



## Anneaux de polynômes III

---

### Exercice 1

Soit  $(x^3 - x + 2)$  l'idéal principal engendré par  $x^3 - x + 2$  dans l'anneau  $\mathbb{Q}[x]$ .

1. Montrer que l'anneau quotient  $\mathbb{Q}[x]/(x^3 - x + 2)$  est un corps.
2. Soit  $y$  l'image de  $x$  dans  $\mathbb{Q}[x]/(x^3 - x + 2)$  par la surjection canonique. Calculer son inverse.
3. Montrer que  $1 + y + y^2$  est non nul et calculer son inverse.

[Correction ▼](#)

[002292]

### Exercice 2

Soit  $f \in A[x]$  un polynôme primitif de degré positif sur l'anneau factoriel  $A$ . Soit  $\pi \in A$  un élément irréductible. Supposons que le coefficient dominant de  $f$  ne soit pas divisible par  $\pi$  et que  $f \pmod{\pi}$  soit irréductible dans l'anneau quotient  $A/(\pi)$ . Montrer que  $f$  est irréductible dans  $A[x]$ .

[Correction ▼](#)

[002293]

### Exercice 3

Les polynômes suivants sont-ils irréductibles ?

1.  $X^5 + 121X^4 + 1221X^3 + 12221X^2 + 122221X + 222222$  dans  $\mathbb{Q}[X]$ .
2.  $f(X, Y) = X^2Y^3 + X^2Y^2 + Y^3 - 2XY^2 + Y^2 + X - 1$  dans  $\mathbb{C}[X, Y]$  et  $\mathbb{F}_2[X, Y]$ .
3.  $f(X, Y) = Y^7 + Y^6 + 7Y^4 + XY^3 + 3X^2Y^2 - 5Y + X^2 + X + 1$  dans  $\mathbb{Q}[X, Y]$ .

[Correction ▼](#)

[002294]

### Exercice 4

L'idéal principal  $(x^2 + y^2 + 1)$  est-il maximal dans les anneaux  $\mathbb{C}[x, y]$ ,  $\mathbb{R}[x, y]$ ,  $\mathbb{Q}[x, y]$ ,  $\mathbb{Z}[x]$ ,  $\mathbb{Z}_2[x, y]$  ?

[Correction ▼](#)

[002295]

### Exercice 5

1. Soit  $f \in \mathbb{Z}[x]$ . Considérons la réduction du polynôme  $f$  modulo  $m : f \pmod{m} \in \mathbb{Z}_m[x]$ . Montrer que

$$\mathbb{Z}[x]/(m, f) \cong \mathbb{Z}_m[x]/(f \pmod{m})$$

où  $(m, f)$  est l'idéal engendré par  $m$  et  $f$  dans  $\mathbb{Z}[x]$  et  $(f \pmod{m})$  est l'idéal engendré par  $f \pmod{m}$  dans  $\mathbb{Z}_m[x]$ . (*Indication* : Utiliser l'exercice 10 de fiche 4.)

2. Si  $p$  est un nombre premier et  $f$  est un polynôme tel que  $f \pmod{p}$  est irréductible sur le corps  $\mathbb{Z}_p$ , alors l'idéal  $(p, f)$  est maximal dans  $\mathbb{Z}[x]$ .

[002296]

### Exercice 6

Soit  $A$  un anneau factoriel.

1. Pour  $a, b \neq 0$  on a  $(a) \cdot (b) = (a) \cap (b)$  ssi  $\text{pgcd}(a, b) \sim 1$ .
2. Si  $(a, b)$  est principal, alors  $(a, b) = (\text{pgcd}(a, b))$ .

**Exercice 7**

1. Montrer que les idéaux  $(5, x^2 + 3)$ ,  $(x^2 + 1, x + 2)$ ,  $(x^3 - 1, x^4 - 1)$  ne sont pas principaux dans  $\mathbb{Z}[x]$ .
2. Les idéaux  $(x, x + 1)$ ,  $(5, x^2 + 4)$  et  $(x^2 + 1, x + 2)$  sont-ils premiers ou maximaux dans  $\mathbb{Z}[x]$  ?

