TD Polynômes, arithmétique

Polynômes en une indéterminée

Exercice 1

Soit A un anneau commutatif, F, G des polynômes de $A[X]$ avec G unitaire de degré $d \geq 1$.

1. Montrer par récurrence sur le degré de F qu'il existe un unique couple de polynômes (Q, R) de $A[X]$ tels que $F = QG + R$ avec $\deg R < d$.
2. Montrer sur un exemple la nécessité de supposer G unitaire.
3. On note x la classe de X dans $A[X]/(G)$. Montrer que tout élément y de $A[X]/(G)$ s'écrit de manière unique sous la forme $y = \sum_{i=0}^{d-1} a_i x^i$ avec $a_0, \ldots, a_{d-1} \in A$.
   (On dit que $(1, x, \ldots, x^{d-1})$ est une base du A-module $A[X]/(G)$.)

Exercice 2

Dans $\mathbf{Z}[X]$, déterminer le reste dans la division euclidienne de $P = (X+1)^n + (X-1)^n$ par les polynômes suivants : X ; $X-1$; X^2 ; $(X-1)^2$; X^2-1 ; $(X+1)(X-1)^2$. À quelle condition X^2+1 divise-t-il P ?

Exercice 3 (Division selon les puissances croissantes)

Soient A un anneau commutatif et F, G des polynômes de $A[X]$ avec $G(0) \in A^\times$.

1. Pour tout $p \in \mathbf{N}$, montrer qu'il existe un unique couple de polynômes (Q, R) de $A[X]$ tels que $F = QG + X^{p+1}R$ avec $\deg Q \leq p$.
2. Soit $\theta \in \mathbf{R}$. Diviser selon les puissances croissantes à l'ordre $p \in \mathbf{N}$ le polynôme $F = 1 - X\cos\theta$ par $G = 1 - 2X\cos\theta + X^2$ dans $\mathbf{R}[X]$.

Exercice 4

Soit P un polynôme de $\mathbf{R}[X]$ tel que $P(x) \geq 0$ pour tout $x \in \mathbf{R}$. Montrer qu'il existe $A, B \in \mathbf{R}[X]$ tels que $P = A^2 + B^2$. Cette écriture est-elle unique (à permutation et aux signes près de A et B) ?

Exercice 5 (Racines sur le cercle unité)

On s'intéresse dans cet exercice à calculer le nombre de racines d'un polynôme $P \in \mathbf{R}[X]$ sur le cercle unité $U = \{z \in \mathbf{C} : |z| = 1\}$.

1. Montrer que l'application $t \mapsto (t-i)/(t+i)$ définit une bijection de $\mathbf{R}$ vers un sous-ensemble de U que l'on précisera.
2. Soit $P \in \mathbf{R}[X]$ un polynôme de degré $n \geq 1$. Montrer qu'il existe un unique couple de polynômes (A, B) de $\mathbf{R}[X]$ tels que
$$(t+i)^n P\Big(\frac{t-i}{t+i}\Big) = A(t) + iB(t) \qquad (t \in \mathbf{R}).$$
3. En déduire une méthode pour calculer le nombre de racines de P dans U.
4. Déterminer le nombre de racines du polynôme $X^4 - 2X^3 - 2X + 1$ dans U.

Polynômes en plusieurs indéterminées

Exercice 6

Soit A un anneau intègre. Montrer la formule $\deg(PQ) = \deg(P) + \deg(Q)$ pour tous polynômes non nuls $P, Q \in A[X_1, \ldots, X_n]$.

Exercice 7

Soient A un anneau intègre infini. Montrer par récurrence sur n que pour toutes parties infinies $S_1, \ldots, S_n$ de A et tout polynôme $P \in A[X_1, \ldots, X_n]$, si P s'annule sur $S_1 \times \cdots \times S_n$ alors $P = 0$.

Exercice 8

Soit K un corps. Monter que si $P \in K[X]$ n'est pas un carré, alors $Y^2 - P(X)$ est irréductible dans $K[X, Y]$.

