Anneaux et corps

Contents

1 Anneaux

1.1 Définition

$(A, +, \times)$ est un anneau si
- $(A, +)$ est un groupe abélien.
- La multiplication est associative, et possède un élément neutre 1_A.
- La multiplication est distributive par rapport à l'addition.

Anneau commutatif

Si de plus la multiplication est commutative.

Inversibles

On appelle inversibles les éléments qui ont un symétrique pour $\times$.

1.2 Exemples

$\mathbb{R}$, $\mathbb{Z}$, $M_n(K)$, $(L(E), +, \circ)$, $(F(I, \mathbb{C}), +, \times)$, $(K[X], +, \times)$.
$(F(\mathbb{R}, \mathbb{R}), +, \circ)$?

Réponse

Ce n'est pas un anneau car la distributivité n'est pas vérifiée.

1.3 Sous-anneau

1.3.1 Définition

B est un sous-anneau de A si
- B est un sous-groupe de $(A, +)$.
- B est stable pour la multiplication.
- $1_A \in B$.

1.3.2 Remarque

Si B est un sous-anneau de A, B est un anneau pour les lois induites.

Pour montrer qu'un ensemble est un anneau, on montre en général que c'est un sous-anneau d'un anneau connu.

1.3.3 Exemples

Dans l'anneau $A = (F(\mathbb{R}, \mathbb{C}), +, \times)$ des fonctions de $\mathbb{R}$ dans $\mathbb{C}$, sont-ils des sous-espaces vectoriels, sont-ils stables pour $\times$, sont-ils des sous-anneaux :
- l'ensemble des fonctions continues
- l'ensemble des fonctions dérivables
- l'ensemble des fonctions bornées
- l'ensemble des fonctions continues bornées intégrables
- l'ensemble des fonctions qui tendent vers 0 en $+\infty$
- l'ensemble des fonctions continues intégrables
- l'ensemble des fonctions entières (DSE de rayon infini)
- l'ensemble des fonctions DSE de rayon $R > 0$ fixé

Réponse

Tous sauf le dernier sont des sous-espaces vectoriels.
Tous sauf deux sont stables pour $\times$.
Plusieurs ne sont pas des sous-anneaux car ils ne contiennent pas 1_A.

1.4 Produit fini d'anneaux

Analogue au produit fini de groupes ; voir le théorème chinois ; sinon, pas grand intérêt...

Exercice

(a, b) est inversible dans $A \times B$ si et seulement si a est inversible dans A et b inversible dans B.

1.5 Morphisme d'anneaux

1.5.1 Définition

Soit A et B deux anneaux, et $f : A \to B$; f est un morphisme d'anneaux si
- f est un morphisme pour $+$
- f est un morphisme pour $\times$
- $f(1_A) = 1_B$

1.5.2 Remarques

Soit f est un morphisme d'anneaux de A dans B.
- L'image de f est un sous-anneau de B.
- Le noyau rarement ; on verra que le noyau est un idéal de A.
- $f(0) = 0$: ce n'est pas un axiome.
- L'image de tout élément inversible de A est inversible dans B.

1.5.3 Exemple : $\mathbb{Z}$

Trouver les endomorphismes d'anneau de $\mathbb{Z}$.

1.5.4 Exercice : $\mathbb{R}$

Montrer que le seul endomorphisme d'anneau f de $\mathbb{R}$ est Id.

Démonstration

On montre par récurrence sur n que pour tout morphisme de groupe g de $\mathbb{R}$ dans $\mathbb{R}$:

$$\forall n \in \mathbb{N}, \forall x \in \mathbb{R}, g(n.x) = n.g(x)$$

En particulier :

$$\forall n \in \mathbb{N}, f(n) = n$$

On montre que $\forall r \in \mathbb{Q}, f(r) = r$.

Soit $r = \frac{p}{q} \in \mathbb{Q}$; $p = f(p) = f(q.r) = q.f(r)$, donc $f(r) = r$.

Ensuite, on montre que f est croissante

Soit $a \in \mathbb{R}$; soit $h > 0$; $f(a+h) - f(a) = f(h) = \left(f\left(\sqrt{h}\right)\right)^2 \geq 0$.

Supposons par l'absurde l'existence de x tel que $f(x) \neq x$.

Par exemple, $f(x) > x$.

On sait qu'il existe un rationnel r tel que

$$x < r < f(x)$$

f étant croissante : $f(x) \leq f(r) = r$, contradiction ; conclusion :

$$f = \mathrm{Id}$$

1.5.5 Exemple : $\mathbb{C}$

Trouver deux endomorphismes d'anneau de $\mathbb{C}$.

Montrer que ce sont les seuls endomorphismes d'anneau de $\mathbb{C}$ continus.

1.5.6 Polynômes

Soit

$$\begin{array}{rl} \varphi : & K[X] \to K^K \\ & P \to \widetilde{P} \end{array}$$

où $\varphi(P) = \widetilde{P}$ est la fonction polynômiale associée à P.

- φ est un morphisme d'anneaux.
- Il est injectif si K est infini.
- Il est surjectif si K est fini (HP).

1.6 Inversibles

1.6.1 Théorème

L'ensemble des éléments inversibles d'un anneau A constitue un groupe pour la loi ... ?

On le note $U(A)$ ou $A^\times$.

Démonstration

Notons $G = U(A)$.

- Soit x, y deux éléments de G et $z = x.y$; z possède un inverse : $y^{-1}.x^{-1}$; donc G est stable pour $\times$.
- Il y a un élément neutre : 1_A.
- La multiplication est associative.
- Soit x un élément de G ; soit $y = x^{-1}$; alors $y \in G$; pourquoi ?

1.6.2 Exemple

$A = \mathbb{Z}$; $U(A)$?

Réponse

$\{-1, 1\} = \mathbb{U}_2$

1.6.3 Exemple

$A = (L(E), +, \circ)$; $U(A)$?

Réponse

$GL(E)$

1.6.4 Exemple

$A = \mathbb{Z}[i] = \{u + iv / \ u, v \in \mathbb{Z}\}$; $U(A)$?

$U(A) = \mathbb{U}_4$.

Démonstration

$(a + ib)(c + id) = 1$; on en déduit $\left(a^2 + b^2\right)\left(c^2 + d^2\right) = 1$...

1.7 Deux formules

Soit a et b deux éléments d'un anneau tels que $a.b = b.a$; soit $n \geq 1$.

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} . a^k . b^{n-k}$$

$$a^n - b^n = (a-b) . \sum_{k=0}^{n-1} a^k . b^{n-1-k}$$

2 Anneaux intègres et corps

2.1 Définitions

2.1.1 Anneau intègre

$(A, +, .)$ est intègre si

- A est un anneau commutatif.
- $A \neq \{0\}$.
- $\forall x, y \in A - \{0\}$, $x.y \neq 0$.

Remarque

Dans un anneau intègre, on peut simplifier par tout élément non nul : si $a \neq 0$, alors

$$ax = ay \Longrightarrow x = y$$

En effet, $a(x - y) = 0$ et $a \neq 0$.

Comparaison au cas des groupes.

2.1.2 Corps

$(K, +, .)$ est un corps si
- K est un anneau commutatif.
- $K \neq \{0\}$.
- Tout élément de $K - \{0\}$ est inversible : $K - \{0\} = K^{\times}$.