Correction ▼

[002298]

**Exercice 8**

Démontrer que si  $J$  est un idéal premier de l'anneau  $\mathbb{Z}[x]$ , alors

$$J = (0), \quad (p), \quad (f) \quad \text{ou} \quad (p, g),$$

où  $p$  est premier,  $f \in \mathbb{Z}[x]$  est un polynôme irréductible de degré positif et  $g$  est un polynôme, tel que sa réduction modulo  $p$  est irréductible sur  $\mathbb{Z}_p$ . Le dernier cas,  $J = (p, g)$ , nous donne la forme générale d'un idéal maximal dans  $\mathbb{Z}[x]$ . *Le plan de la démonstration est le suivant.*

1. Soit  $B$  un sous-anneau de l'anneau  $A$ ,  $I$  un idéal premier de  $A$ . Montrer que  $B \cap I$  est soit un idéal premier de  $B$ , soit l'anneau  $B$  lui-même.
2. Soit  $J$  un idéal premier de  $\mathbb{Z}[x]$ . Montrer que  $\mathbb{Z} \cap J = (0)$  ou  $(p)$  où  $p$  est premier.
3. Supposons que  $\mathbb{Z} \cap J = (0)$ . Montrer que si  $J \neq (0)$ , alors  $J$  est engendré par un polynôme primitif de  $J$  de degré minimal.
4. Supposons que  $\mathbb{Z} \cap J = (p)$ . Soit  $r_p : \mathbb{Z}[x] \rightarrow \mathbb{Z}_p[x]$  la réduction modulo  $p$ . Montrer que l'idéal  $r_p(J)$  est premier et que  $J = (p, g)$ .
5. Montrer que  $J$  est maximal ssi  $J = (p, g)$  où  $p$  est premier et  $r_p(g)$  est irréductible dans  $\mathbb{Z}_p[x]$ .

Correction ▼

[002299]

### Correction de l'exercice 1 ▲

1. Soit  $P = x^3 - x + 2$ . Sa réduction  $\bar{P} = x^3 - x - 1$  modulo 3 est de degré 3 et n'a pas de racine, donc  $\bar{P}$  est irréductible dans  $\mathbb{Z}_3[x]$ . Comme  $P$  est primitif, on en déduit que  $P$  est irréductible dans  $\mathbb{Z}[x]$ , puis dans  $\mathbb{Q}[x]$ . Comme  $\mathbb{Q}[x]$  est principal, on en déduit que  $(P)$  est maximal, et donc que  $\mathbb{Q}[x]/(P)$  est un corps.
2. Dans  $\mathbb{Q}[x]/(P)$ , on a  $y^3 - y + 2 = 0$ , donc  $y(y^2 - 1) = -2$  et finalement  $y(\frac{1}{2}(1 - y^2)) = 1$ . Ainsi  $y^{-1} = \frac{1}{2}(1 - y^2)$ .
3.  $1 + y + y^2 = \pi(1 + x + x^2)$ . On a  $\text{pgcd}(P, 1 + x + x^2) = 1$ , et plus précisément, en utilisant l'algorithme d'Euclide :  $13 = (x + 4)P - (x^2 + 3x - 5)(x^2 + x + 1)$  donc  $(y^2 + y + 1)^{-1} = \frac{1}{13}(y^2 + 3y - 5)$ .

### Correction de l'exercice 2 ▲

Notons  $f = \sum_{i=0}^d a_i x^i$ . On a  $\text{pgcd}(a_0, \dots, a_d) \sim 1$  et  $\pi \nmid a_d$ . Notons  $\bar{f} \in A/(\pi)[X]$  la réduction de  $f$  modulo  $\pi$ . Soit  $f = gh$  une factorisation de  $f$  dans  $A[x]$ . Alors  $\bar{f} = \bar{g}\bar{h}$ , et donc (quitte à échanger  $g$  et  $h$ )  $\bar{g} \sim 1$  et  $\bar{h} \sim \bar{f}$ . Comme  $\pi \nmid a_d$ , on a  $\deg(\bar{f}) = d$ , et donc  $\deg(\bar{h}) = d$  puis  $\deg(h) \geq d$ , et finalement  $\deg(h) = d$ . Par conséquent  $\deg(g) = 0 : g \in A$ . Comme  $g|f$ , on a  $g|c(f) \sim 1$  donc  $g \sim 1$ . Ainsi, toute factorisation de  $f$  dans  $A[x]$  est triviale :  $f$  est irréductible.