Exercice 9

Soit K un corps. Montrer les isomorphismes d'anneaux suivants :

(a) $K[X, Y]/(Y - X^2) \cong K[X]$;

(b) $K[X, Y]/(Y^2 - X^3) \cong K[T^2, T^3]$. *Indication.* Considérer $X \mapsto T^2$ et $Y \mapsto T^3$.

Exercice 10

Exprimer les polynômes suivants de $\mathbf{Z}[X, Y, Z]$ en termes des polynômes symétriques élémentaires : $X^2 + Y^2 + Z^2$; $X^2(Y + Z) + Y^2(X + Z) + Z^2(X + Y)$.

Exercice 11

Pour tout monôme P de $\mathbf{Z}[X_1, \ldots, X_n]$, le *symétrisé* ΣP de P est la somme des éléments de l'orbite de P sous l'action du groupe $\mathfrak{S}_n$.

1. Montrer que le polynôme symétrique élémentaire Σ_k $(1 \leq k \leq n)$ est le symétrisé d'un monôme.
2. Montrer que tout polynôme symétrique $P \in \mathbf{Z}[X_1, \ldots, X_n]$ est combinaison linéaire à coefficients dans $\mathbf{Z}$ de monômes symétrisés.
3. Exprimer en termes des polynômes symétriques élémentaires les polynômes suivants, à l'aide de la méthode de Waring :

   (a) ΣX_1^2 $(n \geq 2)$;

   (b) $\Sigma X_1^2 X_2$, ΣX_1^3 $(n \geq 3)$;

   (c) $\Sigma X_1^2 X_2 X_3$, $\Sigma X_1^2 X_2^2$, $\Sigma X_1^3 X_2$, ΣX_1^4 $(n \geq 4)$.

Exercice 12

Soit $P \in \mathbf{Z}[X]$ unitaire. On pose $P = \prod_{i=1}^{d}(X - \alpha_i)$ avec $\alpha_i \in \mathbf{C}$. Pour tout entier $n \geq 1$, on définit $\Delta_n(P) = \prod_{i=1}^{d}(\alpha_i^n - 1)$.

1. Montrer que $\Delta_n(P) \in \mathbf{Z}$.
2. Calculer $\Delta_2(P)$ et $\Delta_3(P)$ pour $P = X^3 - X - 1$.
3. Montrer que si $P(0)P(1) \neq 0$, alors $\limsup_{n\to\infty} |\Delta_n(P)|^{1/n} = \displaystyle\prod_{i=1}^{d} \max(1, |\alpha_i|)$.

Exercice 13 (Formules de Newton)

Soit A un anneau commutatif et $n \geq 2$. Pour tout entier $k \geq 0$, on pose $S_k = \sum_{i=1}^n X_i^k \in A[X_1, \ldots, X_n]$ (avec la convention $S_0 = n$).

1. Exprimer les coefficients de $F = \prod_{i=1}^n (T - X_i) \in A[X_1, \ldots, X_n][T]$ en termes des polynômes symétriques élémentaires.
2. Soit B un anneau commutatif et $P = T^n + \sum_{k=0}^{n-1} b_k T^k \in B[T]$. Pour tout $c \in B$, donner explicitement le quotient et le reste de la division euclidienne de P par $T - c$.
3. En déduire une expression de $F/(T - X_i)$ en termes des polynômes symétriques élémentaires.
4. En exprimant de deux manières le polynôme dérivé de F par rapport à T, démontrer les relations suivantes

$$S_k + \sum_{j=1}^{k-1} (-1)^j \Sigma_j S_{k-j} + (-1)^k k \Sigma_k = 0 \qquad (1 \leq k \leq n).$$

5. En évaluant $T^{k-n} F$ en X_i, montrer que

$$S_k + \sum_{j=1}^{n} (-1)^j \Sigma_j S_{k-j} = 0 \qquad (k \geq n).$$

6. On suppose que $A = K$ est un corps de caractéristique 0. Montrer que la K-algèbre des polynômes symétriques de $K[X_1, \ldots, X_n]$ est engendrée par $S_1, \ldots, S_n$.