2.1.3 Tout corps est un anneau intègre

Démonstration

Soit x et y deux éléments d'un corps K tels que $x.y = 0$.
Si x est non nul :

$$x^{-1}.(x.y) = 0$$

Donc $y = 0$.

2.2 Sous-corps

Définition

Soit K une partie d'un corps $(L, +, \times)$; K est un sous-corps de L si K est stable pour les deux lois, et constitue un corps pour les lois induites.

Caractérisation

Pour montrer que K est un sous-corps de L, on vérifie que :
- K est un sous-groupe de $(L, +)$
- K est stable pour $\times$
- $1_L \in K$
- Pour tout élément x non nul de K, $\frac{1}{x}$ appartient à K

Exercice

Tout sous-corps de $\mathbb{R}$ contient $\mathbb{Q}$.

2.3 Exemples

Exemples de corps :

$$\mathbb{C}, \mathbb{R}, \mathbb{Q}, K(X)$$

Des anneaux intègres qui ne sont pas des corps :

$$\mathbb{Z}, \mathbb{Z}[i], K[X], \mathbb{D}$$

$$\mathbb{D} = \left\{ \frac{p}{10^q} / \, p \in \mathbb{Z}, q \in \mathbb{N} \right\}$$

Des anneaux non intègres :
$M_n(\mathbb{R})$, $L(E)$...
Des anneaux commutatifs non intègres :
$(F(I, \mathbb{C}), +, \times)$, $D_n(\mathbb{C})$: les matrices diagonales de $M_n(\mathbb{C})$.

2.4 Le corps $\mathbb{Q}\left[\sqrt{2}\right]$

Exercice

On pose $K = \mathbb{Q}\left[\sqrt{2}\right] = \left\{x + y\sqrt{2} / \, x, y \in \mathbb{Q}\right\}$; montrer que c'est un corps.

Démonstration

Soit $z = x + y\sqrt{2}$ un élément non nul de K.

$$\frac{1}{z} = \frac{x - y\sqrt{2}}{x^2 - 2y^2} \in K$$

2.5 Corps et polynômes

2.5.1 Racines

Théorème

Soit K un corps, et $P \in K[X]$ un polynôme de degré $n \geq 1$; alors P a au plus n racines.

Démonstration

Par récurrence sur n ; c'est clair pour $n = 1$.

Soit $n \geq 2$; supposons la propriété au rang $n-1$; soit P de degré n ; si P a une racine a :

$$P = (X - a).Q$$

Conclusion ?

2.5.2 Matrices réelles semblables dans $M_n(\mathbb{C})$

Exercice

Deux matrices réelles semblables dans $M_n(\mathbb{C})$ le sont dans $M_n(\mathbb{R})$.

Démonstration

Soit $A, B \in M_n(\mathbb{R})$; on les suppose semblables dans $M_n(\mathbb{C})$; soit $P \in GL_n(\mathbb{C})$ telle que

$$B = P^{-1}.A.P$$

Alors

$$P.B = A.P$$

Ecrivons $P = P_1 + iP_2$ avec $P_1, P_2 \in M_n(\mathbb{R})$; on en déduit facilement

$P_1.B = A.P_1$ et $P_2.B = A.P_2$; puis, si on note

$$M_t = P_1 + t.P_2$$

Alors :

$$\forall t \in \mathbb{R}, M_t.B = A.M_t$$

Il reste à montrer l'existence de $t \in \mathbb{R}$ tel que M_t soit inversible ; comment ?

Réponse

$Q : t \to \det(M_t) = \det(P_1 + t.P_2)$ est une fonction polynomiale telle que $Q(i) \neq 0$; donc il existe $t \in \mathbb{R}$ tel que $Q(t) \neq 0$.

2.6 Divisibilité

Dans un anneau commutatif A, on dit que x divise y si :

$$\exists u \in A,\ x.u = y$$

On dit aussi que y est un multiple de x.

Notation

On note

$$(x) = x.A = \{x.u / u \in A\}$$

l'ensemble des multiples de x. Remarquons que x divise y si et seulement si $(y) \subset (x)$.

Condition pour que $(x) = (y)$: chacun des deux divise l'autre.

Exercice

On suppose que A est intègre.
Montrer que $(x) = (y)$ si et seulement si $\exists u \in U(A)$, $y = u.x$.

Démonstration

Supposons que x divise y et y divise x :

$$\exists u \in A,\ x.u = y$$

et

$$\exists v \in A,\ y.v = x$$

Donc

$$y = (y.v).u$$

Donc

$$y.(1 - v.u) = 0$$

Si y n'est pas nul, $u \in U(A)$.

3 Idéaux d'un anneau commutatif

3.1 Définition

I est un idéal de A si
- I est un sous-groupe de $(A, +)$.
- $\forall x \in I, \forall y \in A,\ x.y \in I$.

3.2 Exemples

3.2.1 Dans $\mathbb{Z}$

L'ensemble des entiers pairs, multiples de 3...

3.2.2 Idéaux principaux

Soit a un élément de l'anneau A ; on note (a) ou $a.A$ l'ensemble des multiples de a :

$$a.A = \{a.x / x \in A\}$$

Il s'agit d'un idéal de A.

3.2.3 Le noyau

Théorème

Le noyau d'un morphisme d'anneaux est un idéal.

3.2.4 Les nilpotents

$$N = \{x \in A / \exists q \geq 1, x^q = 0\}$$

A étant commutatif, N est un idéal de A.
En particulier, si $q, r \geq 1$ et $x^q = 0$ et $y^r = 0$, alors $(x + y)^s = 0$ avec $s = ?$

Réponse

$s = q + r - 1$.

3.3 Idéaux de $\mathbb{Z}$

Théorème

Tous les idéaux de $\mathbb{Z}$ sont principaux : $n\mathbb{Z}$, où n décrit $\mathbb{N}$.

3.4 Propriétés

3.4.1 Toute intersection d'idéaux est un idéal.

3.4.2 Somme

On note $I + J = \{x + y / x \in I, y \in J\}$; la somme de deux idéaux est un idéal.

3.4.3 Produit

Exercice

On note $I.J$ l'ensemble des sommes de produits $x.y$ où $x \in I$ et $y \in J$; $I.J$ est un idéal.

3.5 Un idéal non principal

Exercice

$A = \mathbb{Z}[X]$; $I = \{P \in A / P(0) \in 2\mathbb{Z}\} = 2.A + X.A$.
Montrer qu'il n'est pas principal.

Démonstration

Supposons $I = P.\mathbb{Z}[X]$; donc 2 et X sont multiples de P ; donc P est constant : $P = p \in \mathbb{Z}$; finalement, $p = \pm 1$: impossible car $P \in I$.

4 Exercices : étude de l'anneau $A = \mathbb{Z}\left[\sqrt{2}\right]$

4.1 $\mathbb{Z}\left[\sqrt{2}\right] = \left\{a + b\sqrt{2} / a, b \in \mathbb{Z}\right\}$

Montrer que c'est un anneau.

4.2 L'application σ

Soit $\sigma : a + b\sqrt{2} \to a - b\sqrt{2}$; est-elle bien définie ? Que dire de σ?

Réponse

Elle est bien définie car $\sqrt{2}$ est irrationnel ; σ est un automorphisme d'anneau involutif.

4.3 Inversibles

Montrer que $z = a + b\sqrt{2}$ est inversible dans A si et seulement si

$$a^2 - 2b^2 = \pm 1$$

4.4 Lemme

Montrer que $U(A) \cap \left]1, 1 + \sqrt{2}\right[= \varnothing$. (Examiner les signes de a et b).