### Correction de l'exercice 3 ▲

1. Ce polynôme est unitaire donc primitif. 11 est nombre premier qui divise tous les coefficients sauf le dominant.  $11^2 = 121$  ne divise pas le coefficient de degré 0, donc, d'après le critère d'Eisenstein, c'est un polynôme irréductible de  $\mathbb{Q}[X]$ .
2.  $f(X, Y) = (X^2 + 1)Y^3 + (X - 1)^2 Y^2 + (X - 1)$ . Regardons  $f$  comme un polynôme de  $A[Y]$  avec  $A = \mathbb{C}[X]$ . Alors,  $f$  est primitif sur  $A$ , et  $(X - 1)$  est un irréductible de  $A$  qui divise tous les coefficients de  $f$  sauf le dominant, et dont le carré ne divise pas le terme constant. D'après le critère d'Eisenstein, on en déduit que  $f$  est irréductible dans  $A[Y] = \mathbb{C}[X, Y]$ .  
Dans  $\mathbb{Z}_2[X, Y]$ , on a  $(X^2 + 1) = (X + 1)^2$  et  $f = (X + 1)((X + 1)(Y^3 + Y^2) + 1)$ , donc  $f$  n'est pas irréductible..
3.  $f(X, Y) = Y^7 + Y^6 + 7Y^4 + XY^3 + 3X^2 Y^2 - 5Y + X^2 + X + 1$ . Considérons  $f$  comme un polynôme de  $A[X]$  où  $A = \mathbb{Q}[Y]$ . Alors  $f$  est primitif sur  $A$ . Soit  $\pi = Y \in A$ .  $\pi$  est irréductible,  $\pi$  ne divise pas le coefficient dominant de  $f$ , et la réduction  $\bar{f}$  modulo  $\pi$  est  $\bar{f} = X^2 + X + 1 \in A/(\pi)[X] = \mathbb{Q}[X, Y]/(Y) \simeq \mathbb{Q}[X]$ .  $\bar{f}$  est donc irréductible dans  $A/(\pi)$ , donc d'après l'exercice précédent,  $f$  est irréductible dans  $\mathbb{Q}[X, Y]$ .

### Correction de l'exercice 4 ▲

Soit  $f = x^2 + y^2 + 1 \in A[x, y]$  ( $A = \mathbb{C}, \mathbb{R}, \mathbb{Q}, \mathbb{Z}, \mathbb{Z}_2$ ). Soit  $B = A[y]$ , et regardons  $f$  comme un polynôme de  $B[x]$ . Le coefficient dominant de  $f$  (qui est 1) est inversible dans  $B$ , donc on peut effectuer la division euclidienne de tout polynôme par  $f : \forall g \in B[y], \exists (q, r) \in B[x]^2, g = qf + r$  et  $\deg_x r \leq 1$ . Notons  $r = a(y)x + b(y), a, b \in A[y]$ . De plus, pour des raisons de degré, le quotient et le reste de cette division sont uniques. On peut donc identifier  $A[x, y]/(x^2 + y^2 + 1)$  à  $\{a(y)x + b(y), a(y), b(y) \in A[y]\}$ . Supposons que  $\bar{y}$  soit inversible dans cet quotient. Il existe  $a, b \in A[y]$  tels que  $y(a(y)x + b(y)) = \bar{1}$ . On a donc  $ya(y) = 0$  et  $yb(y) = 1$ , ce qui est impossible.