Exercice 14

Soit $\Delta = \prod_{1 \leq i < j \leq n} (X_i - X_j) \in \mathbf{Z}[X_1, \ldots, X_n]$.

1. Montrer que Δ est antisymétrique : pour tout $\sigma \in \mathfrak{S}_n$, on a $\sigma \cdot \Delta = \varepsilon(\sigma)\Delta$.
2. Pour $n = 2$ et $n = 3$, exprimer Δ^2 en termes des polynômes symétriques élémentaires.
3. Montrer que tout polynôme $P \in \mathbf{Z}[X_1, \ldots, X_n]$ antisymétrique s'écrit de manière unique $P = \Delta \cdot Q$ avec $Q \in \mathbf{Z}[X_1, \ldots, X_n]$ symétrique (on pourra commencer par le cas $n = 2$).

Exercice 15

Soit K un corps et $P \in K[X_1, \ldots, X_n]$ un polynôme homogène non nul.

1. On suppose $P = FG$ avec $F, G \in K[X_1, \ldots, X_n]$. Montrer que F et G sont homogènes.
2. En déduire que la décomposition en irréductibles de P dans $K[X_1, \ldots, X_n]$ ne fait intervenir que des polynômes homogènes.
3. Montrer que $X_1^2 + \ldots + X_n^2$ est irréductible dans $\mathbf{R}[X_1, \ldots, X_n]$ si $n \geq 2$.
4. Le polynôme $X_1^2 + \ldots + X_n^2$ est-il irréductible dans $\mathbf{C}[X_1, \ldots, X_n]$?

Exercice 16

Soit $P \in K[X_1, \ldots, X_n]$ un polynôme homogène symétrique, que l'on écrit sous la forme $P = Q(\Sigma_1, \ldots, \Sigma_n)$. Le polynôme Q est-il alors homogène ?

Exercice 17

Soit I un idéal de $K[X_1, \ldots, X_n]$.

1. On suppose que I est engendré par des polynômes homogènes $P_1, \ldots, P_r$ avec $r \geq 1$. Montrer que si P est dans I, alors les composantes homogènes de P le sont aussi.

2. Réciproquement, supposons que $P \in I$ entraîne que toutes les composantes homogènes de P sont dans I. Montrer que I est engendré par des polynômes homogènes.

Exercice 18

Le but de cet exercice est de montrer que le polynôme $P = X^n - X - 1$ est irréductible dans $\mathbf{Q}[X]$ pour $n \geq 2$.

1. Traiter les cas $n = 2$ et $n = 3$.
2. On suppose $n \geq 4$. Montrer que les racines de P dans $\mathbf{C}$ sont simples et n'appartiennent pas à $\mathbf{Q}$.
3. Si Q est un diviseur de P dans $\mathbf{Z}[X]$, on pose

$$S(Q) = \sum_{Q(z)=0} z - \frac{1}{z}.$$

   Montrer que $S(Q) \in \mathbf{Z}$. Que vaut $S(P)$?
4. On suppose $P = QR$ avec $Q, R \in \mathbf{Q}[X]$ unitaires de degré ≥ 2. Montrer que Q et R sont dans $\mathbf{Z}[X]$.
5. Si z est une racine de P, montrer que $\Re(z - \frac{1}{z}) > \frac{1}{|z|^2} - 1$.
6. En déduire $S(Q) \geq 1$ et conclure.

Arithmétique dans Z

Exercice 19

Déterminer le pgcd et une relation de Bézout pour les entiers suivants : $(21, 34)$; $(220, 284)$; $(10; 142857)$; $(10, 12, 15)$; $(2^n - 1, 2^n + 1)$ avec $n \geq 1$.

Exercice 20

1. Résoudre la congruence $8x \equiv 6 \pmod{50}$.
2. Résoudre le système de congruences

$$\begin{cases} x \equiv 1 \pmod 7 \\ x \equiv 4 \pmod 9 \\ x \equiv 3 \pmod 5. \end{cases}$$

Exercice 21

Résoudre les problèmes suivants du *Liber Abaci* de Fibonacci (1202).