4.5 Conclusion

Montrer que

$$U(A) = \left\{\pm\left(1 + \sqrt{2}\right)^n / n \in \mathbb{Z}\right\}$$

5 Arithmétique dans $\mathbb{Z}$

5.1 PGCD dans $\mathbb{Z}$

5.1.1 Définition

Soit a et b deux éléments de $\mathbb{Z}$; soit I la somme des deux idéaux (a) et (b) :

$$I = \{au + bv/u, v \in \mathbb{Z}\}$$

Soit d le générateur positif de I : $I = d\mathbb{Z}$; on pose

$$a \wedge b = d$$

Remarque : si $a = b = 0$, on pose $d = 0$.
Retenons qu'il existe u et v tels que

$$d = au + bv$$

(relation de Bézout).

5.1.2 Diviseurs communs

d divise a et b ; les diviseurs communs à a et b sont les diviseurs de d.

Démonstration

Si d' divise a et b, alors il divise $au + bv$, donc il divise d.

5.1.3 Lemme de Gauss

Soit a, b, c trois éléments de $\mathbb{Z}$; on suppose $a \wedge b = 1$ et a divise bc. Alors a divise c.

Démonstration

Soit u, v, k entiers tels que $au + bv = 1$ et $ak = bc$; en multipliant par c :

$$auc + bvc = c$$

d'où

$$auc + akv = c$$

soit

$$a\,(uc + kv) = c$$

5.1.4 Propriété

Si $p \wedge q_1 = 1$ et $p \wedge q_2 = 1$, alors $p \wedge q_1 q_2 = 1$.

Démonstration

Supposons $ap + bq_1 = 1$ et $cp + dq_2 = 1$.
Alors

$$(acp + adq_2 + bcq_1)\,p + (bd)\,q_1 q_2 = 1$$

Remarque

Si $p \wedge q = 1$, alors $p \wedge q^n = 1$ pour tout $n \geq 1$.

5.2 PPCM dans $\mathbb{Z}$

5.2.1 Définition

Soit a et b deux éléments de $\mathbb{Z}$; l'ensemble des multiples communs est

$$I = (a) \cap (b)$$

C'est donc un idéal de $\mathbb{Z}$; il existe un unique $m \geq 0$ tel que $I = m\mathbb{Z}$; les multiples communs sont exactement les multiples de m ; on note

$$m = a \vee b$$

Remarque

$m = a \vee b$ divise toujours ab.

En effet ab est un multiple commun.

5.2.2 Si $a \wedge b = 1$

Dans ce cas, $a \vee b = ab$, ou $|ab|$ dans $\mathbb{Z}$.

Démonstration

Soit $m = a \vee b$.

- m est un multiple de b : $m = k_1.b$.
- a divise donc $k_1.b$; avec le lemme de Gauss, a divise k_1 :

$$k_1 = a.k_2$$

- donc $m = a.b.k_2$: ab divise m.

Conclusion : m divise ab et réciproquement, donc

$$m = ab$$

5.2.3 Propriétés

$\wedge$ et $\vee$ sont associatives et commutatives.

Si on multiplie a et b par un même entier q, $a \wedge b$ et $a \vee b$ sont multipliés par $|q|$.

5.2.4 Relation entre $a \wedge b$ et $a \vee b$.

Théorème

Si a et b sont dans $\mathbb{N}$, $ab = (a \wedge b) \,.\, (a \vee b)$.

Démonstration

On se ramène au cas où $a \wedge b = 1$ en posant

$$\begin{cases} d = a \wedge b \\ a = d.a' \\ b = d.b' \end{cases}$$

Dans ce cas

$$a' \wedge b' = 1$$

5.3 Les nombres premiers

5.3.1 Décomposition

Théorème

Tout entier $n \geq 2$ est produit de nombres premiers ; la décomposition est unique à l'ordre près.

Démonstration

Par récurrence sur n.

Si $n \geq 2$ n'est pas premier,

$$n = r.s$$

avec $2 \leq r \leq n-1$ et $2 \leq s \leq n-1$.

5.3.2 Infinité

Théorème

L'ensemble des nombres premiers est infini.

Démonstration

Supposons par l'absurde qu'il soit fini ; soit $\{p_1, ..., p_r\}$ l'ensemble des nombres premiers ; soit

$$n = 1 + p_1.p_2...p_r$$

n est divisible par un nombre premier, l'un des p_j, donc p_j divise 1, contradiction.

5.3.3 Valuation $p-$adique

Soit p un nombre premier, et $n \geq 2$; $v_p(n)$ est l'exposant de p dans la décomposition de n.

$v_3(48)$?
$v_2(48)$?
$v_p(a \wedge b)$?
$v_p(a.b)$?
$v_p(a \vee b)$?

Réponses

$v_3(48) = 1$
$v_2(48) = 4$
$v_p(a \wedge b) = \min(v_p(a), v_p(b))$
$v_p(a.b) = v_p(a) + v_p(b)$
$v_p(a \vee b) = \max(v_p(a), v_p(b))$

A quelle condition a divise b ?

Si pour tout p premier, $v_p(a) \leq v_p(b)$.

5.3.4 Valuation $p-$adique d'une somme

Exercice

Que dire de $v_p(a+b)$?

Réponse

Si $\alpha = v_p(a) < \beta = v_p(b)$, alors

$$v_p(a+b) = v_p(a)$$

Si $v_p(a) = v_p(b)$, alors

$$v_p(a+b) \geq v_p(a)$$

Démonstration

$a = p^{\alpha}.r$ et $b = p^{\beta}.s$; donc

$$a + b = p^{\alpha}.\left(r + p^{\beta-\alpha}.s\right)$$

De plus $r + p^{\beta-\alpha}.s$ n'est pas multiple de p si $\beta > \alpha$.

5.3.5 La formule de Legendre : $v_p(n!)$

Exercice

Soit p premier et $n \geq 1$.

$$v_p(n!) = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor$$

Démonstration

$\left\lfloor \frac{n}{p^k} \right\rfloor$ est le nombre de multiples de p^k dans $[\![1, n]\!]$. C'est donc le nombre d'éléments m de valuation $v_p(m) \geq k$.

Le nombre d'éléments de valuation exactement k est donc

$$\left\lfloor \frac{n}{p^k} \right\rfloor - \left\lfloor \frac{n}{p^{k+1}} \right\rfloor$$

Donc

$$v_p(n!) = \sum_{k=1}^{\infty} k\left(\left\lfloor \frac{n}{p^k} \right\rfloor - \left\lfloor \frac{n}{p^{k+1}} \right\rfloor\right) = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor$$

Le rapport de tout ça avec l'espérance ?

$n \geq 1$ et p premier étant fixés, v_p est une variable aléatoire sur

$$\Omega = [\![1, n]\!]$$

On a vu que

$$E(v_p) = \sum_{k=1}^{\infty} \mathbb{P}(v_p \geq k)$$

Or

$$E(v_p) = \frac{1}{n}.\sum_{j=1}^{n} v_p(j) = \frac{1}{n}.v_p(n!)$$

et

$$\mathbb{P}(v_p \geq k) = \frac{1}{n}.\left\lfloor \frac{n}{p^k} \right\rfloor$$

6 L'algorithme d'Euclide

6.1 Lemme

Soit $a, b, k \in \mathbb{Z}$.

$$a \wedge b = (a + kb) \wedge b$$

6.2 L'algorithme d'Euclide

Supposons $a_0 \geq a_1 \geq 0$; on veut calculer $d = a_0 \wedge a_1$.

