1 Niveau 1

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. $f = X^{p-1} + \dots + X + 1$, où p est premier.

Exercice 3 Exprimer à l'aide des polynômes symétriques fondamentaux :

1. $(x_1^2 + x_2^2)(x_1^2 + x_3^2)(x_2^2 + x_3^2)$;
2. $(x_1 + x_2)(x_1 + x_3)(x_1 + x_4)(x_2 + x_3)(x_2 + x_4)(x_3 + x_4)$;
3. $(x_1 + x_2 - x_3 - x_4)(x_1 - x_2 + x_3 - x_4)(x_1 - x_2 - x_3 + x_4)$.

Exercice 4 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 $\mathbb{C}$ est un espace vectoriel sur $\mathbb{R}$.
2. Trouver un automorphisme de ce corps.
3. Montrer que $A \rightarrow \sqrt{A\bar{A}}$ est une norme.

Exercice 5 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 6 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 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 7 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 8 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 Niveau 2

Exercice 9 On considère un polynôme $P(X) = a_n X^n + \dots + a_0$. On note $\sigma_i, S_i, 1 \leq i \leq n$ les polynômes symétriques fondamentaux et les sommes de Newton en les racines de P .

1. Montrer que l'on a pour tout entier $h \leq n$:

$$(-1)^h h \sigma_h = \sum_{i=0}^{h-1} (-1)^{-i-1} \sigma_i S_{h-i}.$$

On commencera par le cas $h = n$.

2. Montrer que l'on a pour tout entier $h \geq n + 1$:

$$0 = \sum_{i=0}^n (-1)^{-i-1} \sigma_i S_{h-i}.$$

3. Montrer que l'on a pour tout entier $i \leq n$:

$$a_n S_i = (-1)^i a_{n-1} \sigma_1 + \dots + a_1 \sigma_{i-1} + (-1)^{i-1} i a_{n-i}.$$

4. Vérifier les formules pour $P(X) = X^2 - X + 1$ et pour $Q(X) = (X - 1)(X - 2)(X + 1)$.

Exercice 10 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 $z \mapsto \bar{z} = a - ib$ est un automorphisme d'anneaux.
3. Montrer que $z \mapsto N(z) = z\bar{z}$ 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 11 On considère l'ensemble

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

1. Montrer que si $n \equiv 3 \pmod{4}$ 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 12 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 13

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

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

3. Montrer que ces corps ne sont pas isomorphes.

3 Niveau 3

Exercice 14 Nombres p -adiques.

Soit p un nombre premier. On considère $v_p : \mathbb{Z} \rightarrow \mathbb{N}$ la valuation p -adique définie par $v_p(n) = k$ si p^k divise n et p^{k+1} ne divise pas n . On pose $v_p(n) = +\infty$ si p ne divise pas n . On étend v_p en une fonction définie sur $\mathbb{Q}$ par $v_p(\frac{a}{b}) = v_p(a) - v_p(b)$. On définit enfin $|r|_p = p^{-v_p(r)}$ la valeur absolue p -adique. On pose $\mathbb{Q}_p$ le complété de $\mathbb{Q}$ pour cette distance.

1. Montrer que $|\cdot|_p$ définit une norme sur $\mathbb{Q}_p$.
2. Montrer que la suite $(p^n)_n$ converge et que si $q \neq p$ est un nombre premier, alors la suite $(\frac{1}{q^n})_n$ diverge.
3. Montrer que pour qu'une série converge dans $\mathbb{Q}_p$ il suffit que le terme général tende vers zéro.
4. On définit enfin $\mathbb{Z}_p$ comme le complété de $\mathbb{Z}$. Montrer que le corps des fractions de $\mathbb{Z}_p$ est égal à $\mathbb{Q}_p$.

Exercice 15 On considère p un nombre premier et l'anneau $\mathbb{Z}/p^n\mathbb{Z}$. On définit alors le morphisme de $\mathbb{Z}/p^{n+1}\mathbb{Z}$ dans $\mathbb{Z}/p^n\mathbb{Z}$ par la réduction modulo p^n . On considère alors les suites $(a_n)_{n \in \mathbb{N}}$ d'éléments vérifiant $a_n \in \mathbb{Z}/p^n\mathbb{Z}$ et $a_{n+1} = a_n \pmod{p^n}$.

1. Montrer que ces suites possèdent une structure d'anneau.
2. Définir un isomorphisme avec $\mathbb{Z}_p$.
3. On pourra montrer que, si $p = 2, 7$ est représenté par $(1, 3, 7, 7, \dots, 7, \dots)$. Trouver l'inverse de 7.

Exercice 16 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 17 (Application du précédent) 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 18 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 annihilant 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.