}$ tels que $p(a+b\jmath) = x+\jmath$ ou $p(a+b\jmath) = x+\bar{\jmath}$. En identifiant les parties imaginaires, on en déduit que $pb\sqrt{3}/2 = \pm\sqrt{3}/2$, ou encore $pb = \pm 1$, ce qui est absurde car p est premier. Donc p est réductible dans $\mathbb{Z}[\jmath]$.

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

Comme $p \in \mathbb{Z}[\jmath]$ est réductible, on peut écrire $p = z_1 z_2$ où z_1 et z_2 ne sont pas inversibles. On a donc $p^2 = \mathrm{N}(p) = \mathrm{N}(z_1)\,\mathrm{N}(z_2)$. Comme z_1, z_2 ne sont pas inversibles, $\mathrm{N}(z_1), \mathrm{N}(z_2) \neq 1$, donc on a $\mathrm{N}(z_1) = \mathrm{N}(z_2) = p$. On peut donc prendre $z_0 = z_1$ ou z_2.

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

Si $\mathrm{N}(z_0) = p$, comme $\mathrm{N}(\jmath) = 1$, alors $\mathrm{N}(\jmath^{\pm 1} z_0) = \mathrm{N}(\bar{\jmath}^{\pm 1} z_0) = p$. Parmi les cinq nombres $\{z_0, \jmath^{\pm 1} z_0,\ \jmath^{\pm 1}\bar{z}_0\}$, au moins un est de la forme $m + 2n\jmath = a + bi\sqrt{3}$ avec $m, n \in \mathbb{Z}$, donc quitte à échanger on peut prendre $z_0 = a + bi\sqrt{3}$. Alors $\mathrm{N}(z_0) = a^2 + 3b^2 = p$.

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 $\mathbb{R}$?

On peut appliquer le critère d'Eisenstein : $p = 3$ est irréductible et divise tous les coefficients non-dominants de P, et $p^2 = 9$ ne divise pas $P(0)$. Le polynôme P est donc irréductible sur $\mathbb{Q}$. Il est réductible sur $\mathbb{R}$, car $P\left(\sqrt[4]{3}\right) = 0$.

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

Le corps de décomposition $\mathbb{K}$ est engendré par les racines $\pm\sqrt[4]{3}, \pm i\sqrt[4]{3}$ de P, donc on a bien $\mathbb{K} \subset \mathbb{Q}\left(\sqrt[4]{3}, i\right)$. Réciproquement, $\sqrt[4]{3}$ appartient bien à $\mathbb{K}$, et $i = \left(i\sqrt[4]{3}\right)/\left(\sqrt[4]{3}\right)$ appartient aussi à $\mathbb{K}$, donc $\mathbb{Q}\left(\sqrt[4]{3}, i\right) \subset \mathbb{K}$.

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

Soit $\alpha = \sqrt[4]{3}$. Une base de $\mathbb{K}$ est donnée par $(1, \alpha, \alpha^2, \alpha^3, i, i\alpha, i\alpha^2, i\alpha^3)$. Le degré $[\mathbb{K}\colon \mathbb{Q}]$ vaut donc 8.

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

L'extension est normale car c'est le corps de décomposition d'un polynôme. Elle est séparable car la caractéristique de $\mathbb{Q}$ est nulle.

Le cardinal du groupe de Galois $\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$ vaut donc 8.

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

Le degré de l'extension $[\mathbb{Q}(i)\colon \mathbb{Q}]$ vaut 2. L'extension est galoisienne car c'est le corps de décomposition de $X^2 + 1$. Le groupe de Galois est donc de cardinal 2, c'est donc un groupe isomorphe à $\mathbb{Z}/2\mathbb{Z}$. Ses deux éléments sont l'identité et la conjugaison complexe.

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

Le groupe $\mathrm{Gal}\big(\mathbb{K}/\mathbb{Q}(i)\big)$ est un sous-groupe de $\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$: si $\sigma \in \mathrm{Gal}\big(\mathbb{K}/\mathbb{Q}(i)\big)$ est un automorphisme tel que $\sigma|_{\mathbb{Q}(i)}$ est l'identité, alors $\sigma|_{\mathbb{Q}}$ est aussi l'identité, et donc $\sigma \in \mathrm{Gal}(\mathbb{K}/\mathbb{Q})$. Ce sous-groupe est de plus distingué, car la sous-extension $\mathbb{Q} \subset \mathbb{Q}(i)$ de $\mathbb{Q} \subset \mathbb{K}$ est normale. Le groupe quotient $\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$ / $\mathrm{Gal}\big(\mathbb{K}/\mathbb{Q}(i)\big)$ est isomorphe au groupe de Galois $\mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q})$.