Si $a_1 = 0$, $d = a_0$

Sinon : $a_0 = a_1 q_1 + a_2$ et $d = a_1 \wedge a_2$; remarquons que $a_0 \geq a_1 > a_2$.

$$\begin{gathered} a_0 = a_1 q_1 + a_2 \\ a_1 = a_2 q_2 + a_3 \\ \ldots \\ a_{n-2} = a_{n-1} q_{n-1} + a_n \\ a_{n-1} = a_n q_n \end{gathered}$$

$$a_0 \geq a_1 > a_2 > ... > a_n > a_{n+1} = 0$$

$$d = a_0 \wedge a_1 = a_n$$

6.3 La complexité de l'algorithme

Problème

6.3.1 n étant donné, minorer a_1.

Réponse

$$a_n \geq 1,\ a_{n-1} \geq 2,\ a_{n-2} \geq a_{n-1} + a_n,\ ...,\ a_1 \geq a_2 + a_3$$

ce qui fait penser à ?

6.3.2 Les nombres de Fibonacci

$$F_0 = 0,\ F_1 = 1,\ F_{n+2} = F_{n+1} + F_n$$

On constate que :

$$a_n \geq F_2,\ a_{n-1} \geq F_3, ...,\ a_1 \geq F_{n+1}$$

6.3.3 Calcul de F_n

$F_n = \frac{1}{\sqrt{5}}\left(\beta^n - \alpha^n\right)$ où $\alpha = \frac{1-\sqrt{5}}{2}$ et $\beta = \frac{1+\sqrt{5}}{2}$.

Conclusion :

$$n \leq \frac{\ln a_1}{\ln \beta} + C$$

Il s'agit donc d'un algorithme très rapide.

6.4 Equation $au + bv = c$

Exercice

Soit a, b, c entiers ; on suppose $a \wedge b = 1$; connaissant une solution (u_0, v_0) de l'équation $au + bv = c$, les trouver toutes.

Réponse

Remarquons que a et b ne sont pas nuls tous les deux ; on suppose par exemple b non nul.

On part de

$$au + bv = au_0 + bv_0$$

Alors

$$a\left(u - u_0\right) = b\left(v_0 - v\right)$$

On utilise le théorème de Gauss : b divise $u - u_0$; on écrit

$$u = u_0 + kb$$

et on remplace dans l'équation. On obtient

$$v = v_0 - ka$$

Réciproquement, on vérifie que les couples suivants sont des solutions

$$\{u_0 + kb, v_0 - ka / \ k \in \mathbb{Z}\}$$

Remarque

Comment trouver au moins une solution ? Réponse :

6.5 L'algorithme d'Euclide étendu

$d = a_n$ s'exprime en fonction de a_{n-1} et a_{n-2} ; a_{n-1} s'exprime en fonction de a_{n-2} et a_{n-3}...

7 Anneau $\mathbb{Z}/n\mathbb{Z}$

7.1 Multiplication dans $\mathbb{Z}/n\mathbb{Z}$ ($n \geq 1$)

On se propose de définir une multiplication dans $\mathbb{Z}/n\mathbb{Z}$ de manière analogue à l'addition :

Soit $\alpha = \overline{a}$ et $\beta = \overline{b}$; on pose

$$\alpha \times \beta = \overline{a.b}$$

Un exemple :

$n = 10$; $\alpha = \overline{6}$; $\beta = \overline{7}$; on pose $\alpha \times \beta = \overline{6.7} = \overline{42} = \overline{2}$.

Problème :

Il y a plusieurs représentants dans chaque classe ; combien ? Il est donc nécessaire de vérifier que le résultat $\alpha \times \beta$ ne dépend que de α et β.

7.1.1 Lemme

Si $a \equiv a'\,[n]$ et $b \equiv b'\,[n]$, alors $a.b \equiv a'.b'\,[n]$.

Démonstration

Si $a' = a + n.p$, $b' = b + n.q$, alors

$$a'.b' = a.b + n.\,(pb + aq + npq)$$

7.1.2 Théorème

$(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un anneau commutatif.

- L'associativité et la distributivité découlent de l'associativité et la distributivité dans $\mathbb{Z}$.
- $\overline{1}$ est l'élément neutre pour $\times$.

7.2 Inversibles

7.2.1 Théorème

$\overline{k}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ si et seulement si $k \wedge n = 1$.

Démonstration

Découle du théorème de Bézout :

$\overline{k}$ est inversible $\Longleftrightarrow \exists p \in \mathbb{Z}, \overline{k}.\overline{p} = \overline{1} \Longleftrightarrow \exists p \in \mathbb{Z}, \exists q \in \mathbb{Z}, kp = 1 + nq \Longleftrightarrow k \wedge n = 1$.

7.2.2 Exemple 1

$n = 20$; donner la liste des éléments inversibles et de leurs inverses ; ce groupe est-il cyclique ?

Réponse

$\begin{bmatrix} 1 & 3 & 7 & 9 & 11 & 13 & 17 & 19 \\ 1 & 7 & 3 & 9 & 11 & 17 & 13 & 19 \end{bmatrix}$. Non cyclique ; voir le théorème chinois.

7.2.3 Exemple 2

$n = 22$; donner la liste des éléments inversibles et de leurs inverses ; ce groupe est-il cyclique ?

Réponse

$$\begin{bmatrix} 1 & 3 & 5 & 7 & 9 & 13 & 15 & 17 & 19 & 21 \\ 1 & 15 & 9 & 19 & 5 & 17 & 3 & 13 & 7 & 21 \end{bmatrix}.$$

On montre que $\overline{3}$ est d'ordre 5 ; on en déduit que $\overline{-3} = \overline{19}$ est d'ordre 10 : le groupe est cyclique ; y a-t-il d'autres générateurs ?

Il y en a $\varphi(10) = 4$.

7.2.4 Exemple 3

Chercher l'inverse de $\overline{17}$ dans $\mathbb{Z}/427\mathbb{Z}$.

Réponse

Algorithme d'Euclide :

$$427 = 17 \times 25 + 2$$

$$17 = 2 \times 8 + 1$$

D'où

$$1 = 17 - (427 - 17 \times 25).8$$

$$1 = 17.201 - 427.8$$

On en déduit que l'inverse de $\overline{17}$ est $\overline{201}$.

7.3 Calcul de l'ordre avec Python

Calculer l'ordre de x dans le groupe $(\mathbb{Z}/n\mathbb{Z})^\times$ en supposant $n \wedge x = 1$.

```
def ordre(x,n):
    u = x  % n
    k = 1
    while u != 1:
        k += 1
        u = (u*x) % n
    return k
```

8 Corps $\mathbb{Z}/p\mathbb{Z}$

8.1 Caractérisation des corps $\mathbb{Z}/p\mathbb{Z}$

Théorème

Soit $p \geq 1$; $\mathbb{Z}/p\mathbb{Z}$ est un corps si et seulement si p est premier.

Démonstration

Si p n'est pas premier, il existe deux entiers a et b tels que

- $2 \leq a, b \leq p - 1$
- $ab = p$

$\overline{a}$ et $\overline{b}$ sont non nuls et non inversibles, donc $\mathbb{Z}/p\mathbb{Z}$ n'est pas un corps ; il n'est même pas intègre car

$$\overline{a}.\overline{b} = \overline{p} = \overline{0}$$

Si p est premier, pour tout entier k tel que $1 \leq k \leq p - 1$, $k \wedge p = 1$, donc $\overline{k}$ est inversible.

