

Algèbre : Série 8

Exercice 1

- Démontrer que si un polynôme de $\mathbb{Z}[X]$ non constant n'est pas irréductible dans $\mathbb{Q}[X]$ alors il est produit de deux polynômes non constants à coefficients dans \mathbb{Z} .

Soit A un anneau factoriel (par exemple \mathbb{Z}) et Q_A son corps de fractions et soit $f(X) = \sum_{i=0}^n a_i X^i \in A[X]$.

Définition

On appelle contenu de f le p.g.c.d des coefficients de f .

$$c(f) = \text{pgcd}(a_0, a_1, \dots, a_n).$$

Remarquons que si $c(f) = c$ alors $f = cf_1$ avec $c(f_1) = 1$.

Lemme

Lemme de Gauss. Soient $f, g \in A[X]$ alors $c(fg) = c(f)c(g)$.

PREUVE

Par la remarque, il suffit de montrer que si $f, g \in A[X]$ tels que $f \neq 0, g \neq 0, c(f) = c(g) = 1$ alors $c(fg) = 1$.

Soit p un nombre premier. Comme $c(f) = c(g) = 1$ alors p ne divise pas tous les coefficients de f et de g également. On écrit

$$f(X) = a_n X^n + \dots + a_0, \quad g(X) = b_m X^m + \dots + b_0, \quad fg = c_{m+n} X^{m+n} + \dots + c_0.$$

Soient r et s les plus petits entiers tels que p ne divise pas a_r et p ne divise pas b_s . Dans le produit fg on considère le coefficient du monôme X^{r+s} qui est égal à

$$a_0 b_{r+s} + \dots + a_r b_s + \dots + a_{r+s} b_0.$$

Par définition p divise tous les termes de cette somme sauf $a_r b_s$. Par conséquent p ne divise pas c_{r+s} .

Conclusion $c(fg) = 1$. □

Corollaire

Soit $f \in A[X]$ et $g, h \in Q_A[X]$ tels que $f = gh$. alors il existe $g', h' \in A[X]$ et $r, s \in Q_A \setminus \{0\}$ tels que

$$g(X) = r g'(X), \quad h(X) = s h'(X), \quad f = c(f) g' h', \quad c(g') = c(h') = 1.$$

PREUVE

On désigne par a et b les ppcm des dénominateurs des coefficients de g et h . On a alors $g = \frac{1}{a} g_1$ et $h = \frac{1}{b} h_1$ où $a, b \in A \setminus \{0\}$ et $g_1, h_1 \in A[X]$. On a

$$f = g.h \implies ab.f = g_1.h_1 \implies ab.c(f) = c(g_1 h_1) = c(g_1) c(h_1)$$

On pose

$$h_1 = c(h_1) h', \quad g_1 = c(g_1) g'$$

On a que $c(h') = c(g') = 1$. et par conséquent

$$ab.f = g_1.h_1 = c(g_1) c(h_1).g'h' = ab.c(f)g'h' \implies f = c(f)g'h'.$$

De plus

$$g = \frac{1}{a} g_1 = \frac{c(g_1)}{a} g', \quad h = \frac{1}{b} h_1 = \frac{c(h_1)}{b} h'$$

2. En déduire la critère d'Eisenstein :

Soit $f(X) = a_0 + a_1X + \dots + a_nX^n$ un polynôme de $\mathbb{Z}[X]$ et p un nombre premier tel que

- (a) p divise a_0, \dots, a_{n-1} ;
- (b) p ne divise pas a_n ;
- (c) p^2 ne divise pas a_0 .

Alors f est irréductible dans $\mathbb{Q}[X]$.

