Mathématiques discrètes

Michel Rigo

http://www.discmath.ulg.ac.be/

Année 2007–2008

UNIVERSITÉ de Liège

- "Algèbre" $\longrightarrow$ corps (champs) finis
  - Construction, propriétés,...
  - Applications : codes correcteurs, ...
- Cryptographie
  - Cryptographie "classique" à clé secrète
  - Cryptographie à clé publique, RSA
  - RSA et sa mise en oeuvre (nombres premiers,...)
  - Logarithme discret, ElGamal,...
- Suites linéaires récurrentes (sur un anneau quelconque)
  - Premières propriétés
  - Cas d'un champ fini
  - Séries formelles et fonctions génératrices
  - Problèmes de dénombrement (nombres de Catalan)

DÉFINITION : GROUPE $(G, \circ)$ OU $(G, \circ, e)$

Un groupe : ensemble G
opération interne et partout définie $\circ : G \times G \to G$ t.q.

- $\circ$ est associative : $\forall x, y, z \in G,\ x \circ (y \circ z) = (x \circ y) \circ z$
- élément (unique) $e \in G$ neutre t.q.

$$x \circ e = x = e \circ x,\ \forall x \in G,$$

- tout élément de G est inversible, i.e., $\forall x \in G$, $\exists y \in G$ (unique, noté x^{-1} ou $-x$) t.q. $x \circ y = y \circ x = e$

Si $\forall x, y \in G$, $x \circ y = y \circ x$, alors groupe commutatif ou abélien.

Définition

Si un ensemble jouit uniquement des deux premières propriétés, on dit alors qu'il s'agit d'un monoïde

Exemples

- L'ensemble $(\mathbb{Z}/m\mathbb{Z}, +)$, aussi noté $(\mathbb{Z}_m, +)$, des entiers modulo m muni de l'opération d'addition correspondante est un groupe.
- L'ensemble $(\mathbb{Q} \setminus \{0\}, \cdot)$ en est un aussi.
- L'ensemble $\mathrm{GL}_n(\mathbb{R})$ des matrices carrées inversibles de dimension n muni de la multiplication matricielle est un groupe non commutatif.
- Par contre, $(\mathbb{N}, +)$ est un monoïde qui n'est pas un groupe.

DÉFINITION

Soient $(G, \circ, e_G)$ et $(H, \diamond, e_H)$ deux groupes. Un homomorphisme de groupes est une application $f : G \to H$ telle que

$$\forall x, y \in G : f(x \circ y) = f(x) \diamond f(y).$$

PROPRIÉTÉS

$f(e_G) = e_H$ et $f(x^{-1}) = f(x)^{-1}$ pour tout $x \in G$.

Pour tout $x \in G$, on a $f(x) = f(x \circ e_G) = f(x) \diamond f(e_G)$.
Multiplier à gauche par $f(x)^{-1}$:
$f(x)^{-1} \diamond f(x) = f(x)^{-1} \diamond f(x) \diamond f(e_G)$ donc $e_H = f(e_G)$

pour tout $x \in G$, $f(e_G) = f(x \circ x^{-1}) = f(x) \diamond f(x^{-1}) = e_H$.

DÉFINITION

Soient $(G, \circ, e_G)$ et $(H, \diamond, e_H)$ deux monoïdes. Un homomorphisme de monoïdes est une application $f : G \to H$ telle que

$$\forall x, y \in G : f(x \circ y) = f(x) \diamond f(y) \quad \textbf{et} \quad f(e_G) = e_H.$$

DÉFINITION : ANNEAU $(A,+,\cdot,0,1)$ OU $(A,+,\cdot)$

Un anneau : ensemble A muni de deux opérations internes et partout définies, $+$ et $\cdot$ de neutre respectif 0 et 1

- $(A,+,0)$ est un groupe commutatif,
- $\cdot$ est associatif, i.e., $\forall x,y,z \in A$, $(x.y).z = x.(y.z)$,
- 1 neutre pour $\cdot$, i.e., $\forall x \in A$, $1.x = x.1 = x$,
- $\cdot$ est distributif par rapport à $+$,

$$\forall x,y,z \in A,\; (x+y).z = x.z + y.z \text{ et } x.(y+z) = x.y + x.z.$$

Un anneau est commutatif si $\cdot$ est commutative.

