Examen

Algèbre – M1 MIC

lundi 6 janvier 2024

Durée : 3h. Les documents et le matériel informatique ne sont pas autorisés.
Lisez tout le sujet avant de commencer.

Exercice 1. Soit $p > 3$ un nombre premier. On suppose que :

- Il n'existe pas d'entier x tel que $x^2 \equiv 2 \pmod{p}$.
- Il n'existe pas d'entier y tel que $y^2 \equiv p \pmod{3}$.

Démontrer qu'il existe un entier z tel que $z^2 \equiv -6 \pmod{p}$.

Réponse : Comme p est premier, il existe une solution à $z^2 \equiv -6 \pmod{p}$ si et seulement si le symbole de Legendre vérifie $\left(\frac{-6}{p}\right) = 1$ (ce ne serait pas nécessairement le cas si p n'était pas premier). Le symbole de Legendre étant multiplicatif, on a :

$$\left(\frac{-6}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)\left(\frac{3}{p}\right).$$

D'après les hypothèses, on a $\left(\frac{2}{p}\right) = -1$ et $\left(\frac{p}{3}\right) = -1$. On a deux cas possibles.

- Si $p \equiv 1 \pmod{4}$, alors par réciprocité quadratique on a $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = 1$ et $\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right) = -1$, d'où $\left(\frac{-6}{p}\right) = (-1) \cdot 1 \cdot (-1) = 1$.
- Si $p \equiv 3 \pmod{4}$, alors $\left(\frac{-1}{p}\right) = -1$ et $\left(\frac{3}{p}\right) = -\left(\frac{p}{3}\right) = 1$ d'où encore $\left(\frac{-6}{p}\right) = 1$.

Exercice 2. On considère $A = \{a + ib\sqrt{13} \mid a, b \in \mathbb{Z}\}$.

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

Réponse : Il suffit de vérifier tous les axiomes, pas de difficulté particulière.

On considère $N : A \to \mathbb{N}$ définie par $N(a + ib\sqrt{13}) = a^2 + 13b^2$.

(b) Démontrer que pour tout $z, z' \in A$, on a $N(zz') = N(z)N(z')$.

Réponse : On peut faire le calcul à la main, ou bien noter que $N(z) = z\bar{z}$, donc :

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

(c) Démontrer que $N(z) = 1$ si et seulement si z est inversible.

Réponse : Si $N(z) = 1$, alors $b = 0$ (car sinon $N(z) \geq 13$) et $a^2 = 1$ d'où $z = \pm 1$ est inversible.
Réciproquement, si z est inversible, disons $zz^{-1} = 1$, alors on a $1 = N(zz^{-1}) = N(z)N(z^{-1})$. Donc $N(z)$ est un entier positif inversible, d'où $N(z) = 1$.

(d) Est-ce que A contient des éléments de norme 2, de norme 11 ?

Réponse : Non, il n'en contient pas. En effet, pour $z = a + ib\sqrt{13}$, si $b \neq 0$ alors $N(z) \geq 13b^2 \geq 13$. Si au contraire $b = 0$, alors $N(z) = a^2$ est un carré, et 2 et 11 ne sont pas des carrés.

(e) En déduire que 2, 11, $3 + i\sqrt{13}$ et $3 - i\sqrt{13}$ sont irréductibles dans A.

Réponse : Ces quatre éléments sont respectivement de normes $4 = 2^2$, $121 = 11^2$, $22 = 2 \times 11$ et $22 = 2 \times 11$. Si par exemple 2 était réductible, disons $2 = zz'$ avec z et z' non inversibles, alors on aurait $N(z)N(z') = 4$, d'où $N(z) = N(z') = 2$, ce qui est impossible. Le raisonnement est similaire pour les trois autres.

(f) En déduire que A n'est pas factoriel.