8.2 Théorème de Fermat

8.2.1 Théorème

Soit p premier et a non divisible par p ; alors $a^{p-1} \equiv 1\,[p]$.

Démonstration

Le groupe G des inversibles de $\mathbb{Z}/p\mathbb{Z}$ est de cardinal $p-1$, donc l'ordre de tout élément $\overline{a}$ de G divise $p-1$. Donc

$$\overline{a}^{p-1} = \overline{1}$$

8.2.2 Corollaire

$\forall a \in \mathbb{Z}, a^p \equiv a\,[p]$

Démonstration

Si a est un multiple de p, c'est clair ; sinon, c'est clair.

8.2.3 Une propriété des coefficients binomiaux

Si p est premier, et si $1 \leq k \leq p-1$, alors p divise $\binom{p}{k}$.

Démonstration

p divise $p! = k!\,(p-k)!\binom{p}{k}$.

Or, $p \wedge k!\,(p-k)! = 1$, donc, d'après le théorème de Gauss, p divise $\binom{p}{k}$.

8.2.4 Autre démonstration du théorème de Fermat

On montre par récurrence sur n que

$$\forall n \geq 0, n^p \equiv n\,[p]$$

Pour cela, on montre que $(n+1)^p \equiv n^p + 1\,[p]$ à l'aide de la formule du binôme.

8.3 Le théorème de Wilson

Exercice

Soit $p \geq 3$; p est premier si et seulement si p divise $1 + (p-1)!$

Démonstration

Supposons p premier ; soit G le groupe des inversibles de $\mathbb{Z}/p\mathbb{Z}$; dans G tout élément a un inverse ; cherchons ceux qui sont leur propre inverse : on résout

$$x^2 = \overline{1}$$

On obtient $\overline{1}$ et $\overline{-1}$; donc le produit des éléments de G est $\overline{-1}$:

$$\overline{1}.\overline{2}...\overline{p-1} = \overline{-1}$$

Réciproque

On suppose que p divise $1 + (p-1)!$; soit q tel que $2 \leq q \leq p-1$.

q divise $(p-1)!$, donc il ne divise pas $1 + (p-1)!$, donc il ne divise pas p.

Donc p est premier.

9 Indicatrice d'Euler

9.1 Définition

Pour $n \geq 1$, $\varphi(n)$ est le cardinal de

$$\{k / 1 \leq k \leq n,\ k \wedge n = 1\}$$

- C'est le nombre de générateurs du groupe additif $\mathbb{Z}/n\mathbb{Z}$.
- C'est donc le nombre de générateurs de tout groupe cyclique de cardinal n.
- C'est aussi le nombre d'inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$.

Premières valeurs

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 1 & 1 & 2 & 2 & 4 & 2 & 6 & 4 & 6 & 4 & 10 & 4 & 12 & 6 & 8 \end{bmatrix}$$

9.2 $n = \sum_{d|n} \varphi(d)$

Exercice

Pour tout $n \geq 1$:

$$n = \sum_{d|n} \varphi(d)$$

Démonstration

Soit

$$E = \left\{ \frac{k}{n} / 1 \leq k \leq n \right\}$$

Le cardinal de E est n ; chaque élément de E s'écrit $\frac{k}{n} = \frac{r}{d}$, avec $r \wedge d = 1$.

Pour tout diviseur d de n, notons

$$E_d = \left\{ \frac{r}{d} / 1 \leq r \leq d,\ r \wedge d = 1 \right\}$$

E_d est de cardinal $\varphi(d)$ et ces ensembles constituent une partition de E.

Variante

$E = \mathbb{U}_n$ et E_d l'ensemble des éléments de E d'ordre d.

Exemple : $n = 10$

$10 = \varphi(1) + \varphi(2) + \varphi(5) + \varphi(10) = 1 + 1 + 4 + 4$.

9.3 Si p est premier

$\varphi(p)$? $\varphi(p^n)$?

Réponses

$\varphi(p) = p - 1$; $\varphi(p^n) = p^n - p^{n-1}$.

9.4 Le théorème d'Euler

Soit $n \geq 1$ et a premier avec n ; alors

$$a^{\varphi(n)} \equiv 1\,[n]$$

Démonstration

$\overline{a}$ appartient au groupe G des inversibles de $\mathbb{Z}/n\mathbb{Z}$ qui est de cardinal $\varphi(n)$.

Il s'agit d'une généralisation du théorème de Fermat.

9.5 Exercice : $(\mathbb{Z}/p\mathbb{Z})^*$ est cyclique

9.5.1 Enoncé

Soit $(K, +, X)$ un corps ; soit G un sous-groupe fini du groupe $(K^*, \times)$; alors G est cyclique. On notera n son cardinal.

En particulier : soit p premier, K le corps $\mathbb{Z}/p\mathbb{Z}$ et G le groupe $(K^*, \times)$. G est cyclique. Combien a-t-il de générateurs ?

Réponse

$\varphi(n)$, où $n = \operatorname{card} G = p - 1$.

9.5.2 Exemple

Etudier le cas $p = 7$.

Réponse

Il y a donc deux générateurs : $\overline{3}$ et $\overline{5}$.

9.5.3 Démonstration

Pour tout diviseur d de n, notons $f(d)$ le nombre d'éléments de G d'ordre d ; on veut donc montrer que $f(n) \geq 1$. On sait déjà que

$$n = \sum_{d|n} \varphi(d)$$

De plus

$$n = \sum_{d|n} f(d)$$

Soit d un diviseur fixé de n ; on veut montrer que

$$f(d) \leq \varphi(d)$$

Supposons qu'il existe un élément a de G d'ordre d ; a engendre un sous-groupe H de cardinal d ; les éléments de H sont racines du polynôme

$$P = X^d - 1$$

Or dans un corps, un polynôme de degré d n'a pas plus de d racines. Donc les racines de P sont exactement les éléments de H.

Or les éléments de G d'ordre d sont forcément racines de P.

Finalement

Les éléments de G d'ordre d sont les éléments de H d'ordre d ; donc il y en a $\varphi(d)$.

Pour conclure

On a montré que pour tout diviseur d de n, $f(d) = 0$, ou $f(d) = \varphi(d)$; on sait aussi que

$$\sum_{d|n} (\varphi(d) - f(d)) = 0$$

On en déduit que $f(d) = \varphi(d)$ pour tout d, en particulier pour $d = n$.

10 Le théorème chinois

10.1 Théorème

Si p et q sont premiers entre eux, les anneaux $\mathbb{Z}/pq\mathbb{Z}$ et $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$ sont isomorphes.

10.1.1 Démonstration

Soit

$$f : \to \mathbb{Z} \to \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$$

le morphisme d'anneaux canonique ; il ne peut pas être injectif ; on cherche son noyau :

$k \in \ker f$ si et seulement si k est un multiple commun à p et q ; donc

$$\ker f = pq\mathbb{Z}$$

Donc deux entiers k, k' ont la même image par f si et seulement si $k \equiv k' \,[pq]$; ou encore s'ils sont dans la même classe dans $\mathbb{Z}/pq\mathbb{Z}$.

