Aix–Marseille Université 2019-2020

Mathématiques – M1

TDS

1 Polynômes

Exercice 1 Trouver le pgcd dans $\mathbb{Z}/3\mathbb{Z}[X]$ de $f = X^4 + 1$, $g = X^3 + X + 1$.

Exercice 2 Montrer que f est irréductible dans $\mathbb{Q}[X]$ en utilisant le critère d'Eisenstein :

1. $f = X^4 - 8X^3 + 12X^2 - 6X + 2$;
2. $f = X^5 - 12X^3 + 36X - 12$;
3. $f = X^4 - X^3 + 2X + 1$;
4. $f = X^{p-1} + \cdots + X + 1$, où p est premier.

Exercice 3 On considère les trois matrices I, J, K suivantes.

$$I = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, J = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}, K = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

Soit $\mathbb{H}$ l'ensemble des matrices de la forme $aId + bI + cJ + dK$ avec a, b, c, d réels.

1. Montrer que $\mathbb{H}$ est un corps. Montrer que c'est un espace vectoriel sur $\mathbb{R}$.
2. Trouver un automorphisme de ce corps.
3. Montrer que $A \to \sqrt{detA\overline{A}}$ est une norme.

Exercice 4 Soit $E = \{a + b\sqrt{2}, (a, b) \in \mathbb{Q}\}$

1. Montrer que E est un sous corps de $\mathbb{C}$.
2. Déterminer les automorphismes de E.

Exercice 5 Soit E le $\mathbb{Q}$ espace vectoriel engendré par $1, \sqrt{2}, \sqrt{3}$.

1. Montrer qu'il est de dimension trois.
2. Soit F le $\mathbb{Q}(\sqrt{2})$ espace vectoriel engendré par $1, \sqrt{3}$. Montrer qu'il est de de dimension deux.

3. En déduire que F est un $\mathbb{Q}$ espace vectoriel de dimension quatre. On utilisera le fait que $\mathbb{Q}(\sqrt{2})$ est un corps.

Exercice 6 Soit E le $\mathbb{Q}$ espace vectoriel engendré par $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$.

1. On considère l'endomorphisme de E donné par $f : x \mapsto (\sqrt{2}+\sqrt{3})x$. Écrire la matrice de f dans la base $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$.
2. Calculer le polynôme caractéristique de f.
3. En utilisant le théorème de Cayley Hamilton en déduire un polynôme annulateur de $\sqrt{2} + \sqrt{3}$.

Exercice 7 Montrer que $[\mathbb{Q}(\sqrt{2}, 2^{1/3}) : \mathbb{Q}] = 6$. En déduire qu'il est égal à $\mathbb{Q}(2^{1/6})$

2 Anneau et corps

Exercice 8 On considère l'ensemble

$$\mathbb{Z}[i] = \{a + ib, a, b \in \mathbb{Z}\}$$

1. Montrer que c'est un anneau intègre.
2. Montrer que $z \mapsto \overline{z} = a - ib$ est un automorphisme d'anneaux.
3. Montrer que $z \mapsto N(z) = z\overline{z}$ est multiplicative.
4. Trouver $\mathbb{Z}[i]^*$.
5. Montrer que l'anneau est euclidien relativement à N. On utilisera la notion d'entier le plus proche d'un réel.

Exercice 9 On considère l'ensemble

$$\Sigma = \{n \in \mathbb{N} | n = a^2 + b^2; a, b \in \mathbb{N}\}$$

1. Montrer que si $n = 3 \mod 4$ alors n n'appartient pas à Σ.
2. Montrer que l'ensemble est stable par multiplication.
3. Montrer qu'il suffit de trouver les entiers $n \in \Sigma$ premier, notés p.
4. Montrer que $p \in \Sigma$ si et seulement si p n'est pas irréductible dans $\mathbb{Z}[i]$.
5. Montrer que $\mathbb{Z}[i]/(p) \sim \mathbb{F}_p[X]/(X^2 + 1)$.
6. En déduire que $p \in \Sigma$ si et seulement si -1 est un carré de $\mathbb{F}_p$.

Exercice 10 Pour $n \in \mathbb{N}^*$, soit $\mathcal{P}_n$ l'ensemble des racines n-èmes primitives de l'unité dans $\mathbb{C}$. On pose $\Phi_1(X) = X - 1$ et $\Phi_n(X) = \prod_{\zeta \in \mathcal{P}_n} (X - \zeta)$. Φ_n est appelé *le n-ème polynôme cyclotomique* (son degré est $\varphi(n)$ où φ est l'indicateur d'Euler).

