Université de Bordeaux
UF Mathématiques et Interactions

Licence de Mathématiques

DS UE Structures algébriques 2

21 octobre 2019, 9h30–11h00. Documents interdits.

Exercice 1 (**Irréductibilité de polynômes**)

1. Montrer que $Y^2 + X^3 - 1 \in \mathbb{Q}[X, Y]$ est irréductible.
2. Le polynôme $5X^{10} + 10X^5 + 30 \in \mathbb{Z}[X]$ est-il irréductible dans $\mathbb{Z}[X]$? Et dans $\mathbb{Q}[X]$? (Prouvez votre réponse).
3. Soit $\mathbb{F}_3$ le corps $\mathbb{Z}/3\mathbb{Z}$. Déterminer si les polynômes suivants

$$X^3 - X + 1, \quad X^4 - X^2 + 1 \in \mathbb{F}_3[X]$$

sont irréductibles.

Solution

(1) Dans l'anneau principal $\mathbb{Q}[X]$, $X - 1$ est un facteur premier de $X^3 - 1 = (X - 1)(X^2 + X + 1)$ et $(X - 1)^2$ ne divise pas $X^3 - 1$. On peut appliquer le critère d'Eisentein dans $A[Y]$ avec $f = X - 1 \in A$ premier, et conclure que $Y^2 + (X^3 - 1)$ est irréductible dans $A[Y] = \mathbb{Q}[X, Y]$.

(2) On a que $5X^{10} + 10X^5 + 30 = 5P(X)$, où $P(X) = X^{10} + 2X^5 + 6$, est le produit de deux éléments non-inversibles de $\mathbb{Z}[X]$, il n'est donc pas irréductible dans $\mathbb{Z}[X]$.

Le critère d'Eisenstein appliqué à $X^{10} + 2X^5 + 6 \in \mathbb{Z}[X]$ avec $f = 2$ montre que $P(X)$ est irréductible dans $\mathbb{Z}[X]$, donc irréductible dans $\mathbb{Q}[X]$ d'après le cours. Par conséquent, $5X^{10} + 10X^5 + 30$, qui est associé à $P(X)$ dans $\mathbb{Q}[X]$ (mais pas dans $\mathbb{Z}[X]$), est irréductible dans $\mathbb{Q}[X]$.

(3) Le polynôme $X^3 - X + 1$ de degré 3 ne s'annule en aucun élément de $\mathbb{F}_3 = \{0, 1, -1\}$, il est donc irréductible dans $\mathbb{F}_3[X]$.

Le second polynôme $X^4 - X^2 + 1 = X^4 + 2X^2 + 1 = (X^2 + 1)^2$ n'est pas irréductible. Noter qu'il n'a pas de racine dans $\mathbb{F}_3$, mais que cela n'implique pas l'irréductibilité pour les polynômes de degré > 3.

Exercice 2 Soit $(a, b) \in \mathbb{Q}^2$. On note $\mathfrak{m}_{(a,b)} = (X - a, Y - b) \subset \mathbb{Q}[X, Y]$ l'idéal engendré par $X - a$ et $Y - b$ (également noté $\langle X - a, Y - b \rangle$ en TD).

1. Soit $a' \neq a$. Montrer que $X - a' \notin \mathfrak{m}_{(a,b)}$.
2. Montrer que si $(a, b) \neq (a', b')$, alors $\mathfrak{m}_{(a,b)} \neq \mathfrak{m}_{(a',b')}$.

Solution

(1) Supposons que $X - a' \in \mathfrak{m}_{(a,b)}$. Alors

$$X - a' = (X - a)F_1(X, Y) + (Y - b)F_2(X, Y)$$

pour certains $F_1, F_2 \in \mathbb{Q}[X, Y]$. En évaluant en $X = a$, on trouve $\mathbb{Q}^* \ni a - a' = (Y - b)F_2(a, Y)$ dans $\mathbb{Q}[Y]$. Ce qui est absurde puisque le membre de droite est nul ou de degré ≥ 1 en Y.

(2) Si $(a, b) \neq (a', b')$, on a $a \neq a'$ ou $b \neq b'$. Dans le premier cas l'assertion à montrer résulte de (1). Le second cas est similaire (symétrique).

Exercice 3 Soit A un anneau principal. Soit $f \in A$ non nul et non inversible. Montrer que le radical de fA (c'est-à-dire l'ensemble des éléments $a \in A$ tels que $a^n \in fA$ pour un entier $n \geq 1$ dépendant de a) est donné par $\sqrt{fA} = (p_1 \cdots p_n)A$ où les p_i sont les facteurs irréductibles (2 à 2 non associés) de f.

Solution

Écrivons $f = up_1^{r_1} \cdots p_n^{r_n}$ avec $u \in A$ inversible et $r_i \geq 1$. Posons $q = p_1 \cdots p_n$. Soit r le maximum des r_i. Alors $q^r = u^{-1}(\prod_i p_i^{r-r_i})f \in fA$. Donc $q \in \sqrt{fA}$ et $qA \subseteq \sqrt{fA}$.