On peut alors définir $\overline{f}$ qui à une classe $\alpha \in \mathbb{Z}/pq\mathbb{Z}$ associe $f(k)$, image de n'importe quel représentant k de α.

$$\overline{f} : \overline{k}_{pq} \to \left(\overline{k}_p, \overline{k}_q\right)$$

- $\overline{f}$ est un morphisme d'anneaux, car f en est un.
- $\overline{f}$ est injectif par construction.
- $\overline{f}$ est surjectif, pourquoi ?

Conclusion

$\overline{f}$ est un isomorphisme d'anneaux de $\mathbb{Z}/pq\mathbb{Z}$ sur $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$.

10.1.2 Exercice

Montrer directement que f et $\overline{f}$ sont surjectifs.

Démonstration

Soit $a, b \in \mathbb{Z}$; on cherche $m \in \mathbb{Z}$ tel que $f(m) = \left(\overline{a}, \overline{b}\right)$, c'est-à-dire $m \equiv a \,[p]$ et $m \equiv b \,[q]$.

Autrement dit, on cherche m, u, v tels que :

$$m = a + up = b + vq$$

Or, il existe u, v entiers tels que

$$b - a = up - vq$$

L'entier suivant convient :

$$m = a + up = b + vq$$

10.2 Application à φ

10.2.1 Lemme

Si $p \wedge q = 1$, $\varphi(p.q) = \varphi(p).\varphi(q)$.

Démonstration

Les anneaux $\mathbb{Z}/pq\mathbb{Z}$ et $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$ sont isomorphes, donc ont le même nombre d'inversibles.

10.2.2 Conclusion pour φ

Théorème

Pour tout $n \geq 2$,

$$\varphi(n) = n.\prod_p \left(1 - \frac{1}{p}\right)$$

où p décrit l'ensemble des diviseurs premiers de n.

10.3 Application aux congruences

Un exemple :

$$\begin{cases} x \equiv 6\,[25] \\ x \equiv 8\,[28] \end{cases}$$

25 et 28 étant premiers entre eux, il existe une solution unique modulo $25 \times 28 = 700$; comment la trouver ?

Méthode 1

On essaie 0, 1, 2, 3,...

Méthode 2

$x = 6 + 25p = 8 + 28q$; d'où

$$25p - 28q = 2$$

On pense à ?

$$28 = 25 + 3$$

$$25 = 3 \times 8 + 1$$

D'où

$$1 = 25 - (28 - 25) \times 8 = 25 \times 9 - 28 \times 8$$

D'où

$$p = 18, q = 16$$

Conclusion :

$$x = 456$$

11 Le RSA

Initiales de Rivest, Shamir, et Adleman.

Pour démarrer

On se donne deux nombres premiers distincts p et q ; on note $n = pq$.

On sait que

$$\varphi(n) = (p-1)(q-1)$$

11.1 Lemme

Soit u un élément de $\mathbb{N}^*$ tel que $u \equiv 1\,[\varphi(n)]$; alors :

$$\forall t \in \mathbb{Z}, t^u \equiv t\,[n]$$

Démonstration

Notons $u = 1 + k.\varphi(n)$.

Il suffit de montrer que p et q divisent $t\left(t^{u-1} - 1\right)$; si p ne divise pas t, alors $t \wedge p = 1$, et on sait que

$$t^{p-1} \equiv 1\,[p]$$

Plus généralement, $t^m \equiv 1\,[p]$ pour tout multiple m de $p-1$, en particulier pour $m = u - 1 = k.\varphi(n)$.

11.2 Remarque

Cas particulier : $u = d.e$ où d et e sont deux entiers naturels.

Que peut-on dire des deux applications $f : t \to t^d$ et $g : t \to t^e$ de $\mathbb{Z}/n\mathbb{Z}$ dans lui-même ?

11.3 Principe du RSA

Alice
- choisit deux nombres premiers distincts p et q.
- calcule $n = p.q$.
- choisit d tel que $d \wedge \varphi(n) = 1$.
- calcule e tel que $d.e \equiv 1\,[\varphi(n)]$.
- enfin publie (n, e) : la clé publique.

Bob
- choisit un message M.
- calcule $C = M^e\,[n]$.
- envoie C.

Alice retrouve M en calculant ... ?

Réponse

$M = C^d\,[n]$. Si tout va bien, Alice est seule à connaître d.

11.4 Algorithmes utiles

Pour trouver e ? Pour calculer M^e ou C^d ?

Réponses

Algorithme d'Euclide ; exponentiation rapide.

11.5 Construire de grands nombres premiers

Pour obtenir de très, très grands nombres premiers, les méthodes élémentaires sont insuffisantes. On utilise d'autres méthodes, en particulier des méthodes probabilistes, qui produisent des nombres très probablement premiers.

11.5.1 Méthode élémentaire

```
from math import sqrt
def premier(n):
    if n < 2:
        return False
    maxi = int(sqrt(n))
    k = 2
    while k <= maxi:
        if n % k == 0:
            return False
        k += 1
    return True
```

11.5.2 Le test de Fermat

Soit $p > 2$ premier ; on sait que si $a \wedge p = 1$:

$$a^{p-1} \equiv 1\,[p]$$

S'il existe a tel que $a \wedge p = 1$, et $a^{p-1} \neq 1\,[p]$, on sait que p n'est pas premier ; on dit que a est un témoin de Fermat pour p.

Problème

Il existe des entiers p, les nombres de Carmichael, qui ne sont pas premiers, mais pour lesquels, si $a \wedge p = 1$, alors $a^{p-1} \equiv 1\,[p]$: ils n'ont pas de témoin de Fermat.

Exemple : 561.

11.5.3 Le test de Miller-Rabin

Exercice

Soit $p > 2$ premier ; on écrit

$$p - 1 = 2^s.t$$

avec t impair et $s \geq 1$: $s = v_2(p-1)$; soit a premier avec p ; alors
- soit $a^t \equiv 1\,[p]$
- soit il existe j tel que $0 \leq j < s$ et $a^{2^j.t} \equiv -1\,[p]$

Démonstration

$K = \mathbb{Z}/p\mathbb{Z}$ étant un corps, le polynôme $X^2 - \overline{1} = \left(X - \overline{1}\right)\left(X + \overline{1}\right)$ n'a que deux racines, $\overline{1}$ et $\overline{-1}$.

Soit $b = \overline{a}^t$; on sait que $b^{2^s} = \overline{1}$; examinons la liste

$$b, b^2, b^4, ..., b^{2^s} = \overline{1}$$

Chacun est le carré du précédent.

Le premier de la liste qui vaut $\overline{1}$ est précédé de $\overline{-1}$, sauf si c'est b.

Utilisation

p étant donné, on essaie des valeurs de a au hasard ; si p n'est pas premier, on trouve assez vite une valeur de a qui ne vérifie pas le critère ; un tel entier a est appelé un témoin de Miller.

Tous les entiers composés ont beaucoup de témoins de Miller.

12 Anneau $K[X]$

Dans ce paragraphe et le suivant, K est un sous-corps de $\mathbb{C}$.

12.1 Inversibles

Théorème

L'ensemble des inversibles de l'anneau $K[X]$ est K^*.

Démonstration

Supposons $P.Q = 1$; que dire des degrés ?

12.2 Idéaux de $K[X]$

Théorème

Tout idéal I de $K[X]$ est principal.

Si $I \neq \{0\}$, il admet un unique générateur unitaire.