1. *"Il y a un nombre qui, divisé par 2, ou 3, ou 4, ou 5, ou 6, a toujours un reste de 1, et il est divisible par 7. Quel est ce nombre ?"*
2. *"Il y a aussi un nombre qui, divisé par 2, a un reste de 1 ; divisé par 3, a un reste de 2 ; divisé par 4, a un reste de 3, et ainsi de suite jusqu'à 10 ; quand le nombre est divisé par 10, il a un reste de 9 ; le nombre est divisible par 11. Quel est-il ?"*

Exercice 22

Soit $a, b, m \in \mathbf{Z}$. Montrer que la congruence $ax \equiv b \pmod m$ a une solution dans $\mathbf{Z}$ si et seulement si $\text{pgcd}(a, m)$ divise b. Donner dans ce cas la solution générale.

Exercice 23

Soit $a, b, c \in \mathbf{Z}$. On considère l'équation $ax + by = c$ avec $x, y \in \mathbf{Z}$.

1. Montrer que cette équation a une solution si et seulement si $\mathrm{pgcd}(a,b)$ divise c.
2. On suppose que $(x_0, y_0) \in \mathbf{Z}^2$ est une solution. Montrer que la solution générale est donnée par $x = x_0 + tb/d$ et $y = y_0 - ta/d$ avec $d = \mathrm{pgcd}(a,b)$ et $t \in \mathbf{Z}$.

Exercice 24

Soit $a, b \geq 1$. Posons $d = \mathrm{pgcd}(a,b)$ et $m = \mathrm{ppcm}(a,b)$. Montrer les identités $\phi(a)\phi(b) = \phi(d)\phi(m)$ et $\phi(ab)\phi(d) = d\phi(a)\phi(b)$, où ϕ est l'indicatrice d'Euler.

Exercice 25

Montrer que les nombres de Fermat $F_n = 2^{2^n} + 1$ $(n \geq 0)$ sont deux à deux premiers entre eux. En déduire qu'il existe une infinité de nombres premiers.

Exercice 26

1. Montrer que $1 + \frac{1}{2} + \cdots + \frac{1}{n} \notin \mathbf{Z}$ pour $n \geq 2$.
2. Montrer que tout p premier ≥ 3 divise le numérateur de $1 + \frac{1}{2} + \cdots + \frac{1}{p-1}$.
3. Montrer que pour tout $k \in \{1, \ldots, (p-1)/2\}$, il existe un unique $\ell \in \{1, \ldots, (p-1)/2\}$ tel que $\frac{1}{k(p-k)} = -\ell^2 + h$ où le numérateur de h est divisible par p.
4. Montrer que si p est premier ≥ 5, alors p^2 divise le numérateur de $1 + \frac{1}{2} + \cdots + \frac{1}{p-1}$.

Exercice 27

1. Pour tout n impair, montrer $n^2 \equiv 1 \pmod 8$.
2. Pour tout n non divisible par 3, montrer $n^2 \equiv 1 \pmod 3$.
3. Pour tout $n \in \mathbf{Z}$, montrer $n^5 \equiv n \pmod{30}$ et $n^7 \equiv n \pmod{42}$.

Exercice 28

Pour un entier $n \geq 1$, on considère la congruence $x^2 \equiv 1 \pmod{10^n}$.

1. Résoudre cette congruence pour $n \in \{1, 2, 3\}$.
2. Déterminer le nombre de solutions de cette congruence pour n quelconque.
3. Soit $n \geq 1$. Montrer qu'il existe un entier naturel A de n chiffres tel que l'écriture décimale de A^2 se termine par A. En trouver pour $n = 1, 2, 3$.

Exercice 29 (Lemme de Hensel)

Soit p un nombre premier et $P \in \mathbf{Z}[X]$. On suppose qu'il existe $x_1 \in \mathbf{Z}$ tel que $P(x_1) \equiv 0 \pmod p$ et $P'(x_1) \not\equiv 0 \pmod p$.