1. Démontrer : $(\forall\, n \in \mathbb{N}^*)\ X^n - 1 = \prod_{d|n} \Phi_d(X)$.
2. En déduire, par récurrence, que $\Phi_n(X)$ a tous ses coefficients dans $\mathbb{Z}$.
3. Calculer explicitement $\Phi_n(X)$ pour $n \leq 16$.
4. Démontrer que, pour p premier et $\alpha \in \mathbb{N}^*$, $\Phi_{p^\alpha}(X) = \sum_{k=0}^{p-1} X^{kp^{\alpha-1}}$.
5. Montrer que le degré de Φ_n est égal à $\varphi(n)$.
6. Montrer que, si $d < n$ et d divise n, alors $X^d - 1$ divise $X^n - 1$ dans $\mathbb{Z}[X]$, puis que $\Phi_n(X)$ divise $X^n - 1$ et $\frac{X^n-1}{X^d-1}$ dans $\mathbb{Z}[X]$.

Exercice 11

1. Montrer que $\mathbb{Q}[\sqrt{7}], \mathbb{Q}[\sqrt{11}]$ sont des corps. Montrer que ce sont des espaces vectoriels sur $\mathbb{Q}$ de dimension 2.
2. Montrer que l'application suivante n'est pas un morphisme de corps

$$\begin{array}{ccc} \mathbb{Q}[\sqrt{7}] & \mapsto & \mathbb{Q}[\sqrt{11}] \\ a + b\sqrt{7} & \mapsto & a + b\sqrt{11} \end{array}$$

3. Montrer que ces corps ne sont pas isomorphes.

Exercice 12 Soit k un corps et P un polynôme sur k de degré n. Soit K un corps contenant k, tel que ce soit un espace vectoriel sur k de dimension m.

1. Si P est irréductible sur k de degré n et x une racine de P dans K, montrer que $m \geq n$ en considérant $k[x]$.
2. Si $P = QR$ montrer qu'un des deux polynômes Q, R est de degré inférieur à $n/2$. Considérer un de ses facteurs irréductibles et montrer que P a une racine dans un corps de dimension inférieure à $n/2$.

On a donc montré que P est irréductible sur k s'il n'a pas de racine dans une extension de degré inférieur à $n/2$.

Exercice 13 En utilisant les réductions $\mod 2$ ou $\mod 3$ montrer que les polynômes suivant sont irréductibles dans $\mathbb{Z}[X]$:

$$X^5 - 6X^3 + 2X^2 - 4X + 5, 7X^4 + 8X^3 + 11X^2 - 24X - 455.$$

Exercice 14 Soit α un nombre algébrique.

1. Montrer qu'il existe un unique polynôme de $\mathbb{Q}[X]$ de degré minimal et de coefficient dominant 1 annulant α.
2. En déduire que si Q est un polynôme rationnel satisfaisant $Q(\alpha) \neq 0$ il existe un polynôme h de $\mathbb{Q}[X]$ tel que $\frac{1}{Q(\alpha)} = h(\alpha)$.
3. En déduire que $\mathbb{Q}(\alpha)$ est un $\mathbb{Q}$ espace vectoriel de dimension finie.

3 Corps finis

Exercice 15 Déterminer à isomorphisme près tous les corps de cardinal 4.

Exercice 16 Soit p un nombre premier. Montrer qu'il y a $\frac{p(p-1)}{2}$ polynômes irréductibles de degré deux dans $\mathbb{Z}/p\mathbb{Z}[X]$.

Exercice 17 Résoudre dans $\mathbb{Z}/5\mathbb{Z}$ l'équation $X^2 - 3X + a = 0$ en fonction de a.

Exercice 18 Montrer que $X^2 + X + 1$ est irréductible sur $\mathbb{F}_5$.

Trouver les polynômes irréductibles de degré inférieur ou égal à 4 sur $\mathbb{F}_2$.

Exercice 19 Soit $\mathbb{K}$ un corps de caractéristique p et $f : x \mapsto x^k$.

Trouver des conditions pour que ce soit une bijection.

Exercice 20 Donner une description des éléments du groupe des inversibles de $\mathbb{F}_9$.

Exercice 21 On considère des corps à 16 éléments.

1. Montrer que $\mathbb{Z}_2[X]/(X^4 + X + 1)$ est isomorphe à un tel corps.
2. Montrer que $\mathbb{Z}_2[X]/(X^4 + X^3 + 1)$ est isomorphe à un tel corps.
3. Trouver le groupe des inversibles de chacun de ces corps en fonction de la classe de X.
4. Trouver les isomorphismes entre ces deux corps.

Exercice 22 Le but est de montrer que -1 est un carré de $\mathbb{F}_p$ si et seulement si $p = 2$ ou $p = 1 \mod 4$. Soit F^2 l'ensemble des éléments de $\mathbb{F}_p^*$ qui s'écrivent comme carré d'un élément.

1. Montrer que $x \in F^2 \iff x^{(p-1)/2} = 1$:
   (a) Considérer $x \mapsto x^2$. Montrer que c'est un morphisme et calculer son noyau.

(b) Conclure par un argument de cardinalité.

2. En déduire le résultat.

Exercice 23 Le but est de montrer que Φ_8 est réductible dans tout corps fini.

