Université Bordeaux I - 2011
N1MA5011
Liste complémentaire 2

Anneaux principaux.

On cherche les solutions dans $\mathbb{N}$ de l'équation :

$$X^2 + Y^2 = Z^2 \tag{1}$$

Soit $(x, y, z) \in \mathbb{Z}^3$ une solution de (1) et soit $d = \text{pgcd}(x, y, z)$.

1. Soient $a = x/d$, $b = y/d$, $c = z/d$. Montrez que $(a, b, c) \in \mathbb{Z}^3$ est une solution de (1) et que a, b, c sont premiers entre eux.
2. Montrez que c est impair et que soit a soit b est pair. Par exemple $a \equiv 0[2]$ et $b \equiv 1[2]$.
3. On décompose $a^2 + b^2$ dans $\mathbb{Z}[i]$, $a^2 + b^2 = (a + ib)(a - ib)$. Montrez que $\text{pgcd}(a + ib, a - ib)$ divise 2. En déduire que $\text{pgcd}(a + ib, a - ib) = 1$.
4. Montrez qu'il existe $m, n \in \mathbb{Z}$ tels que $a + ib = (m + in)^2$.
5. Montrez que $\text{pgcd}(m, n) = 1$ et que $a = m^2 - n^2$, $b = 2mn$, $c = m^2 + n^2$.
6. Conclure.

Polynômes irréductibles.

1. Le polynôme $Y^7 + Y^6 + 7Y^4 + XY^3 + 3X^2Y^2 - 5Y + X^2 + X + 1$ est-il un irréductible de $\mathbb{R}[X, Y]$? de $\mathbb{Z}[X, Y]$?
2. Montrer que l'anneau $\mathbb{R}[X, Y]/(X^2 + Y^2 + 1)$ est intègre.
3. Le polynôme $Y^5 + X^2Y^3 + 1 + 2XY + 2X + X^2 + X^3$ est-il un irréductible de $\mathbb{Z}[X, Y]$?
4. Le polynôme $W^2 - W - T^3$ est-il un irréductible de $\mathbb{F}_2[W, T]$? de $\mathbb{F}_3[W, T]$?
5. Le polynôme $X^8 + Y^7 + 1$ est-il un irréductible de $\mathbb{Q}[X, Y]$? de $\mathbb{Z}[X, Y]$?
6. Le polynôme $14X^{10} - 21$ est-il un irréductible de $\mathbb{Z}[X]$? de $\mathbb{Q}[X]$?
7. L'anneau $\mathbb{Z}[X]/(X^4 - 5X^3 + 12X^2 - 2X - 1)$ est-il intègre ? est-ce un corps ?
8. L'idéal $(2, X^2 + X + 1)$ est-il premier de $\mathbb{Z}[X]$? maximal de $\mathbb{Z}[X]$?
9. L'idéal $(4, X^2 + X + 1)$ est-il premier de $\mathbb{Z}[X]$? premier de $\mathbb{Q}[X]$?

Polynômes cyclotomiques.

Exercice 1. Calculer Φ_{22} et Φ_{33}.

Exercice 2. Soit $n \in \mathbb{N} - \{0\}$, $n := mp^r$ avec $(m, p) = 1$ et x un entier tel que p divise $\Phi_n(x)$. On veut montrer que p est le plus grand facteur premier de n.

1. Montrer que pour tout $j \geq 0$ on a $\Phi_m(X^{p^{j-1}})\Phi_{mp^j}(X) = \Phi_m(X^{p^j})$.
2. Montrer que $\Phi_{mp^j}(X) \equiv \Phi_m^{p^j - p^{j-1}}(X) \bmod p$.
3. Montrer que $X^n - 1 \equiv (X^m - 1)^{p^r} \bmod p$.
4. Montrer par récurrence forte sur n que $\Phi_n(X) \equiv \Phi_m^{p^r - p^{r-1}}(X) \bmod p$. (Attention, question difficile).
5. Montrer l'image de x dans $\mathbb{F}_p^\times$ est d'ordre m. En déduire que m divise $p - 1$.

Eléments algébriques.

1. Soit p un nombre premier et $A := \mathbb{F}_p[X]/(X^n)$. Calculer $|A|$, montrer que l'anneau A est un $\mathbb{F}_p$-espace vectoriel et en donner une base. L'anneau A est-il un corps ? Déterminer $|A^\times|$.
2. Quel est le corps de décomposition sur $\mathbb{Q}$ de $\Phi_n(X)$?
3. Montrer que $\overline{\mathbb{Q}} := \{z \in \mathbb{C} \text{ tel que } z \text{ est algébrique sur } \mathbb{Q}\}$ est algébriquement clos.
4. Soit $\alpha := \sqrt{3 + \sqrt{4}}$. Déterminer le polynôme minimal $P(X)$ de α sur $\mathbb{Q}$. Quel est le degré de α sur $\mathbb{Q}$? Déterminer β tel qu'un corps de décomposition $\mathbb{L}$ de $P(X)$ sur $\mathbb{Q}$ soit de la forme $\mathbb{Q}(\beta)$. Calculer $[\mathbb{L} : \mathbb{Q}]$.
5. Soient $P(Y) = Y^4 + X^2 \in \mathbb{R}(X)[Y]$ et α une racine de $P(Y)$. Montrer que $\mathbb{R}(X)(\alpha)$ est un corps de décomposition de $P(Y)$ sur $\mathbb{R}(X)$. Calculer $[\mathbb{R}(X)(\alpha) : \mathbb{R}(X)]$.

Corps finis. Soit p un nombre premier, $n \in \mathbb{N} - \{0\}$ et $q := p^n$.

1. Quels sont les polynômes irréductibles de degré ≤ 2 sur $\mathbb{F}_3$?
2. Existe-t-il des polynômes irréductibles de degré arbitraire sur $\mathbb{F}_p$?
3. Combien y a-t-il de polynômes irréductibles de degré 2 sur $\mathbb{F}_q$?
4. A quelle condition sur n le groupe $\mathrm{Aut}(\mathbb{F}_q)$ est-il trivial ?
5. Décrire le corps à 9 éléments.
6. Donner un générateur du groupe $\mathbb{F}_9^\times$.