Université de Bordeaux
UF Mathématiques et Interactions

Licence de Mathématiques

DS UE Structures algébriques 2

26 octobre 2018, 11h00–12h30. Documents interdits.

Exercice 1 (**Irréductibilité de polynômes**)

1. Soit $\mathbb{F}_3$ le corps $\mathbb{Z}/3\mathbb{Z}$. Montrer que $X^3 - X + 1 \in \mathbb{F}_3[X]$ est irréductible.
2. Montrer que $5X^3 + 27X^2 + 4X + 2$ est irréductible dans $\mathbb{Z}[X]$ et dans $\mathbb{Q}[X]$.
3. Montrer que $X^{10} + X^5Y^2 + Y \in \mathbb{Q}[X, Y]$ est irréductible.

Solution

1. On vérifie directement que ce polynôme de degré 3 n'a pas de racine dans $\mathbb{F}_3$. Il est donc irréductible.

2. Modulo 3, ce polynôme est égal à $-(X^3 - X + 1) \in \mathbb{F}_3[X]$. Ce dernier étant irréductible, $5X^3+27X^2+4X+2$ est irréductible dans $\mathbb{Z}[X]$ par le critère d'irréductibilité par réduction. Comme $\mathbb{Z}$ est factoriel, il est aussi irréductible dans $\mathbb{Q}[X]$.

3. On applique le critère d'Eisenstein avec $A = \mathbb{Q}[Y]$ et $f = Y$.

Exercice 2 Montrer que l'anneau quotient $\mathbb{Z}[X]/(2X^3 + 5X + 15)\mathbb{Z}[X]$ est intègre. Montrer que cet anneau n'est pas un corps (on peut par exemple montrer que la classe $\overline{X}$ de X dans le quotient n'est pas un élément inversible).

Solution

Par Eisenstein avec $A = \mathbb{Z}$ et $f = 5$, on trouve que $2X^3 + 5X + 15$ est irréductible dans $\mathbb{Z}[X]$. Ce dernier étant un anneau factoriel, $2X^3+5X+15$ est premier, donc l'anneau quotient $\mathbb{Z}[X]/(2X^3 + 5X + 15)\mathbb{Z}[X]$ est intègre.

Si la classe $\overline{X}$ de X était inversible, il existerait $P(X) \in \mathbb{Z}[X]$ tel que

$$XP(X) - 1 \in (2X^3 + 5X + 15)\mathbb{Z}[X].$$

On aurait donc une identité

$$1 = XP(X) + (2X^3 + 5X + 15)Q(X)$$

pour un certain $Q(X) \in \mathbb{Z}[X]$. En évaluant cette identité en $X = 0$ on trouve $1 = 15Q(0)$ dans $\mathbb{Z}$, ce qui est impossible. Il suit que $\overline{X}$ n'est pas inversible. Par ailleurs $\overline{X} \neq 0$ car X n'est clairement pas divisible par $2X^3 + 5X + 15$. Donc l'anneau quotient en question n'est pas un corps.

Exercice 3 Soit A un anneau intègre (commutatif unitaire). On sait que si A est factoriel, alors $A[X]$ aussi. Nous allons maintenant montrer la réciproque. Supposons donc $A[X]$ factoriel.

1. Montrer qu'un produit fini $F_1(X)\cdots F_n(X)$ d'éléments non nuls de $A[X]$ appartient à A si et seulement si les $F_i(X)$ appartiennent tous à A.
2. Montrer que $(A[X])^* = A^*$.
3. Soit $a \in A$ non nul. Montrer que a est irréductible en tant qu'élément de A si et seulement s'il est irréductible en tant qu'élément de $A[X]$.
4. Montrer que A est factoriel.

Solution

1. Cela résulte du fait que $\deg(F_1\cdots F_n) = \deg F_1 + \cdots + \deg F_n$ et que $F_i(X) \in A$ équivaut à $\deg F_i(X) = 0$.

2. Si $F(X) \in (A[X])^*$, il existe $G(X) \in A[X]$ tel que $F(X)G(X) = 1$. Par (1), on trouve que $F(X), G(X) \in A$. Donc $F(X) \in A^*$. La réciproque est immédiate.

3. Si a est irréductible dans A et s'il s'écrit comme $a = F(X)G(X)$ dans $A[X]$, alors par (1) $F(X), G(X) \in A$, donc par exemple $F(X) \in A^*$ puisque a est irréductible dans A. Donc $F(X) \in (A[X])^* = A^*$. Supposons maintenant a irréductible dans $A[X]$ et que $a = bc$ avec $b, c \in A$. Alors cette égalité vaut dans $A[X]$ et implique que b ou c appartient à $(A[X])^* = A^*$. Donc a est irréductible dans A.

4. Tout élément non nul $a \in A$ se décompose de façon unique comme produit d'éléments irréductibles $F_1(X), \cdots, F_n(X)$ de $A[X]$. Ceux-ci sont aussi des éléments irréductibles de A par (1) et (3). Donc A est factoriel.