1. Montrer qu'il existe une suite d'entiers $(x_n)_{n\geq 2}$ telle que $P(x_n) \equiv 0 \pmod{p^n}$ et $x_{n+1} \equiv x_n \pmod{p^n}$ pour tout $n \geq 1$.
2. Montrer que si deux suites (x_n) et (y_n) vérifient les conditions ci-dessus alors $x_n \equiv y_n \pmod{p^n}$ pour tout n.
3. *Application.* On suppose p impair. Soit $a \in \mathbf{Z}$ tel que la classe de a dans $\mathbf{Z}/p\mathbf{Z}$ est un carré non nul. Pour tout $n \geq 1$, montrer que la congruence $x^2 \equiv a \pmod{p^n}$ possède exactement deux solutions dans $\mathbf{Z}/p^n\mathbf{Z}$.

Exercice 30

Soit $P \in \mathbf{Z}[X]$ unitaire. On pose $P = \prod_{i=1}^{d}(X - \alpha_i)$ avec $\alpha_i \in \mathbf{C}$. Pour tout entier $n \geq 1$, on définit $\Delta_n(P) = \prod_{i=1}^{d}(\alpha_i^n - 1)$. On a vu dans l'exercice 12 que $\Delta_n(P) \in \mathbf{Z}$.

Montrer que si P est réciproque (c'est-à-dire $P(x) = x^d P(1/x)$), alors $|\Delta_n(P)/\Delta_1(P)|$ est un carré pour tout n impair, et $|\Delta_n(P)/\Delta_2(P)|$ est un carré pour tout n pair.

Indication. Pour n pair, utiliser $\alpha^n - 1 = \alpha^{n/2}(\alpha^{n/2} - \alpha^{-n/2})$, et pour n impair, utiliser

$$\frac{\alpha^n - 1}{\alpha - 1} = \alpha^{(n-1)/2} \sum_{j=-(n-1)/2}^{(n-1)/2} \alpha^j.$$

Quelques équations diophantiennes

Exercice 31 (Racines rationnelles)

Soit $P = \sum_{k=0}^{n} a_k X^k \in \mathbf{Z}[X]$ avec $a_0, a_n \neq 0$. Montrer que pour toute racine $\alpha = p/q \in \mathbf{Q}$ de P, avec $\mathrm{pgcd}(p, q) = 1$, on a $p|a_0$ et $q|a_n$. En déduire une méthode pour trouver toutes les racines rationnelles de P.

Exercice 32

1. Montrer que l'équation $3x^2 + 2 = y^2$ n'a pas de solution dans $\mathbf{Z}^2$, puis dans $\mathbf{Q}^2$.
2. Montrer que l'équation $7x^3 + 2 = y^3$ n'a pas de solution dans $\mathbf{Z}^2$, puis dans $\mathbf{Q}^2$.

Exercice 33

Soit p un nombre premier.

1. On suppose $p \equiv 3 \pmod 4$. En utilisant le fait que -1 n'est pas un carré modulo p, montrer que l'équation $x^2 + y^2 = p$ n'admet pas de solution dans $\mathbf{Q}^2$.
2. Montrer que l'équation $x^2 + y^2 = 1$ admet une infinité de solutions dans $\mathbf{Q}^2$ (on pourra paramétrer le cercle par des fractions rationnelles).
3. En déduire que si $p = 2$ ou $p \equiv 1 \pmod 4$, l'équation $x^2 + y^2 = p$ admet une infinité de solutions dans $\mathbf{Q}^2$.
4. Montrer que l'équation $x^2 + y^2 + z^2 = 7$ n'a pas de solutions dans $\mathbf{Q}^3$.

Exercice 34

Le but de cet exercice est de montrer que l'équation $y^2 = x^3 + 7$ n'admet pas de solution dans $\mathbf{Z}^2$. Par l'absurde, on suppose qu'il existe une solution (x, y).