Réponse : On a l'équation :

$$2 \times 11 = 22 = (3 + i\sqrt{13})(3 - i\sqrt{13}).$$

Chacun des termes des deux produits est inversible. De plus, ces éléments ne sont pas associés deux à deux (les seuls éléments inversibles sont 1 et -1, donc deux éléments sont inversibles si et seulement si ils sont égaux ou opposés). On a donc deux factorisations non équivalentes de 22 dans A, d'où A n'est pas factoriel.

Exercice 3. Soit $n = 2^\alpha$ une puissance de 2 avec $\alpha \geq 1$. Démontrer que le polynôme $X^n + 1$ est irréductible sur $\mathbb{Z}$. (Indication : critère d'Eisenstein.)

Réponse : Le polynôme $P = X^n + 1$ est irréductible si et seulement si $Q = P(X + 1)$ l'est. Or, par la formule du binôme de Newton,

$$Q = X^{2^\alpha} + \binom{2^\alpha}{1} X^{2^\alpha - 1} + \cdots + \binom{2^\alpha}{2^\alpha - 1} X + 2.$$

Or pour $0 < k < 2^\alpha$, le coefficient binomial $\binom{2^\alpha}{k}$ est pair. On peut donc appliquer le critère d'Eisenstein avec $p = 2$.

Exercice 4. On note $\Phi_n \in \mathbb{Z}[X]$ le $n$ième polynôme cyclotomique. On rappelle qu'ils sont irréductibles sur $\mathbb{Z}$ et que l'on a l'équation $X^n - 1 = \prod_{d|n} \Phi_d$ pour tout $n \geq 1$.

(a) Écrire les factorisations de $X^2 - 1$, $X^3 - 1$, $X^6 - 1$ et $X^{12} - 1$ en fonction des polynômes cyclotomiques et indiquer les degrés des polynômes cyclotomiques qui apparaissent.

Réponse : On a :

$$\begin{aligned} X^2 - 1 &= \Phi_1\Phi_2, \\ X^3 - 1 &= \Phi_1\Phi_3, \\ X^6 - 1 &= \Phi_1\Phi_2\Phi_3\Phi_6, \\ X^{12} - 1 &= \Phi_1\Phi_2\Phi_3\Phi_4\Phi_6\Phi_{12}. \end{aligned}$$

D'après la formule on a aussi $X^1 - 1 = \Phi_1$ qui est de degré 1. En comptant les degrés, on a donc $\deg(\Phi_2) = 1$, $\deg(\Phi_3) = 3$, $\deg(\Phi_6) = 2$, $\deg(\Phi_4) = 2$ et enfin $\deg(\Phi_{12}) = 2$.

(b) Calculer le polynôme cyclotomique Φ_{12}.

Réponse : En faisant des divisions de polynômes, on trouve successivement :

$$\begin{aligned} \Phi_2 &= X + 1, & \Phi_3 &= X^2 + X + 1, \\ \Phi_4 &= X^2 + 1, & \Phi_6 &= X^2 - X + 1, \\ \Phi_{12} &= X^4 - X^2 + 1. \end{aligned}$$

On note $\zeta = e^{2i\pi/12} = \frac{\sqrt{3}+i}{2}$ une racine primitive douzième de l'unité et $\mathbb{Q}(\zeta)$ l'extension de $\mathbb{Q}$ engendrée par ζ.

(c) Quel est le degré de l'extension $[\mathbb{Q}(\zeta) : \mathbb{Q}]$?

Réponse : On peut le calculer à la main, ou bien (cours) utiliser le fait que le polynôme minimal de ζ est Φ_{12} qui est de degré 4, donc $[\mathbb{Q}(\zeta) : \mathbb{Q}] = 4$.

(d) Démontrer que $\mathbb{Q}(\zeta)$ est le corps de décomposition de $X^{12} - 1$ sur $\mathbb{Q}$. En déduire que $\mathbb{Q}(\zeta)$ est une extension galoisienne de $\mathbb{Q}$ et l'ordre de son groupe de Galois.