Inversement, soit $a \in \sqrt{fA}$ un élément non nul. On a $a^r \in fA$ pour un certain entier $r \geq 1$. Donc f divise a^r. Chaque p_i divise f, donc divise a^r. Cela veut dire que p_i est un facteur premier de a^r. C'est donc un facteur premier de a. Si on veut une preuve rigoureuse, on peut dire que $a^r \in p_iA$ implique que $a \in p_iA$ car p_iA est un idéal premier. Il suit que dans la décomposition de a, chaque p_i apparaît. Comme les p_i sont deux à deux non-associés, leur produit q apparaît dans la décomppose de a, donc il divise a. Autrement dit $a \in qA$ et $\sqrt{fA} \subseteq qA$. D'où l'égalité.

Exercice 4 Soit $P(X) \in \mathbb{Q}[X]$ un polynôme irréductible. Soit $\mathfrak{m} = (P(X), Y) \subseteq \mathbb{Q}[X, Y]$ l'idéal engendré par $P(X)$ et Y (également noté $\langle P(X), Y \rangle$ en TD). On va montrer que $\mathfrak{m}$ est un idéal maximal.

1. Montrer que $K := \mathbb{Q}[X]/(P(X)\mathbb{Q}[X])$ est un corps. On note $\phi : \mathbb{Q}[X] \to K$ la surjection canonique.
2. Montrer qu'il existe un unique homomorphisme d'anneaux $\tilde{\phi} : \mathbb{Q}[X, Y] \to K$ tel que $\tilde{\phi}(H(X)) = \phi(H(X))$ pour tout $H(X) \in \mathbb{Q}[X]$ et $\tilde{\phi}(Y) = 0$.
3. Montrer que $\tilde{\phi}$ est surjectif.
4. Montrer que $\mathfrak{m} \subseteq \ker(\tilde{\phi})$.
5. Soit $F(X, Y) \in \mathbb{Q}[X, Y]$. Montrer qu'il existe $H(X) \in \mathbb{Q}[X]$ et $G(X, Y) \in \mathbb{Q}[X, Y]$ tels que
$$F(X, Y) = H(X) + G(X, Y)Y.$$
6. Montrer que $\ker(\tilde{\phi}) = \mathfrak{m}$ et que $\mathfrak{m}$ est un idéal maximal.
7. Soit $\alpha \in \mathbb{C}$ une racine complexe de $P(X)$. Justifier qu'il existe un unique homomorphisme d'anneaux $s : \mathbb{Q}[X] \to \mathbb{C}$ tel que $s(a) = a$ pour tout $a \in \mathbb{Q}$ et $s(X) = \alpha$.

8. Déterminer le noyau de s. En déduire que K s'identifie à un sous-corps de $\mathbb{C}$.

Solution

(1) Comme $P(X)$ est irréductible, il engendre un idéal maximal dans $\mathbb{Q}[X]$ (cours de L2). Donc K est un corps.

(2) On a $\mathbb{Q}[X,Y] = \mathbb{Q}[X][Y]$. On applique la propriété universelle des anneaux de polynômes (cours) : il existe un unique homomorphisme d'anneaux $\tilde{\phi} : \mathbb{Q}[X][Y] \to K$ qui étend ϕ et qui vaut 0 en Y.

(3) En effet, ϕ est déjà surjectif.

(4) On a $\tilde{\phi}(P(X)) = \phi(P(X)) = 0$ et $\tilde{\phi}(Y) = 0$ par construction. Donc $P(X), Y \in \ker \tilde{\phi}$, donc l'idéal $\mathfrak{m}$ qu'ils engendrent est contenu dans $\ker \tilde{\phi}$.

(5) On peut considérer $F(X,Y)$ comme un polynôme dans $\mathbb{Q}[X][Y]$ et écrire

$$F(X,Y) = H_0(X) + H_1(X)Y + H_2(X)Y^2 + \cdots + H_d(X)Y^d,$$

avec $H_i(X) \in \mathbb{Q}[X]$. Il suffit alors de prendre $H(X) = H_0(X)$ et $G(X,Y) = H_1(X) + H_2(X)Y + \cdots H_d(X)Y^{d-1}$.

(6) Soit $F(X,Y) \in \ker \tilde{\phi}$. Sous l'écriture de (5) on a alors $0 = \tilde{\phi}(H(X) + G(X,Y)Y) = \phi(H(X))$. Donc $H(X) \in \ker \phi = P(X)\mathbb{Q}[X]$ et $F(X,Y) \in \mathfrak{m}$.

(7) C'est encore la propriété universelle donnée en cours.

(8) Soit $H(X) \in \mathbb{Q}[X]$. Par division euclidienne par $P(X)$, on a $H(X) = P(X)Q(X) + R(X)$ avec $\deg R(X) < \deg P(X)$. On a $H(X) \in \ker s$ si et seulement si $R(\alpha) = 0$. Cela implique que $R(X) = 0$. En effet, si $R(X) \neq 0$, il est alors premier avec $P(X)$ puisque ce dernier est irréductible. Par Bézout (puisque $\mathbb{Q}[X]$ est principal), on a une identité $U(X)P(X) + V(X)R(X) = 1$ pour certains $U(X), V(X) \in \mathbb{Q}[X]$. En évaluant en α on trouve $0 = 1$. Absurde. Par conséquent $\ker s = P(X)\mathbb{Q}[X]$.

Par le théorème de factorisation, s induit un homomorphisme d'anneaux injectif $\tilde{s} : K = \mathbb{Q}[X]/P(X)\mathbb{Q}[X] \to \mathbb{C}$.