PREUVE

Supposons que f soit réductible dans $\mathbb{Q}[X]$ donc aussi réductible dans $\mathbb{Z}[X]$ d'après la question précédente. Soient alors $g, h \in \mathbb{Z}[X]$ tels que $f = gh$. Comme p ne divise pas a_n , il ne divise pas $c(f)$, et puisque $c(f) = c(g)c(h)$ on peut alors se ramener au cas où $c(f) = c(g) = c(h) = 1$. On a

$$f(X) = a_nX^n + \dots + a_0, \quad g(X) = b_rX^r + \dots + b_0, \quad h = c_sX^s + \dots + c_0. \quad r \geq 1, s \geq 1, n = r + s$$

On a $a_0 = b_0c_0$ et par (a) et (c) on a $p|b_0$ **ou bien** $p|c_0$. On peut supposer que $p|b_0$ **et** $p \nmid c_0$. Tous les coefficients de g ne sont pas divisibles par p sinon $p|a_n$. On considère alors le plus petit entier i tel que le coefficient b_i n'est pas divisible par p . On a

$$i \leq r - 1 \leq n - 1, \quad a_i = b_i c_0 + \dots + b_0 c_i$$

Comme $i \leq n - 1$ on sait que p divise a_i et par définition de i il divise tous les coefficients b_k avec $k < i$. donc

$$p|(a_i - b_{i-1}c_1 + \dots + b_0c_i) = b_i c_0$$

Comme p ne divise pas b_i et p premier alors il divise c_0 . On aboutit à une contradiction.

Exercice 2

Soit $P \in \mathbb{Z}[X]$, avec coefficient dominant 1. Montrer que toutes les racines rationnelles de P sont entières.

PREUVE

Soit $\alpha = \frac{p}{q}$ une racine rationnelle de P avec $p \wedge q = 1$. Donc il existe $Q \in \mathbb{Q}[X]$ tel que

$$P(X) = (X - \frac{p}{q})Q(X).$$

On désigne par b le ppcm de tous les dénominateurs des coefficients de Q et soit $Q_1 \in \mathbb{Z}[X]$ tel que $Q = \frac{Q_1}{b}$. On a alors

$$qbP = (qX - p)Q_1(X)(*).$$

Comme le polynome P est unitaire, on, a $c(P) = 1$ et par suite $qb = c(Q_1)$. On en déduit que b divise tous les coefficients de Q_1 et donc Q est à coefficients entiers et par suite $b = 1$. Le coefficient dominant de Q est divisible par q puisque $c(Q) = q$ et par la relation (*) on déduit que q divise le coefficient dominant de P qui est 1. Par conséquent $q = 1$.

Exercice 3

1. Soit $P \in \mathbb{Z}[X]$ tel que $P(0)$ et $P(1)$ sont impairs. Montrer que P n'a pas de racines entiers.

PREUVE

Si k est une racine de P alors on peut factoriser dans $\mathbb{Z}[X]$ le polynôme P par $X - k$.

$$P(X) = (X - k)Q(X)$$

On a $P(0) = -kQ(0)$ et $P(1) = (1 - k)Q(1)$. Comme $P(0)$ et $P(1)$ sont impairs donc non nuls et que $-k$ et $1 - k$ sont de parités différentes on aboutit à une contradiction. \square

2. Montrer que $P(X) \in \mathbb{Z}[X]$ est irréductible si et seulement si $P(X + 1)$ est irréductible.

PREUVE
Evident

□

3. Montrer que pour p premier, le p -ième polynôme cyclotomique

$$\Phi_p(X) = X^{p-1} + X^{p-2} + \dots + X^2 + X + 1$$

est irréductible dans $\mathbb{Z}[X]$.

PREUVE
On a

$$\Phi_p(X + 1) = (X + 1)^{p-1} + (X + 1)^{p-2} + \dots + (X + 1)^2 + (X + 1) + 1 = \sum_{k=0}^{p-1} \left(\sum_{i=k}^{p-1} \binom{i}{k} \right) X^k$$

En utilisant la formule combinatoire

$$\sum_{i=k}^n \binom{i}{k} = \binom{n+1}{k+1}$$

On obtient

$$\Phi_p(X + 1) = \sum_{k=0}^{p-1} \binom{p}{k+1} X^k = X^{p-1} + \sum_{k=1}^{p-2} \binom{p}{k+1} X^k + p$$