Démonstration

$$\{\deg P / \, P \in I \setminus \{0\}\}$$

possède un plus petit élément d ; soit $A \in I \setminus \{0\}$ de degré d ; on peut choisir A unitaire ; ensuite, soit P un élément quelconque de I.

$$P = AQ + R$$

avec $R = 0$ ou $\deg R < d$; or $R \in I$, donc $R = 0$.

Remarque

On dit qu'un anneau est principal s'il est intègre et tout idéal est principal.
Exemples :

$$\mathbb{Z}, K[X]$$

12.3 PGCD, PPCM de deux polynômes

12.3.1 Définition

Soit A et B deux éléments de $K[X]$.
Soit I la somme des deux idéaux (A) et (B) :

$$I = \{AP + BQ/P, Q \in K[X]\}$$

Soit D le générateur unitaire de I ; on pose $A \wedge B = D$
Remarque : si $A = B = 0$, on pose $D = 0$.
Retenons qu'il existe P et Q tels que

$$D = AP + BQ$$

(relation de Bézout).

12.3.2 Diviseurs communs

Les diviseurs communs à A et B sont les diviseurs de D.

12.3.3 Lemme de Gauss

Si $A \wedge B = 1$ et A divise BC, alors A divise C.

12.3.4 Définition

Soit P et Q deux éléments de $K[X]$; l'ensemble des multiples communs est

$$I = (P) \cap (Q)$$

C'est donc un idéal de $K[X]$; il existe un unique M unitaire tel que

$$I = M.K[X]$$

(sauf si P ou Q est nul).
Les multiples communs sont exactement les multiples de M ; on note

$$M = P \vee Q$$

12.4 Généralisation à plusieurs polynômes

La somme et l'intersection des idéaux étant associatives et commutatives, il en est de même de $\wedge$ et $\vee$; on peut donc facilement généraliser au PGCD ou PPCM de plusieurs polynômes.

13 Polynômes irréductibles

13.1 Définition

Dans un anneau intègre A, on dit qu'un élément x est irréductible si
1) $x \neq 0$.
2) x est non inversible.
3) si $x = yz$, alors y ou z est inversible.

13.2 Définition

Dans l'anneau $K[X]$, on dit qu'un élément P est irréductible si
1) P est non constant.
2) si $P = QR$, alors Q ou R est constant.

Remarque

Soit P et Q éléments de $K[X]$ unitaires ; que dire de $D = P \wedge Q$ si P est irréductible ?

Réponse

C'est P si P divise Q, 1 sinon.

A retenir

Si P est unitaire et irréductible, alors, pour tout polynôme Q :
- soit P divise Q
- soit P est premier avec Q

13.3 Décomposition

Théorème

Tout élément de $K[X]$ non constant est produit d'irréductibles.

Démonstration

Par récurrence sur le degré $n \geq 1$.

Si P n'est pas irréductible, $P = QR$, et l'hypothèse de récurrence s'applique à Q et à R.

Théorème

Cette décomposition est unique ; en quel sens ?

Démonstration

Par récurrence sur le degré d ; supposons

$$P_1...P_r = Q_1...Q_s$$

P_r divise $Q_1...Q_s$; d'après le lemme de Gauss, P_r divise l'un des Q_j ; on peut simplifier et appliquer l'hypothèse de récurrence.

13.4 Irréductibles dans $\mathbb{C}[X]$

Ce sont les polynômes de degré 1.

13.5 Irréductibles dans $\mathbb{R}[X]$

13.5.1 Théorème

Les irréductibles dans $\mathbb{R}[X]$ sont les polynômes de degré 1, et ceux de degré 2 sans racines réelles.

13.5.2 Exercice

$P = X^4 + 1$ est-il irréductible dans $\mathbb{R}[X]$?

Réponse

Evidemment non ; le factoriser.

Réponse

$$P = X^4+2X^2+1-2X^2 = \left(X^2+1\right)^2-2X^2 = \left(X^2-\sqrt{2}X+1\right)\left(X^2+\sqrt{2}X+1\right)$$

13.5.3 Vrai ou faux

Tout polynôme non constant sans racine est irréductible dans $K[X]$.

Réponse

C'est vrai pour les polynômes de degré 2 et 3.

14 Fractions rationnelles

14.1 Rappel

$K(X)$ est un corps.

14.2 Pôles simples

On suppose que a est un pôle simple de $R = \frac{P}{Q}$, avec $P \wedge Q = 1$:

$$R = \frac{P}{Q} = \frac{P}{(X-a)Q_1} = \frac{c}{X-a} + \frac{P_1}{Q_1}$$

Que vaut c ?

Réponse

$$c = \frac{P(a)}{Q_1(a)} = \frac{P(a)}{Q'(a)}$$

14.3 Exemple : $R = \frac{1}{X^n-1}$

$$R = \sum_{k=0}^{n-1} \frac{c_k}{X-a_k}$$

avec $a_k = \exp\left(\frac{2ik\pi}{n}\right)$ et c_k ?

Réponse

$$c_k = \frac{a_k}{n}$$

14.4 $\frac{P'}{P}$

Soit $P \in \mathbb{C}[X]$ non constant :

$$P = \prod_{k=1}^{n} (X - a_k)$$

Alors

$$\frac{P'}{P} = \sum_{j=1}^{n} \frac{1}{X-a_k}$$

15 Compléments : l'anneau $\mathbb{Z}[X]$

15.1 Non principal

Montrer que $\mathbb{Z}[X]$ n'est pas principal à l'aide de $I(2,X) = \{P \in \mathbb{Z}[X] / P(0) \in 2\mathbb{Z}\}$.

15.2 Racines rationnelles

Soit

$$r = \frac{p}{q}$$

une racine rationnelle d'un polynôme $P \in \mathbb{Z}[X]$, avec $p \in \mathbb{Z}$, $q \in \mathbb{N}^*$, et $p \wedge q = 1$.

Alors p divise le coefficient constant et q divise le coefficient dominant.

Démonstration

Partons de

$$a_0 + a_1.\frac{p}{q} + ...a_n.\frac{p^n}{q^n} = 0$$

On multiplie par q^n :

$$-a_0.q^n = a_1.p.q^{n-1} + ... + a_n.p^n$$

Donc p divise $a_0.q^n$.

Or $p \wedge q = 1$, donc $p \wedge q^n = 1$, donc, d'après le théorème de Gauss, p divise a_0.

Remarque

Si P est unitaire, les racines rationnelles sont entières.

15.3 Division euclidienne

Soit A et B éléments de $\mathbb{Z}[X]$, B non nul.

$$A = BQ + R$$

avec $\deg R < \deg B$: division euclidienne dans $\mathbb{Q}[X]$.

Condition suffisante pour que Q et R soient dans $\mathbb{Z}[X]$?

Réponse

B unitaire.

15.4 Les polynômes cyclotomiques

15.4.1 Définition

Soit P_n l'ensemble des racines primitives de l'unité : les générateurs de $\mathbb{U}_n$.

On pose

$$\phi_n = \prod_{\omega \in P_n} (X - \omega)$$

Quel est le degré de ϕ_n ?

15.4.2 Calcul des premiers

$$\phi_1 = X-1,\ \phi_2 = X+1,\ \phi_3 = X^2+X+1,\ \phi_4 = X^2+1,\ \phi_5 = X^4+X^3+X^2+X+1$$
$$\phi_6 = X^2 - X + 1,\ \phi_7 = X^6 + ... + 1,\ \phi_8 = X^4 + 1, ...$$

15.4.3 $X^n - 1 = \prod_{d|n} \phi_d$

Démonstration

Soit $n \geq 1$.

$$X^n - 1 = \prod_{\omega \in \mathbb{U}_n} (X - \omega)$$

Chaque élément de $\mathbb{U}_n$ a un ordre d diviseur de n.