1. Montrer que y est pair.
2. Montrer que $x \equiv 1 \pmod 4$ et $x \geq 1$.
3. En déduire qu'il existe p premier $\equiv 3 \pmod 4$ divisant $x + 2$.
4. Montrer que $x + 2$ divise $y^2 + 1$ et conclure.

Remarque : on peut montrer (mais c'est bien plus difficile) que cette équation n'a pas de solution dans $\mathbf{Q}^2$.

Le groupe $(\mathbf{Z}/n\mathbf{Z})^\times$

Exercice 35

1. Soit m un entier impair. Montrer que les groupes $(\mathbf{Z}/m\mathbf{Z})^\times$ et $(\mathbf{Z}/2m\mathbf{Z})^\times$ sont isomorphes.
2. Trouver deux entiers impairs distincts m et n tels que $(\mathbf{Z}/m\mathbf{Z})^\times$ et $(\mathbf{Z}/n\mathbf{Z})^\times$ soient isomorphes.

Exercice 36

1. Déterminer un générateur de $(\mathbf{Z}/17\mathbf{Z})^\times$.
2. En déduire les solutions de $x^4 \equiv 1 \pmod{17}$.
3. Combien y a-t-il de puissances quatrièmes dans $(\mathbf{Z}/17\mathbf{Z})^\times$?

Exercice 37

Soit p premier. Montrer que si l'ordre de a dans $(\mathbf{Z}/p\mathbf{Z})^\times$ est 3, alors l'ordre de $a+1$ est 6.

Exercice 38 (Nombres premiers congrus à 1 modulo n)

1. Soit $p \geq 3$ premier. Montrer que si p divise x^2+1 avec $x \in \mathbf{Z}$, alors x est d'ordre 4 dans $(\mathbf{Z}/p\mathbf{Z})^\times$.
2. En déduire l'existence d'une infinité de nombres premiers congrus à 1 modulo 4.
3. Montrer que si p premier divise $x^4 - x^2 + 1$ avec $x \in \mathbf{Z}$, alors $p \equiv 1 \pmod{12}$.
4. Soit $n \geq 2$ un entier et p un nombre premier ne divisant pas n. Montrer que la réduction du polynôme $X^n - 1$ modulo p n'a que des racines simples dans $\mathbf{Z}/p\mathbf{Z}$.
5. Supposons de plus $p \,|\, \Phi_n(a)$ avec $a \in \mathbf{Z}$, où Φ_n est le n-ième polynôme cyclotomique. Montrer que l'ordre de a dans $(\mathbf{Z}/p\mathbf{Z})^\times$ vaut n.
6. En déduire qu'il existe une infinité de nombres premiers congrus à 1 modulo n. Cette preuve est attribuée à Euler par Dickson (*History of the Theory of Numbers, Vol. I : Divisibility and Primality*, 1919).

Symbole de Legendre

Exercice 39

Pour $p = 3, 5, 7, 13$, calculer le symbole de Legendre $\left(\frac{a}{p}\right)$ pour tout $1 \leq a \leq p-1$.

Exercice 40

Calculer $\left(\frac{13}{37}\right)$, $\left(\frac{45}{109}\right)$, $\left(\frac{11}{199}\right)$. La méthode utilisée permet-elle de calculer $\left(\frac{a}{p}\right)$ lorsque p est "très grand" ?

Exercice 41

1. Déterminer pour quels nombres premiers p, l'entier 3 est un carré modulo p.
2. Même question en remplaçant 3 par 5.

Exercice 42

1. Déterminer les solutions de l'équation $x^2 + 14x + 5 = 0$ dans $\mathbf{Z}/35\mathbf{Z}$.
2. Déterminer pour quels nombres premiers p, l'équation $x^2 + 14x + 5 = 0$ admet une solution dans $\mathbf{Z}/p\mathbf{Z}$.

Exercice 43

Soit $p \geq 3$ premier. Soit q une puissance de p, et $\alpha \in \mathbf{F}_q^\times$. On pose $\theta = \alpha + \alpha^{-1}$.