Comme p est premier, on sait que p divise tous les coefficients du binôme $\binom{p}{k+1}$ pour $1 \leq k+1 \leq p-1$. On peut alors appliquer le critère d'Eisenstein pour conclure. □

Deuxième preuve Remarquons d'abord que

$$\Phi_p(X) = X^{p-1} + X^{p-2} + \dots + X^2 + X + 1 = \frac{X^p - 1}{X - 1} \implies \Phi_p(X+1) = \frac{(X+1)^p - 1}{X} = X^{p-1} + \sum_{k=1}^{p-2} \binom{p}{k+1} X^k + p.$$

On applique ensuite Eisenstein.

Exercice 4

Montrer que les polynômes suivants sont irréductibles dans $\mathbb{Z}[X]$.

1. $X^2 - 2011X + 2011$;

Appliquer Eisenstein en remarquant que 2011 est premier.

2. $X^5 + 5X^2 + 1$;

Considérer $P(X - 1)$.

3. $X^4 + 3X^2 + 3$;

prendre $p = 3$.

4. $X^4 + X + 1$;

PREUVE

Remarquons d'abord que le polynôme n'a pas de racines entières puis que $P(0)$ et $P(1)$ sont impairs (Exercice 3.) Par conséquent, si le polynôme n'est pas irréductible, il se décompose en produit de deux polynômes à coefficients entiers de degré 2 chacun

$$X^4 + X + 1 = (X^2 + ax + b)(X^2 + cX + d)$$

En développant on doit avoir

$$c = -a; d = \frac{1}{b}; b + \frac{1}{b} = a^2; \frac{a}{b} - ab = 1.$$

Comme b est un entier, on doit avoir $b = 1$ et $a^2 = 2$, ce qui n'est pas possible. □

5. $X^4 + 1$.

Considérer $P(X + 1)$ et appliquer Eisenstein avec $p = 2$.

Exercice 5

Soit p un nombre premier. On note $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ le corps à p éléments. Dans les cas suivants, le polynôme $P(X)$ est-il irréductible dans $\mathbb{F}_p[X]$?

1. $p = 3$ et $P(X) = X^2 - 2011X + 2011$;

On a $2011 \equiv 1 \pmod{3}$ et $X^2 - 2011X + 2011 \equiv X^2 + 2X + 1 = (X + 1)^2$.

2. $p = 5$ et $P(X) = X^5 + 5X^2 + 1$;

$$X^5 + 5X^2 + 1 = X^5 + 1 = (X + 1)(X^4 - X^3 + X^2 - X + 1).$$

3. $p = 7$ et $P(X) = X^4 + 3X^2 + 3$;

$$P(1) = 7 \equiv 0.$$

4. $p = 11$ et $P(X) = X^4 + X + 1$;

X	0	1	2	3	4	5	6	7	8	9	10
P(X)	1	3	8	8	8	4	5	0	2	4	1

le polynôme admet 7 comme racine et on a dans $\mathbb{F}_{11}[X]$ la factorisation

$$X^4 + X + 1 = (X - 7)(X^3 + 7X^2 + 5X + 3).$$

Exercice 6

Pour p premier, on note $\mathbb{F}_p^* = \mathbb{F}_p \setminus \{0\}$. Un élément $x \in \mathbb{F}_p$ est un *carré* s'il existe $a \in \mathbb{F}_p$ tel que $a^2 \equiv x \pmod{p}$.

1. Soit $p \geq 3$ premier. Montrer qu'il y a $\frac{p-1}{2}$ carrés dans \mathbb{F}_p^* .

PREUVE

On considère l'application

$$\phi : \mathbb{F}_p^* \longrightarrow \mathbb{F}_p^* \\ x \longmapsto x^2$$

L'application ϕ est un morphisme du groupe multiplicatif \mathbb{F}_p^* dont le noyau est $\{1, -1\}$. On applique le premier théorème d'isomorphisme et on que

$$\mathbb{F}_p^*/\{1, -1\} \cong \text{Im}(\phi).$$

Comme le groupe $\mathbb{F}_p^*/\{1, -1\}$ contient $\frac{p-1}{2}$ éléments, on conclut qu'il y a $\frac{p-1}{2}$ carrés. \square

2. Soit $p \geq 3$ premier. Montrer qu'un au moins -1 , 2 ou -2 est un carré dans \mathbb{F}_p^* . Pour cela, montrer que, si -1 n'est pas un carré, alors 2 ou -2 est un carré dans \mathbb{F}_p^* .