EXEMPLES

- L'ensemble $(\mathbb{Z}_m, +, \cdot)$ possède une structure d'anneau commutatif.
- L'ensemble $\mathbb{R}_n^n$ des matrices carrées de dimension n à coefficients réels muni des opérations usuelles d'addition et de multiplication possède une structure d'anneau (non commutatif).
- Soit $\mathbb{K}$ un champ, l'ensemble $\mathbb{K}[X]$ des polynômes à coefficients dans $\mathbb{K}$ est un anneau commutatif.

EXEMPLE

Si $(A, +, \cdot)$ est un anneau, alors $(A, \cdot, 1)$ possède en particulier une structure de monoïde.

DÉFINITION

Un anneau pour lequel $0 \neq 1$ et tout élément non nul possède un inverse pour $\cdot$, i.e., pour tout $x \in A \setminus \{0\}$, il existe $y \in A$ tel que $x.y = 1 = y.x$, est qualifié de corps. Si de plus, l'anneau est commutatif, on parle alors de champ

EXEMPLES

- L'ensemble $\mathbb{Z}_p$ est un champ si et seulement si p est un nombre premier. On le note parfois $\mathbb{F}_p$.
- Le sous-ensemble $\mathrm{GL}_n(\mathbb{R})$ des matrices inversibles de $\mathbb{R}_n^n$ est un corps.

DÉFINITION

Soient $(A, +_A, \cdot_A, 0_A, 1_A)$ et $(B, +_B, \cdot_B, 0_B, 1_B)$ deux anneaux. Un homomorphisme d'anneaux est une application $f : A \to B$ t.q.

- f homomorphisme de groupes entre $(A, +_A, 0_A)$ et $(B, +_B, 0_B)$
- f homomorphisme de monoïdes entre $(A, \cdot_A, 1_A)$ et $(B, \cdot_B, 1_B)$.

Autrement dit, on a

$$\forall x, y \in A,\ f(x+y) = f(x) + f(y),\ f(x.y) = f(x).f(y)$$

et $f(1_A) = 1_B$.

DÉFINITION

Soit $\mathbb{K}$ un champ (ou simplement un corps). Un espace vectoriel E sur $\mathbb{K}$ ou $\mathbb{K}$-vectoriel est un ensemble E muni d'une addition interne $+ : E \times E \to E$ et d'une multiplication interne $\cdot : \mathbb{K} \times E \to E$ tel que

- $(E, +)$ est un groupe commutatif

et pour tous $x, y \in E$ et tous $\lambda, \mu \in \mathbb{K}$

- $\lambda \cdot (\mu \cdot x) = (\lambda\mu) \cdot x$,
- $1 \cdot x = x$,
- $(\lambda + \mu) \cdot x = \lambda \cdot x + \mu \cdot x$,
- $\lambda \cdot (x + y) = \lambda \cdot x + \lambda \cdot y$.

Si $\mathbb{K}$ n'est pas un champ, mais simplement un anneau, on parle alors de $\mathbb{K}$-module.

SUITE...

Un espace vectoriel est de dimension finie s'il contient une partie génératrice finie.

Sa dimension est alors le nombre d'éléments d'une de ses bases.

REMARQUE

Un A-module ne possède pas toujours de base.

Extension de champ

Soient $\mathbb{K}, \mathbb{L}$ deux champs tels que $\mathbb{K}$ soit un sous-champ de $\mathbb{L}$.

$\mathbb{L}$ est une extension de champ de $\mathbb{K}$.

$\mathbb{L}$ est un $\mathbb{K}$-vectoriel.