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.

On applique l'algorithme vu en cours et en TD. On commence par s'occupe de la première ligne par l'algorithme d'Euclide étendu :

$$\begin{pmatrix} 20 & 8 & 4 \\ -10 & -4 & -2 \\ 8 & 2 & 4 \end{pmatrix} \xrightarrow{C_1 \leftrightarrow C_3} \begin{pmatrix} 4 & 8 & 20 \\ -2 & -4 & -10 \\ 4 & 2 & 8 \end{pmatrix}$$
$$\xrightarrow{C_2 \leftarrow C_2 - 2C_1} \begin{pmatrix} 4 & 0 & 20 \\ -2 & 0 & -10 \\ 4 & -6 & 8 \end{pmatrix}$$
$$\xrightarrow{C_3 \leftarrow C_3 - 5C_1} \begin{pmatrix} 4 & 0 & 0 \\ -2 & 0 & 0 \\ 4 & -6 & -12 \end{pmatrix}$$

Puis la première colonne :

$$\begin{pmatrix} 4 & 0 & 0 \\ -2 & 0 & 0 \\ 4 & -6 & -12 \end{pmatrix} \xrightarrow{L_1 \leftrightarrow L_2} \begin{pmatrix} -2 & 0 & 0 \\ 4 & 0 & 0 \\ 4 & -6 & -12 \end{pmatrix}$$
$$\xrightarrow{L_2 \leftarrow L_2 + 2L_1} \begin{pmatrix} -2 & 0 & 0 \\ 0 & 0 & 0 \\ 4 & -6 & -12 \end{pmatrix}$$
$$\xrightarrow{L_3 \leftarrow L_3 + 2L_1} \begin{pmatrix} -2 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & -6 & -12 \end{pmatrix}$$

On a terminé avec la première ligne et la première colonne. On s'occupe ensuite de la deuxièmie ligne : il n'y a besoin de rien faire. Puis on s'occupe de la deuxième colonne, puis de la deuxième ligne à nouveau :

$$\begin{pmatrix} -2 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & -6 & -12 \end{pmatrix} \xrightarrow{L_2 \leftrightarrow L_3} \begin{pmatrix} -2 & 0 & 0 \\ 0 & -6 & -12 \\ 0 & 0 & 0 \end{pmatrix}$$
$$\xrightarrow{C_3 \leftarrow C_3 - 2C_2} \begin{pmatrix} -2 & 0 & 0 \\ 0 & -6 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

On obtient bien la forme normale de Smith de M, de facteurs invariants $(-2, -6, 0)$.

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

Pour répondre à cette question et à la suivante, il faut récupérer les matrices unimodulaires $U, V \in \mathrm{GL}_3(\mathbb{Z})$ telles que $UMV = D = \mathrm{diag}(-2, -6, 0)$ à partir des opérations élémentaires effectuées précédemment. Les opérations sur les colonnes correspondent à des multiplications à droite (la matrice V), les opérations à gauche correspondent à des multiplications à gauche (la matrice U).

Un manière simple de « garder en tête » les opérations pour obtenir à la fin les matrices U et V est d'appliquer les opérations à une matrice « doublement augmentée » qui commence par $(\ I_3 \mid M \mid I_3\ )$ et se termine par $(\ U \mid D \mid V\ )$, en effectuant en parallèle les opérations sur les lignes sur la matrice de gauche, et les opérations sur les colonnes sur la matrice de droite.

$$\left(\begin{array}{ccc|ccc|ccc} 1 & 0 & 0 & 20 & 8 & 4 & 1 & 0 & 0 \\ 0 & 1 & 0 & -10 & -4 & -2 & 0 & 1 & 0 \\ 0 & 0 & 1 & 8 & 2 & 4 & 0 & 0 & 1 \end{array}\right) \xrightarrow{C_1 \leftrightarrow C_3} \left(\begin{array}{ccc|ccc|ccc} 1 & 0 & 0 & 4 & 8 & 20 & 0 & 0 & 1 \\ 0 & 1 & 0 & -2 & -4 & -10 & 0 & 1 & 0 \\ 0 & 0 & 1 & 4 & 2 & 8 & 1 & 0 & 0 \end{array}\right)$$

$$\xrightarrow{C_2 \leftarrow C_2 - 2C_1} \left(\begin{array}{ccc|ccc|ccc} 1 & 0 & 0 & 4 & 0 & 20 & 0 & 0 & 1 \\ 0 & 1 & 0 & -2 & 0 & -10 & 0 & 1 & 0 \\ 0 & 0 & 1 & 4 & -6 & 8 & 1 & -2 & 0 \end{array}\right)$$