1. Donner la décomposition de Φ_8 dans $\mathbb{F}_2$.
2. Donner la décomposition de Φ_8 dans $\mathbb{F}_3$.
3. Écrire toutes les décompositions possibles de Φ_8 comme produit de deux polynômes de degré deux sur $\mathbb{C}$.
4. Montrer que pour tout nombre premier $p \geq 3$ si x est racine de Φ_8 dans $\mathbb{F}_p$ alors x est racine primitive de $X^8 - 1$.
5. Montrer que le groupe $\mathbb{F}_{p^2}^*$ contient toujours un élément d'ordre 8. On admettra que ce groupe est cyclique. En déduire que Φ_8 admet une racine sur $\mathbb{F}_{p^2}$.
6. Déduire que Φ_8 est réductible dans $\mathbb{F}_p$ en utilisant un exercice précédent.

4 Cercles et droites

Exercice 24 Montrer que l'on peut construire un carré d'aire $2a^2$ connaissant un carré d'aire a^2.

Exercice 25 Montrer que l'on peut diviser un angle en deux parties égales à la règle et au compas.

Exercice 26 Montrer que l'on peut diviser un segment en n parties égales à la règle et au compas.

Exercice 27 Etant donné un cercle, montrer que l'on ne peut construire un carré de même aire que le disque.

Exercice 28 Construire un pentagone régulier à la règle et au compas.

5 Théorie de Galois

Exercice 29 Déterminer les corps de décomposition sur $\mathbb{Q}$ de $X^4 + 1, X^4 - 2$.

Exercice 30 Soit $a = (1-\sqrt{2})^{1/3}$. Montrer que a est algébrique sur $\mathbb{Q}$ et exprimer $\frac{1}{a^2+1}$.

Exercice 31 Soit a une racine complexe de $X^2 + 2X + 5$. Exprimer $\frac{a^3+a+2}{a^2-1}$ en fonction de a.

Exercice 32 On considère $\alpha = \sqrt{2} + \sqrt{5}$ et $K = \mathbb{Q}(\sqrt{2}, \sqrt{5})$.

1. Montrer que K est une extension galoisienne de $\mathbb{Q}$.
2. Trouver le cardinal du groupe de Galois et montrer qu'il possède deux éléments d'ordre deux.
3. En déduire le groupe de Galois et trouver les extensions intermédiaires entre $\mathbb{Q}$ et K.

Exercice 33

1. Montrer que toute extension de $\mathbb{Q}$ de degré deux est galoisienne.
2. Soit ω_n une racine n-ème primitive de l'unité. Montrer que $\mathbb{Q}(\omega_n)$ est galoisienne.
3. Montrer que si $K = \mathbb{Q}[\sqrt{5}]$, alors $L = \mathbb{Q}[\sqrt{2+\sqrt{5}}]$ est galoisienne sur K mais pas sur $\mathbb{Q}$.

Exercice 34 Soit $\alpha = 2^{1/3}$ et $K = \mathbb{Q}[j, \alpha]$ le corps de décomposition de $X^3 - 2$.

1. Montrer que K est une extension galoisienne de $\mathbb{Q}$ et déterminer le cardinal du groupe de Galois.
2. Montrer que l'on peut trouver deux éléments f, g du groupe de Galois en définissant.
$$f(\alpha) = \alpha f(j) = j^2, g(\alpha) = j\alpha, g(j) = j$$
3. Montrer que $g^2 = f^{-1}gf$. En déduire le groupe de Galois.
4. Trouver les extensions intermédiaires entre $\mathbb{Q}$ et K.

Exercice 35 Soit $z = e^{2i\pi/5}$.

1. Montrer que $X^4 + X^3 + X^2 + X + 1$ est irréductible dans $\mathbb{Q}[X]$
2. Calculer le polynôme minimal de z sur $\mathbb{Q}$.
3. En déduire que $\mathbb{Q}(z)$ est une extension galoisienne. Trouver son degré.
4. Montrer que
$$\begin{array}{ccc} \mathbb{Q}(z) & \to & \mathbb{Q}(z) \\ a + bz + cz^2 + dz^3 + ez^4 & \to & a + bz^2 + cz^4 + dz + ez^3 \end{array}$$
est un $\mathbb{Q}$ automorphisme de $\mathbb{Q}(z)$.

5. Calculer le groupe de Galois de $\mathbb{Q}(z)$.
6. En déduire un corps intermédiaire entre $\mathbb{Q}$ et $\mathbb{Q}(z)$.

.

Exercice 36 On considère le polynôme cyclotomique Φ_n et ω_n une racine n-ème primitive de l'unité.

Montrer que le corps de décomposition de Φ_n est égal à $\mathbb{Q}(\omega_n)$. En déduire que le groupe de Galois de Φ_n est le groupe des inversibles de $\mathbb{Z}/n\mathbb{Z}$.