On retrouve la formule

$$n = \sum_{d|n} \varphi(d)$$

15.4.4 $\phi_n \in \mathbb{Z}[X]$

Démonstration

Par récurrence sur n, en utilisant le précédent. ϕ_{105} est le premier à avoir un coefficient autre que $0, 1, -1$.

15.5 Le contenu

Soit $P \in \mathbb{Z}[X]$. On note $c(P)$ le PGCD des coefficients.

On dit que P est primitif si $c(P) = 1$.

Remarque

Soit $P \in \mathbb{Z}[X]$ et $n \in \mathbb{N}$. Alors

$$c(nP) = n.c(P)$$

15.5.1 Produit de primitifs

Soit $P, Q \in \mathbb{Z}[X]$ primitifs. Montrer que $P.Q$ est primitif.

Démonstration avec $\mathbb{Z}/p\mathbb{Z}$

Si PQ n'est pas primitif, il existe p premier qui divise tous les coefficients de PQ :

$$\overline{PQ} = 0$$

D'où $\overline{P}.\overline{Q} = 0$. Or, $\mathbb{Z}/p\mathbb{Z} = K$ est un corps, donc $K[X]$ est intègre.

Démonstration qui respecte scrupuleusement le programme

La même, mais sans que ça se voit.

15.5.2 $c(PQ)$

Soit $P, Q \in \mathbb{Z}[X]$; alors

$$c(PQ) = c(P).c(Q)$$

Démonstration

On écrit

$$P = c(P).P_1,\ Q = c(Q).Q_1$$

avec P_1 et Q_1 primitifs. D'où

$$P.Q = c(P).c(Q).P_1Q_1$$

et on sait que P_1Q_1 est primitif.

15.5.3 Factorisation dans $\mathbb{Z}[X]$ et $\mathbb{Q}[X]$

Soit $P \in \mathbb{Z}[X]$. On suppose que P est produit dans $\mathbb{Q}[X]$ de deux polynômes non constants.

Alors P est produit dans $\mathbb{Z}[X]$ de deux polynômes non constants.

Démonstration

Supposons $P = QR$ dans $\mathbb{Q}[X]$.

Alors dans $\mathbb{Z}[X]$

$$n.P = Q_1.R_1$$

et $n.c(P) = c(Q_1).c(R_1)$. D'où

$$P = c(P).\frac{Q_1}{c(Q_1)}.\frac{R_1}{c(R_1)}$$

15.5.4 Variante avec des polynômes unitaires

Soit P, Q, R trois éléments unitaires de $\mathbb{Q}[X]$. On suppose :
- $P = Q.R$
- P à coefficients dans $\mathbb{Z}$.

Alors Q et R sont aussi à coefficients dans $\mathbb{Z}$.

16 Compléments : les nombres algébriques

16.1 Définition

Soit $\alpha \in \mathbb{C}$; on dit que α est algébrique sur $\mathbb{Q}$ s'il existe un polynôme non nul $P \in \mathbb{Q}[X]$ tel que $P(\alpha) = 0$; premiers exemples ?

16.2 Un morphisme de $\mathbb{Q}$-algèbres

$$f : \begin{array}{c} \mathbb{Q}[X] \to \mathbb{C} \\ P \to P(\alpha) \end{array}$$

On note $\mathbb{Q}[\alpha]$ l'image de f ; que dire de la famille $(\alpha^n)_{n\geq 0}$?

C'est une famille génératrice de $\mathbb{Q}[\alpha]$.

16.2.1 si α n'est pas algébrique

f est donc injectif ; $\mathbb{Q}[\alpha]$ est isomorphe à $\mathbb{Q}[X]$; une base de $\mathbb{Q}[\alpha]$? On dit que α est transcendant.

16.2.2 si α est algébrique

$\ker f$ est donc un idéal de $\mathbb{Q}[X]$ non réduit à $\{0\}$

Il admet un unique générateur unitaire M_α, appelé polynôme minimal de α sur $\mathbb{Q}$.

16.2.3 Propriété

M_α est irréductible dans $\mathbb{Q}[X]$ et α est une racine simple.

C'est donc différent du cas du polynôme minimal d'un endomorphisme.

Démonstration

$M'_\alpha(\alpha)$ est non nul car M'_α n'est pas un multiple de M_α.

16.3 Exemples

Trouver le polynôme minimal de $\sqrt{2}$, i, j, $\sqrt[3]{2}$; plus compliqué : $\alpha = i + \sqrt{2}$.

Réponses

$$X^2 - 2$$

$$X^2 + 1$$

$$X^2 + X + 1$$

$$X^3 - 2$$

$$X^4 - 2X^2 + 9$$

16.4 L'algèbre $\mathbb{Q}[\alpha]$

On suppose que α est algébrique ; on note d le degré de M_α.

16.4.1 Une base

$\left(1, \alpha, ..., \alpha^{d-1}\right)$ est une base de $\mathbb{Q}[\alpha]$.

16.4.2 Corps $\mathbb{Q}[\alpha]$

Lemme

Toute K-algèbre E intègre de dimension finie sur K est un corps.

Démonstration

Soit $a \in E - \{0\}$.

Soit

$$f : x \to a.x$$

f est un endomorphisme injectif d'un K-espace vectoriel de dimension finie, donc f est bijectif.

Donc 1 possède un antécédent par f :

$$\exists b \in E, a.b = 1 = b.a$$

ce qui prouve que a est inversible dans E.

16.4.3 Réciproque partielle

Si K est un sous-corps de $\mathbb{C}$ de dimension finie sur $\mathbb{Q}$, tout élément de K est algébrique.

16.5 Corps $\mathbb{A}$ des algébriques

16.5.1 $\mathbb{A}$ est dénombrable

Démonstration

Soit $n \geq 0$; soit $\mathbb{A}_n$ l'ensemble des racines des éléments non nuls de $\mathbb{Z}_n[X]$.

$\mathbb{Z}_n[X]$ est dénombrable, donc $\mathbb{A}_n$ l'est ; $\mathbb{A}$ est donc une union dénombrable d'ensembles dénombrables...

16.5.2 Inverse

Si α est un algébrique non nul, $\frac{1}{\alpha}$ est algébrique.

Démonstration

Soit $a_0, ..., a_n$ des entiers non tous nuls tels que

$$a_0 + a_1\alpha + ...a_n\alpha^n = 0$$

Alors

$$\frac{a_0}{\alpha^n} + \frac{a_1}{\alpha^{n-1}} + ...a_n = 0$$

16.5.3 Un lemme

Soit L un corps de dimension n sur K ; soit E un L-espace vectoriel de dimension p ; alors E est un K-espace vectoriel de dimension np.

16.5.4 Somme et produit

La somme et le produit de deux algébriques sont algébriques.

Démonstration

Soit $K = \mathbb{Q}[\alpha]$; $\mathbb{Q} \subset K \subset K[\beta]$; on utilise ce qui précède...

16.5.5 Conclusion

L'ensemble $\mathbb{A}$ des algébriques est un sous-corps de $\mathbb{C}$.

16.5.6 $\mathbb{A}$ est algébriquement clos