$$\xrightarrow{C_3 \leftarrow C_3 - 5C_1} \left(\begin{array}{ccc|ccc|ccc} 1 & 0 & 0 & 4 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & -2 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 4 & -6 & -12 & 1 & -2 & -5 \end{array}\right)$$

$$\xrightarrow{L_1 \leftrightarrow L_2} \left(\begin{array}{ccc|ccc|ccc} 0 & 1 & 0 & -2 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 4 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 4 & -6 & -12 & 1 & -2 & -5 \end{array}\right)$$

$$\xrightarrow{L_2 \leftarrow L_2 + 2L_1} \left(\begin{array}{ccc|ccc|ccc} 0 & 1 & 0 & -2 & 0 & 0 & 0 & 0 & 1 \\ 1 & 2 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 4 & -6 & -12 & 1 & -2 & -5 \end{array}\right)$$

$$\xrightarrow{L_3 \leftarrow L_3 + 2L_1} \left(\begin{array}{ccc|ccc|ccc} 0 & 1 & 0 & -2 & 0 & 0 & 0 & 0 & 1 \\ 1 & 2 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 2 & 1 & 0 & -6 & -12 & 1 & -2 & -5 \end{array}\right)$$

$$\xrightarrow{L_2 \leftrightarrow L_3} \left(\begin{array}{ccc|ccc|ccc} 0 & 1 & 0 & -2 & 0 & 0 & 0 & 0 & 1 \\ 0 & 2 & 1 & 0 & -6 & -12 & 0 & 1 & 0 \\ 1 & 2 & 0 & 0 & 0 & 0 & 1 & -2 & -5 \end{array}\right)$$

$$\xrightarrow{C_3 \leftarrow C_3 - 2C_2} \left(\begin{array}{ccc|ccc|ccc} 0 & 1 & 0 & -2 & 0 & 0 & 0 & 0 & 1 \\ 1 & 2 & 1 & 0 & -6 & 0 & 0 & 1 & -2 \\ 0 & 2 & 0 & 0 & 0 & 0 & 1 & -2 & -1 \end{array}\right)$$

On trouve donc $U = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 2 & 1 \\ 1 & 2 & 0 \end{pmatrix}$ et $V = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & -2 \\ 1 & -2 & -1 \end{pmatrix}$ telles que $UMV = D$.

Les colonnes non-nulles de $U^{-1}D$ représentent une base de G. On calcule par les méthodes habituelles que $U^{-1} = \begin{pmatrix} -2 & 0 & 1 \\ 1 & 0 & 0 \\ -2 & 1 & 0 \end{pmatrix}$. Une base de G est donnée par les deux vecteurs colonnes $\begin{pmatrix} 4 \\ -2 \\ 4 \end{pmatrix}$ et $\begin{pmatrix} 0 \\ 0 \\ -6 \end{pmatrix}$.

(c) ★ Décomposer le quotient $Q = \mathbb{Z}^3/G$ sous la forme $\mathbb{Z}^r \times \mathbb{Z}/n_1\mathbb{Z} \times \ldots \times \mathbb{Z}/n_s\mathbb{Z}$ 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.

D'après ce qui précède, $Q = \mathbb{Z}^3/G$ est isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}$. Un générateur de $\mathbb{Z}/2\mathbb{Z}$ est représenté par la première colonne de U^{-1}, un représentant de $\mathbb{Z}/6\mathbb{Z}$ par la seconde colonne de U^{-1}, et une base de la partie libre par la troisième colonne de U^{-1}.

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 $A[X]$.

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 $\jmath = \exp(2i\pi/3)$ be one of the solutions of $1 + \jmath + \jmath^2 = 0$.

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

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

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

(e) Prove that for all $z \in \mathbb{C}$, there exists $w \in \mathbb{Z}[\jmath]$ such that $|z - w| < 1$. A drawing can help. Deduce that $\mathbb{Z}[\jmath]$ 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 $1 \bmod 3$. Prove that there exists $x \in \mathbb{Z}$ such that p divides the product $(x + \jmath)(x + \bar{\jmath})$ in $\mathbb{Z}[\jmath]$.

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

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

(j) By considering the set $\{\jmath^{\pm 1} z_0,\ \jmath^{\pm 1}\bar{z}_0\}$, 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.

---

[1] Unique Factorization Domain = "*anneau factoriel*" in French.

[2] Principal Ideal Domain = "*anneau principal*" in French.

(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 $[\mathbb{K}: \mathbb{Q}]$ 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 $\mathrm{Gal}\left(\mathbb{K}/\mathbb{Q}(i)\right)$?

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.