Exercice 4 (Étude d'un anneau principal) On fixe un nombre premier p. Considérons le sous-ensemble A des nombres rationnels $r \in \mathbb{Q}$ qui admettent un dénominateur premier à p (c'est-à-dire qu'il existe $k \in \mathbb{Z}$ non nul et premier à p tel que $kr \in \mathbb{Z}$).

1. Montrer que A est un sous-anneau de $\mathbb{Q}$.
2. Montrer que les éléments de A^* (éléments inversibles de A) sont les fractions de la forme a/b avec $a, b \in \mathbb{Z}$ non nuls et premiers à p.
3. Nous montrons que A est principal.
   (a) Montrer que tout élément non nul $r \in A$ s'écrit de façon unique sous la forme $r = p^n w$ avec $n \geq 0$ et $w \in A^*$. On note $v_p(r)$ l'exposant n.
   (b) Soit I un idéal non nul de A. Soit $v_p(I)$ le minimum des $v_p(r)$ avec $r \in I \setminus \{0\}$. Montrer que $p^{v_p(I)} \in I$ et que $I = p^{v_p(I)}A$.
4. Idéaux de A.
   (a) Montrer que $p^m A = p^n A$ $(m, n \geq 0)$ si et seulement si $m = n$.
   (b) Décrire explicitement l'ensemble des idéaux de A.
   (c) Quels sont les idéaux premiers et les idéaux maximaux de A ?

5. Étude de A/pA.

   (a) Soit $r = a/b \in A$ avec $b \geq 1$ et premier à p. Montrer qu'il existe $u, v \in \mathbb{Z}$ tels que $ub + vp = 1$. En déduire que r peut s'écrire comme $r = k + pr'$ avec $k \in \mathbb{Z}$ et $r' \in A$.

   (b) Montrer que l'inclusion canonique $\mathbb{Z} \to A$ induit un homomorphisme d'anneaux surjectif $\phi : \mathbb{Z}/p\mathbb{Z} \to A/pA$.

   (c) En utilisant le fait que $Z/p\mathbb{Z}$ est un corps, montrer que ϕ est un isomorphisme.

Solution

1. Les nombres rationnels $0, 1 \in A$. Si $r_1 = a_1/b_1, r_2 = a_2/b_2 \in A$ avec b_i premiers à p, alors $r_1 - r_2 = (a_1b_2 - a_2b_1)/(b_1b_2)$ et $r_1r_2 = (a_1a_2)/(b_1b_2)$ avec b_1b_2 premier à p. Donc $r_1 - r_2, r_1r_2 \in A$. Cela implique que A est un sous-anneau de $\mathbb{Q}$.

2. Si $r = a/b \in A$ avec b premier à p est inversible dans A, alors il existe $c/d \in A$ avec d premier à p tel que $(a/b)(c/d) = 1$. Donc $ac = bd$ est premier à p. Il suit que a est aussi premier à p. Inversement si a, b sont premiers à p, alors $b/a \in A$ et c'est l'inverse de $a/b \in A$.

3.(a) Soit $r = a/b$ avec b premier à p. On a $a = p^n c$ avec c premier à p. Il suit que $r = p^n.(c/b)$ avec $c/b \in A^*$. Si $r = p^m w$ avec $m \in \mathbb{N}$ et $w \in A^*$, alors $p^{m-n} \in A^*$. Par (2), cela implique que $m = n$ et donc $w = c/b$. D'où l'unicité.

3.(b) Soit $t_0 \in I$ non nul tel que $v_p(t_0) = v_p(I)$. On écrit $t_0 = p^{v_p(t_0)}w_0$ avec $w_0 \in A^*$. Alors $p^{v_p(I)} = p^{v_p(t_0)} = w_0^{-1}t_0 \in I$. Pour tout $r \in I$ non nul, il existe $w \in A^*$ tel que

$$r = p^{v_p(r)}w = (p^{v_p(r)-v_p(I)}w)p^{v_p(I)} \in p^{v_p(I)}A$$

car $v_p(r) \geq v_p(I)$. Donc $I = p^{v_p(I)}A$ et A est principal.

4.(a) Si $p^mA = p^nA$, alors $p^m = p^nr$ pour un $r \in A$. On a $r = p^{v_p(r)}w$ avec $w \in A^*$. Donc $p^m = p^{n+v_p(r)}w$. Par l'unicité prouvée dans (2), on obtient $m = n + v_p(r) \geq n$. Par symétrie on obtient $n \geq m$. Donc $m = n$. La réciproque est triviale.

4.(b) L'ensemble des idéaux de A est constitué de l'idéal nul et les p^nA avec $n \geq 0$.

De plus l'application qui à tout entier naturel $n \geq 0$ associe l'idéal p^nA de A est une strictement décroissante d'après 4(a).

4.(c). Les idéaux premiers sont $\{0\}$ et pA. Et pA est l'unique idéal maximal de A.