1. Montrer que $\theta^2 = 2 \Leftrightarrow \alpha$ est racine de Φ_8, où Φ_8 est le huitième polynôme cyclotomique.
2. On choisit pour $\mathbf{F}_q$ un corps de décomposition de Φ_8 sur $\mathbf{F}_p$, et pour α une racine de Φ_8. Montrer que $2^{(p-1)/2} = \theta^p/\theta$, et que $\alpha^p \in \{\alpha, -\alpha, \alpha^{-1}, -\alpha^{-1}\}$.
3. En déduire $\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{si } p \equiv \pm 1 \bmod 8, \\ -1 & \text{si } p \equiv \pm 3 \bmod 8. \end{cases}$

Arithmétique dans les anneaux

Exercice 44

Un sous-anneau d'un anneau intègre est-il intègre ? Même question avec noethérien, factoriel, principal, euclidien et toutes vos propriétés préférées pour les anneaux. Même question pour le quotient d'un anneau.

Exercice 45

Déterminer le pgcd et une relation de Bézout pour les éléments $3 + i$ et $1 + 3i$ dans $\mathbf{Z}[i]$.

Exercice 46

1. En utilisant la fonction $|\cdot|^2$, montrer que $\mathbf{Z}[i]^\times = \{\pm 1, \pm i\}$ et $\mathbf{Z}[j]^\times = \{\pm 1, \pm j, \pm j^2\}$.
2. Montrer que 2 est associé à un carré dans $\mathbf{Z}[i]$.
3. Soit $j = e^{2i\pi/3}$. Montrer que 3 est associé à un carré dans $\mathbf{Z}[j]$.

Exercice 47

Soit $j = e^{2i\pi/3}$. Soient $x, y, z \in \mathbf{Z}[j]$ tels que $x^3 + y^3 = z^3$. Montrer que $1 - j$ divise xyz.

Exercice 48 (Quotients de $\mathbf{Z}[i]$)

1. Montrer l'isomorphisme d'anneaux $\mathbf{Z}[X]/(X^2 + 1) \cong \mathbf{Z}[i]$.
2. Soit A un anneau commutatif et I, J des idéaux de A. On note $\pi : A \to A/I$ la projection canonique. Montrer l'isomorphisme d'anneaux $(A/I)/\pi(J) \cong A/(I + J)$.
3. En utilisant la question précédente, montrer que l'anneau quotient $\mathbf{Z}[i]/(1 + i)$ est isomorphe à $\mathbf{Z}/2\mathbf{Z}$.
4. Montrer que si p est un nombre premier, on a $\mathbf{Z}[i]/(p) \cong \mathbf{F}_p[X]/(X^2 + 1)$.
5. Montrer que $\mathbf{Z}[i]/(3)$ est isomorphe à $\mathbf{F}_9$.
6. Montrer que $\mathbf{Z}[i]/(p)$ est isomorphe à $\mathbf{F}_p \times \mathbf{F}_p$ si $p \equiv 1 \bmod 4$, et à $\mathbf{F}_{p^2}$ si $p \equiv 3 \bmod 4$.

Exercice 49 (Irréductibles de $\mathbf{Z}[i]$)

Le but de cet exercice est de décrire les éléments irréductibles de l'anneau $A = \mathbf{Z}[i]$. Pour tout a dans A, on note $N(a) = |a|^2$.

1. Soit p un nombre premier impair. Montrer que le corps $\mathbf{Z}/p\mathbf{Z}$ contient $\frac{p+1}{2}$ éléments qui sont des carrés.
2. Montrer que $x \in (\mathbf{Z}/p\mathbf{Z})^\times$ est un carré si et seulement si $x^{\frac{p-1}{2}} = 1$.
3. À quelle condition la classe de -1 mod p est-elle un carré dans $\mathbf{Z}/p\mathbf{Z}$?

Soit p un nombre premier. On rappelle (cf. exercice 48 sur les quotients de $\mathbf{Z}[i]$) que l'anneau A/pA est isomorphe à $\mathbf{F}_p[X]/(X^2+1)$.