Si la dimension de $\mathbb{L}$ comme $\mathbb{K}$-vectoriel est finie et égale à d, on parle d'extension finie et d = degré de l'extension, $[\mathbb{L} : \mathbb{K}]$

Plus généralement, si $\mathbb{K}$ et $\mathbb{L}$ sont deux champs et s'il existe un plongement $h : \mathbb{K} \to \mathbb{L}$ (i.e., un homomorphisme injectif), alors on dit que $\mathbb{L}$ est une extension de $\mathbb{K}$ car $\mathbb{K}$ est isomorphe à un sous-champ de $\mathbb{L}$.

Remarque

Si $\mathbb{K}$ est un champ fini contenant t éléments et si $\mathbb{L}$ est une extension de $\mathbb{K}$ de degré fini d, alors $\mathbb{L}$ contient t^d éléments.

Il existe une base $(\ell_1, \ldots, \ell_d)$ de $\mathbb{L}$

tout élément de $\mathbb{L}$ se décompose de manière unique comme

$$k_1\ell_1 + \cdots + k_d\ell_d$$

avec les $k_i \in \mathbb{K}$.

EXEMPLE - EXTENSION DE CHAMP

$\mathbb{Q}(\sqrt{2})$ = {expr. rationnelles avec $\sqrt{2}$ et des éléments de $\mathbb{Q}$ }
plus petit champ contenant $\mathbb{Q}$ et $\sqrt{2}$

$$\frac{\sum_{i=0}^{m} q_i\,(\sqrt{2})^i}{\sum_{j=0}^{n} r_j\,(\sqrt{2})^j}, \quad q_i, r_j \in \mathbb{Q}, m, n \in \mathbb{N}.$$

$$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$$

$(1, \sqrt{2})$ base de $\mathbb{Q}(\sqrt{2})$ vu comme $\mathbb{Q}$-vectoriel, $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$.

Par des raisonnements analogues,

$$\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \mid a, b, c, d \in \mathbb{Q}\}$$

et $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$.

DÉFINITION

Un idéal (bilatère) d'un anneau $(A, +, \cdot)$ est un sous-ensemble $I \subset A$ tel que

- $(I, +, 0)$ est un groupe commutatif,
- pour tous $i \in I$ et $a \in A$, $a.i$ et $i.a$ appartiennent à I.

DÉFINITION

Soient $a_1, \ldots, a_k$ des éléments de A. Dans le cas où A est un anneau commutatif, l'idéal engendré par $a_1, \ldots, a_k$ est

$$\langle a_1, \ldots, a_k \rangle = \left\{ \sum_{i=1}^{k} b_i a_i \mid b_i \in A \right\}.$$

DÉFINITION

Un idéal engendré par un unique élément $a \in A$, i.e.,

$$I = \langle a \rangle$$

est qualifié de principal.

Un anneau principal est un anneau intègre dans lequel tout idéal est principal.

DÉFINITION

Un idéal I d'un anneau A est maximal si I est propre, i.e., $I \neq A$, et s'il n'est contenu strictement dans aucun idéal propre, i.e., si J est un idéal tel que $I \subsetneq J$, alors $J = A$.

EXEMPLE

Si $\mathbb{K}$ est un champ, les seuls idéaux de $\mathbb{K}$ sont $\{0\}$ et $\mathbb{K}$.

si $a \neq 0$ appartient à un idéal $I \neq \{0\}$, alors $a^{-1}.a = 1 \in I$ et de là, tout élément de $\mathbb{K}$ appartient à I.

EXEMPLE

Les idéaux de $\mathbb{Z}$ sont les $m\mathbb{Z} = \langle m \rangle$ et $\mathbb{Z}$ est donc un anneau principal.

DÉFINITION - QUOTIENT D'UN ANNEAU PAR UN IDÉAL

$(A, +, \cdot, 0, 1)$ anneau et I idéal de A.