### Correction de l'exercice 6 ▲

Rappelons que  $(a) \cdot (b) = \{\sum_{i=1}^n a_i b_i, n \in \mathbb{N}, a_i \in (a), b_i \in (b)\} = (ab)$ . De plus  $(ab) \subset (a) \cap (b)$  donc

$$\begin{aligned}(ab) = (a) \cap (b) &\Leftrightarrow (a) \cap (b) \subset (ab) \\ &\Leftrightarrow \forall m \in A, (a|m \text{ et } b|m \Rightarrow ab|m) \\ &\Leftrightarrow \text{ppcm}(a, b) \sim ab \\ &\Leftrightarrow \text{ppcm}(a, b) \sim \text{pgcd}(a, b) \text{ppcm}(a, b) \\ &\Leftrightarrow \text{pgcd}(a, b) \sim 1\end{aligned}$$

Si  $A$  est principal, alors  $\exists d \in A$ ,  $(a, b) = (d)$ . Alors  $a \in (d)$  et  $b \in (d)$  donc  $d$  est un diviseur commun à  $a$  et  $b$ . Si de plus  $d'$  est un autre diviseur commun à  $a$  et  $b$ , alors  $a \in (d')$  et  $b \in (d')$  et comme  $(a, b)$  est le plus petit idéal contenant  $a$  et  $b$ , on en déduit que  $(a, b) = (d) \subset (d')$ , et donc que  $d' | d$  : finalement,  $\text{pgcd}(a, b) = d$ .

### Correction de l'exercice 7 ▲

1.  $I = (5, x^2 + 3)$ . On a  $\text{pgcd}(5, x^2 + 3) = 1$ , donc si  $I$  était principal, on aurait  $1 \in I$ , et donc  $I = \mathbb{Z}[X]$ . Si  $1 \in I$ , il existe  $P, Q \in \mathbb{Z}[x]$ , tels que  $1 = 5P + (x^2 + 3)Q$ . En considérant la réduction modulo 5 de ces polynômes, on obtient  $(x^2 + \bar{3})\bar{Q} = \bar{1}$ , ce qui est impossible pour des raisons de degré ( $\mathbb{Z}/5\mathbb{Z}$  est intègre). Donc  $1 \notin I$ , et  $I$  n'est donc pas intègre.

$x^2 + 1 = (x + 2)(x - 2) + 5$ , donc  $(x^2 + 1, x + 2) = (x + 2, 5)$ . Or  $(x + 2, 5)$  n'est pas principal pour les mêmes raisons que précédemment.

On a  $(x - 1) = (x^4 - 1) - x(x^3 - 1)$  donc  $(x - 1) \subset (x^4 - 1, x^3 - 1)$ . Par ailleurs,  $(x - 1) | (x^4 - 1)$  et  $(x - 1) | (x^3 - 1)$  donc  $x^4 - 1 \in (x - 1)$  et  $x^3 - 1 \in (x - 1)$ , donc  $(x^4 - 1, x^3 - 1) \subset (x - 1)$ . Donc  $(x^4 - 1, x^3 - 1)$  est principal.

2.  $I = (x, x + 1) = \mathbb{Z}$  car  $1 = (x + 1) - x$ . Donc  $I$  n'est pas propre.  
 $I = (5, x^2 + 4)$ .  $\mathbb{Z}[X]/I \sim \mathbb{Z}_5/(x^2 + \bar{4})$ . Mais  $(x^2 + \bar{4}) = (x - \bar{1})(x + \bar{1})$  est réductible dans  $\mathbb{Z}_5[x]$ , donc  $\mathbb{Z}_5/(x^2 + \bar{4})$  n'est pas intègre :  $I$  n'est pas premier.  
 $I = (x^2 + 1, x + 2) = (x + 2, 5)$ .  $\mathbb{Z}[x]/I \simeq \mathbb{Z}_5[x]/(x + \bar{2})$ .  $x + \bar{2}$  est irréductible dans  $\mathbb{Z}_5[x]$ , qui est principal, donc  $(x + \bar{2})$  est maximal, donc le quotient est un corps, et  $I$  est maximal.