4. Quels sont les nombres premiers de $\mathbf{Z}$ qui restent premiers dans A ?
5. Soit p un nombre premier de $\mathbf{Z}$ qui ne reste pas premier dans A. Montrer que p s'écrit comme produit de deux irréductibles u et v de A qui sont conjugués complexes l'un de l'autre et tels que $N(u) = N(v) = p$.
6. Déterminer l'ensemble des nombres premiers de $\mathbf{Z}$ qui s'écrivent comme somme de deux carrés.
7. Montrer que tout élément irréductible de A divise un élément irréductible de $\mathbf{Z}$. En déduire les éléments irréductibles de A.

Exercice 50

Montrer que $\mathbf{Z}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbf{Z}\}$ est un anneau euclidien pour la norme $N(a + b\sqrt{2}) = |a^2 - 2b^2|$.

Arithmétique dans les anneaux de polynômes

Exercice 51

1. Soit K un corps et $P \in K[X]$ de degré 2 ou 3. Montrer que P est irréductible si et seulement si P n'a pas de racine dans K.
2. Quels sont les polynômes irréductibles de degré 2 de $\mathbf{Z}/2\mathbf{Z}[X]$?
3. En déduire un critère pour déterminer si un polynôme de degré ≤ 5 de $\mathbf{Z}/2\mathbf{Z}[X]$ est irréductible.
4. *Application.* montrer que $P = X^5 + X^3 + 1$ est irréductible dans $\mathbf{Q}[X]$.

Exercice 52

Dans cet exercice, on montre que le polynôme $P = X^4 + 1$ est irréductible dans $\mathbf{Z}[X]$, mais est réductible modulo tout nombre premier.

1. Donner la décomposition de P en irréductibles dans $\mathbf{C}[X]$, puis dans $\mathbf{R}[X]$.
2. Montrer que P est irréductible dans $\mathbf{Q}[X]$ et dans $\mathbf{Z}[X]$.
3. Soit $p \geq 3$ un nombre premier. Montrer que le groupe $\mathbf{F}_{p^2}^\times$ possède un élément d'ordre 8.
4. En déduire que $X^4 + 1$ admet une racine dans $\mathbf{F}_{p^2}$, et conclure.

Exercice 53

Soit A un anneau commutatif. Montrer que $A[X]$ est principal si et seulement si A est un corps. Expliciter un idéal non principal de $\mathbf{Z}[X]$, de $K[X, Y]$.

Exercice 54

Montrer que $\mathbf{C}[X^2, X^3]$ n'est pas factoriel.

Exercice 55

Montrer que si K est un corps, l'anneau $K[[X]]$ est euclidien.

Exercice 56

On note $\mathbf{R}^{\mathbf{R}}$ la $\mathbf{R}$-algèbre des fonctions de $\mathbf{R}$ dans $\mathbf{R}$, et $\varphi : \mathbf{R}[X,Y] \to \mathbf{R}^{\mathbf{R}}$ le morphisme de $\mathbf{R}$-algèbres défini par $\varphi(X) = \cos$ et $\varphi(Y) = \sin$. Par définition, l'anneau A des polynômes trigonométriques est l'image de φ. Le but de cet exercice est de montrer que A n'est pas factoriel.

1. Montrer que $\ker\varphi = (X^2 + Y^2 - 1)$.
2. Montrer qu'il existe un morphisme d'anneaux $\psi : A \to \mathbf{R}(t)$ vérifiant $\psi(\cos) = \frac{t^2-1}{t^2+1}$ et $\psi(\sin) = \frac{2t}{t^2+1}$.
3. Montrer que tout $F \in \psi(A)$ est de la forme $F = \frac{P(t)}{(t^2+1)^n}$ avec $n \geq 0$, $P \in \mathbf{R}[t]$ de degré $\leq 2n$, et P non divisible par t^2+1.
4. Montrer que cos est irréductible dans A.
5. En utilisant $\cos^2 + \sin^2 = 1$, montrer que A n'est pas factoriel.