Réponse : Les racines de $X^{12} - 1$ sont les racines douzièmes de l'unité, qui sont toutes des puissances de ζ, et on a $X^{12}-1 = \prod_{k=0}^{11}(X-\zeta^k)$. Donc $\mathbb{Q}(\zeta)$ est engendré par les racines de $X^{12} - 1$ qui est scindé dans cette extension.
D'après le cours, un cours de décomposition est une extension normale du corps de base. De plus, $\mathbb{Q}$ est de caractéristique nulle, donc parfait, donc l'extension est séparable. Elle est donc bien galoisienne. L'ordre de son groupe de Galois est donc le degré de l'extension, à savoir 4.

(e) Quel sont les éléments $(\mathbb{Z}/12\mathbb{Z})^\times$? Est-ce que ce groupe est cyclique ?

Réponse : Ce sont les classes d'entiers premiers avec 12, donc

$$(\mathbb{Z}/12\mathbb{Z})^\times = \{[1], [5], [7], [11]\}.$$

Ce groupe n'est pas cyclique : il ne contient aucun élément d'ordre 4 (tous ses éléments vérifient $x^2 = 1$). D'après le cours, on a même $(\mathbb{Z}/12\mathbb{Z})^\times \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$.

(f) Étant donné $k \in (\mathbb{Z}/12\mathbb{Z})^\times$, on note σ_k l'unique automorphisme de $\mathbb{Q}(\zeta)$ tel que $\sigma_k(\zeta) = \zeta^k$. Démontrer que $k \mapsto \sigma_k$ est un isomorphisme de groupes $(\mathbb{Z}/12\mathbb{Z})^\times \to \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$.

Réponse : Il faut déjà démontrer que cette application définit un morphisme de groupe. On a $\sigma_1(\zeta) = \zeta$, et l'identité est un automorphisme de $\mathbb{Q}(\zeta)$ qui envoie ζ sur ζ, donc σ_1 est l'identité. De plus, $(\sigma_k \circ \sigma_l)(\zeta) = \sigma_k(\zeta^l) = (\sigma_k(\zeta))^l = (\zeta^k)^l = \zeta^{kl} = \sigma_{kl}(\zeta)$, donc c'est un morphisme de groupes.
Pour démontrer que c'est un isomorphisme, comme les deux groupes ont le même cardinal, il suffit de démontrer qu'il est injectif. Or, si $k \not\equiv l \pmod{12}$, alors $\sigma_k(\zeta) = \zeta^k \neq \zeta^l = \sigma_l(\zeta)$, donc le morphisme est bien injectif.

Exercice 5. (a) Lister toutes les matrices de taille 2×2 à coefficients entiers et de déterminant 10 sous forme normale de Smith.

Réponse :
$$\begin{pmatrix} \pm 1 & 0 \\ 0 & \pm 10 \end{pmatrix}.$$

On considère la matrice :
$$M = \begin{pmatrix} 2 & 6 \\ 3 & 4 \end{pmatrix} \in M_2(\mathbb{Z}).$$

(b) Déterminer la forme normale de Smith de M.

Réponse : On peut appliquer l'algorithme du pivot de Gauss à coefficients entiers, ou bien utiliser la question précédente : la forme normale de Smith est $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 10 \end{smallmatrix}\right)$.

(c) Résoudre dans $\mathbb{Z}$ le système d'équations linéaires :

$$\begin{cases} 2x + 6y &= 52, \\ 3x + 4y &= 23. \end{cases}$$

Réponse : Unique solution : $x = -7$, $y = 11$.

(d) On considère $u = (2, 3)$ et $v = (6, 4)$ dans $\mathbb{Z}^2$. Démontrer que $\mathbb{Z}^2/\langle u, v\rangle$ est un groupe fini et l'exprimer comme un produit de groupes cycliques.

Réponse : Le groupe est isomorphe à $\mathbb{Z}/10\mathbb{Z}$ d'après ce qui précède.