I est un sous-groupe du groupe commutatif $(A, +, 0)$, on peut considérer le groupe quotient A/I

les éléments de A/I sont les classes de la forme

$$a + I = \{a + i \mid i \in I\}, \quad a \in A.$$

La somme de deux classes $a + I$ et $b + I$ est la classe

$$(a + b) + I$$

Le neutre : la classe

$$0 + I = I$$

Définition - Quotient d'un anneau par un idéal

On munit A/I d'une structure d'anneau :

le produit des classes $a + I$ et $b + I$ est la classe

$$(a.b) + I$$

le neutre est

$$1 + I$$

La projection canonique $\pi : A \to A/I : a \mapsto a + I$ est alors un homomorphisme d'anneaux.

Exemple

L'anneau quotient de $\mathbb{Z}$ par l'idéal $m\mathbb{Z}$ est l'anneau $\mathbb{Z}_m$.
Une classe est un élément de la forme $a + \langle m \rangle$.

Pour $m = 3$, on a par exemple,

$$(1 + \langle 3 \rangle) + (2 + \langle 3 \rangle) = 3 + \langle 3 \rangle = 0 + \langle 3 \rangle$$

et

$$(2 + \langle 3 \rangle).(2 + \langle 3 \rangle) = 4 + \langle 3 \rangle = 1 + \langle 3 \rangle.$$

Dans $\mathbb{Z}_m$,

$$\forall a, b \in \mathbb{Z} : \; a + \langle m \rangle = b + \langle m \rangle \Leftrightarrow a \equiv b \pmod{m}.$$

REMARQUE

Un élément $a + I$ de A/I est nul (i.e., correspond au neutre pour l'addition dans l'anneau quotient) SSI $a \in I$.

$$a + I = \{a + i \mid i \in I\} = I \Leftrightarrow a \in I$$

THÉORÈME

Soient A un anneau commutatif et I un idéal de A.

L'anneau quotient A/I est un champ si et seulement si I est un idéal maximal.

Idéaux et divisibilité

Soient A un anneau principal (muni d'une division euclidienne) et $a, b \in A \setminus \{0\}$. On a

- $\langle a \rangle \supset \langle b \rangle$ SSI a divise b.
- $\langle a \rangle = \langle b \rangle$ SSI $a = ub$ avec u inversible dans A.

Rappel

Si $a = ub$ avec u inversible, a et b associés

$\mathbb{K}$ est un champ.

Définition

Un polynôme à coeff. dans $\mathbb{K}$ est une suite $(\alpha_n)_{n\in\mathbb{N}}$ d'éléments de $\mathbb{K}$ non tous nuls t.q. $\exists d \geq 0$ t.q. $\alpha_n = 0$ pour tout $n > d$.

$$P = \sum_{i=0}^{d} \alpha_i X^i = \alpha_d X^d + \cdots + \alpha_1 X + \alpha_0, \quad \alpha_d \neq 0$$

d : degré, $\deg P$.

La valeur $P(\beta)$ de ce polynôme évalué en $\beta \in \mathbb{K}$ est

$$P(\beta) = \sum_{i=0}^{d} \alpha_i \beta^i = \alpha_d \beta^d + \cdots + \alpha_1 \beta + \alpha_0.$$

Terminologie

La suite nulle est appelé polynôme nul.

Si $\alpha_d = 1$, polynôme monique (ou unitaire).

Si $d = 0$, le polynôme est constant.

Structure algébrique

L'ensemble $\mathbb{K}[X]$ des polynômes à coefficients dans $\mathbb{K}$ possède alors une structure d'anneau.

Polynôme $\neq$ fonction polynomiale

sur $\mathbb{Z}_3[X]$, $P(X) = X^2 + 1$ et $Q(X) = X^3 + X^2 - X + 1$ sont distincts mais représentent la même fonction : $\forall z \in \mathbb{Z}_3$, $P(z) = Q(z)$

Il est aisé de munir $\mathbb{K}[X]$ de la divison euclidienne (calcul écrit comme dans $\mathbb{C}[z]$)

THÉORÈME

Soit $\mathbb{K}$ un champ. Si $D \in \mathbb{K}[X]$ est non nul, alors pour tout $P \in \mathbb{K}[X]$, il existe des polynômes uniques Q et R tels que

$$P = Q.D + R, \quad \text{avec } \deg R < \deg D.$$

REMAQUE

Si $\mathbb{K}$ n'est pas un champ mais simplement un anneau, pour assurer l'existence des polynômes Q et R, il faut que le coefficient principal de D soit inversible.

l'unicité de Q et R n'est assurée que si l'anneau est intègre.