### Correction de l'exercice 8 ▲

1. Soit  $a, b \in B$ ,  $ab \in I \cap B$ . Alors  $ab \in I$  donc  $a \in I$  ou  $b \in I$ . Comme  $a, b \in B$ , on a  $a \in I \cap B$  ou  $b \in I \cap B$ . Donc, si  $I \cap B$  est propre,  $I \cap B$  est premier.
2. Soit  $J$  un idéal premier de  $\mathbb{Z}[X]$ . Alors  $J \cap \mathbb{Z}$  est soit  $\mathbb{Z}$  soit un idéal premier de  $\mathbb{Z}$ . Si  $J \cap \mathbb{Z} = \mathbb{Z}$ , alors  $1 \in J$ , et donc  $J = \mathbb{Z}[X]$ , ce qui est exclu. On en déduit que  $J = (0)$  ou  $J = (p)$  avec  $p$  premier.
3. On suppose  $J \cap \mathbb{Z} = (0)$  et  $J \neq (0)$ . Soit alors  $f$  un polynôme de  $J \setminus \{0\}$  de degré minimal. Notons  $f = c(f)f_0$  où  $f_0 \in \mathbb{Z}[x]$  est primitif. Comme  $J$  est premier, on a  $c(f) \in J$  ou  $f_0 \in J$ . Comme  $J \cap \mathbb{Z} = \{0\}$ , le premier cas est exclu, donc  $f_0 \in J$ .

Soit maintenant  $g \in J$ . Soit  $g = f_0q + r$  la division euclidienne de  $g$  par  $f_0$  dans  $\mathbb{Q}$  ( $q, r \in \mathbb{Q}[x]$ ). Notons  $q = \frac{a}{b}q_0$  avec  $q_0 \in \mathbb{Z}[x]$  primitif, et  $r = \frac{a'}{b'}r_0$ , avec  $r_0 \in \mathbb{Q}[x]$  primitif.

Alors  $bb'g = ab'q_0f_0 + a'b'r_0$ . On en déduit que  $a'b'r_0 \in J$ , et pour des raisons de degré,  $r_0 = 0$ . Finalement,  $bb'g = ab'q_0f_0$ , et en considérant les contenus, on en déduit que  $bb' | ab'$ , donc  $b | a$ , et donc  $q \in \mathbb{Z}[x]$ . On en déduit que  $g \in (f_0)$ , et finalement  $J = (f_0)$ .

4. On suppose que  $J \cap \mathbb{Z} = (p)$ . Soit  $r_p$  la projection  $\mathbb{Z}[x] \rightarrow \mathbb{Z}_p[x]$ . Soit  $\alpha, \beta \in \mathbb{Z}_p[x]$  tels que  $\alpha\beta \in r_p(J)$ . Soit  $f, g$  des représentants de  $\alpha$  et  $\beta$  (i.e.  $r_p(f) = \alpha$ ,  $r_p(g) = \beta$ ). Alors  $fg \in r_p^{-1}(r_p(J)) = J + (p) = J$ . Donc  $f \in J$  ou  $g \in J$ , et donc  $\alpha \in r_p(J)$  ou  $\beta \in r_p(J)$  :  $r_p(J)$  est premier.

$\mathbb{Z}_p[x]$  est principal, donc il existe un polynôme  $\pi$  irréductible dans  $\mathbb{Z}_p[x]$  tel que  $r_p(J) = (\pi)$ . Soit  $g$  un représentant de  $\pi$ . Alors  $J = (p, g)$  : en effet, on a vu que  $J = r_p^{-1}((\pi))$  et  $r_p^{-1}((\pi)) = (g) + (p) = (p, g)$ .

5. Supposons  $J$  maximal dans  $\mathbb{Z}[x]$ .  $J$  est en particulier premier, donc a une des deux formes ci dessus. Supposons  $J = (f)$ , avec  $f$  irréductible et primitif. Soit  $p$  un nombre premier ne divisant pas le coefficient dominant de  $f$ . Alors  $J \subset (p, f) \subset \mathbb{Z}[x]$ , mais  $(p, f) \neq \mathbb{Z}[x]$ . En effet, sinon, il existerait  $g, h \in \mathbb{Z}[x]$  tels que  $1 = pg + fh$ , et en considérant la réduction modulo  $p$ ,  $\bar{f}$  serait inversible dans  $\mathbb{Z}_p[x]$  : comme  $\deg \bar{f} > 0$ , c'est impossible. On en déduit que  $J$  n'est pas maximal.

$J$  est donc de la forme  $(p, g)$ , avec  $r_p(g)$  irréductible dans  $\mathbb{Z}_p[x]$ .