PREUVE

Supposons que -1 ne soit pas un carré et soit $x \in \mathbb{F}_p^*$, alors x ou bien $-x$ est un carré. En effet si x et $-x$ sont des carrés et $p \neq 2$, on a

$$x = a^2 \quad \text{et} \quad -x = b^2 \implies -1 = \left(\frac{a}{b}\right)^2.$$

Comme dans \mathbb{F}_p^* il y a $p - 1$ éléments, la moitié sont des carrés et l'autre moitié est constituée des opposés des carrés. \square

3. Démontrer que le polynôme $X^4 + 1$ est réductible dans \mathbb{F}_p , pour tout nombre premier $p \geq 2$.

PREUVE

On distingue deux cas selon que -1 est un carré ou non.

- S'il existe $a \in \mathbb{F}_p$ tel que $a^2 = -1$ alors on peut écrire

$$X^4 + 1 = X^4 - a^2 = (X^2 - a)(X^2 + a).$$

- Si -1 n'est pas un carré, alors il existe $a \in \mathbb{F}_p$ tel que $a^2 = 2$ ou $a^2 = -2$. En remarquant que

$$(X^2 + aX + 1)(X^2 - aX + 1) = X^4 + (2 - a^2)X^2 + 1 = X^4 + 1 \quad \text{si } a^2 = 2$$

ou

$$(X^2 + aX - 1)(X^2 - aX - 1) = X^4 - (2 + a^2)X^2 + 1 = X^4 + 1 \quad \text{si } a^2 = -2.$$

On peut conclure dans tous les cas de la réductibilité de $X^4 + 1$. □

Exercice 7

Soit k un corps. On note I le sous-ensemble de $k[X]$ formé des polynômes dont la somme des coefficients est nulle. Montrer que I est un idéal de $k[X]$ et trouver $P \in k[X]$ tel que $I = (P)$.

PREUVE

Il est évident que I est un idéal de $k[X]$ et que $X - 1 \in I$. Remarquons d'abord que le seul polynôme constant qui appartient à I est le polynôme nul.

Soit $A \in I$. En effectuant la division euclidienne de A par $X - 1$ on obtient

$$A = (X - 1)Q(X) + R, \quad \deg(R) < 1.$$

Le polynôme R est alors constant et appartient à I . Donc $R = 0$.

Conclusion : $I = (X - 1)$ □

Exercice 8

Soit A un anneau commutatif et unitaire. Montrer que $A[X]$ est principal si et seulement si A est un corps.

PREUVE

On sait que si A est un corps alors l'anneau des polynômes $A[X]$ est un anneau euclidien donc principal.

Réciproquement on suppose que l'anneau $A[X]$ est principal. Soit $a \in A$ non nul et montrons que a est inversible. On considère l'idéal $I(a, X)$ engendré par a et X . Comme $A[X]$ est principal il existe $P \in A[X]$ tel que $I = (P)$. Ce polynôme P est forcément constant puisque a est un multiple de P . Donc il existe $(\alpha, \beta, \gamma) \in A^3$ tels que

$$a = \alpha R, \quad X = (\beta X + \gamma)R = R\beta X + R\gamma \implies R\beta = 1, \gamma = 0.$$

On obtient

$$a\beta = \alpha R\beta = \alpha \cdot 1 = \alpha \implies R = 1 \implies 1 \in I \text{ et } I = A[X].$$

En écrivant que $1 \in (a, X)$ sous la forme $1 = aP + XQ$ et en évaluant l'expression en $X = 0$ on obtient $1 = aP(0)$. Donc a est inversible.