Si $P = Q.R$, alors le polynôme Q divise le polynôme P.

Propriété

Puisque $\mathbb{K}$ est un champ

$$\deg P.Q = \deg P + \deg Q$$

donc $\mathbb{K}[X]$ est un anneau intègre.
$P.Q = 0$ entraîne $P = 0$ ou $Q = 0$.

Remarque

Si $\mathbb{K}$ est simplement un anneau, dans $\mathbb{Z}_4[X]$,

$$(2X^2 + 1).(2X + 1) = 2X^2 + 2X + 1$$

$\mathbb{Z}_4[X]$ n'est pas intègre.

DÉFINITION

Un polynôme non constant P est irréductible si $P = Q.R$ entraîne que Q ou R est constant.

P ne peut pas s'écrire comme le produit de deux polynômes de degré strictement inférieur au degré de P.

En particulier, tout polynôme de degré 1 est irréductible.

EXEMPLE

Le polynôme $X^2 + 1$ est irréductible sur $\mathbb{R}[X]$ mais pas sur $\mathbb{C}[X]$

Remarques

Dans $\mathbb{K}[X]$, les seuls éléments inversibles sont les polynômes constants $k \in \mathbb{K} \setminus \{0\}$.

Si P est de deg≥ 1, alors pour tout $Q \in \mathbb{K}[X]$, $\deg P.Q \geq 1$ et P n'est pas inversible.

$\langle P \rangle = \mathbb{K}[X]$ SSI $P \neq 0$ est constant.

Une conséquence de la division euclidienne. . .

THÉORÈME

Soit $\mathbb{K}$ un champ. L'anneau $\mathbb{K}[X]$ des polynômes à coefficients dans $\mathbb{K}$ est principal.

COROLLAIRE

Soient $\mathbb{K}$ un champ et $P \in \mathbb{K}[X]$.

L'idéal $\langle P \rangle$ est un idéal maximal SSI P est irréductible.

Démonstration ...

Nous pouvons construire des champs finis...

Ingrédient 1

THÉORÈME

Soient A un anneau commutatif et I un idéal de A.
L'anneau quotient A/I est un champ SSI I est un idéal maximal.

Ingrédient 2

COROLLAIRE

Soient $\mathbb{K}$ un champ et $P \in \mathbb{K}[X]$.
L'idéal $\langle P \rangle$ est un idéal maximal SSI P est irréductible.

PROPOSITION

Soit $\mathbb{K}$ un champ. L'anneau quotient $\mathbb{K}[X]/\langle P \rangle$ est un champ SSI P est un polynôme irréductible.

EXEMPLE

$\mathbb{Z}_3[X]$ quotienté par l'idéal $\langle X^2+1\rangle$.

X^2+1 irréductible sur $\mathbb{Z}_3[X]$?

$$1,\ 2,\ X,\ X+1,\ X+2,\ 2X,\ 2x+1,\ 2X+2$$

Les classes de l'anneau quotient sont de la forme

$$P+\langle X^2+1\rangle, \quad \deg P<2$$

car pour tous $P, Q \in \mathbb{K}[X]$, $P+\langle X^2+1\rangle = Q+\langle X^2+1\rangle$
SSI P et Q ont même reste après division par X^2+1.

Notons $P+\langle X^2+1\rangle$ simplement P.

EXEMPLE

$\mathbb{Z}_3[X]$ quotienté par l'idéal $\langle X^2+1\rangle$.

X^2+1 irréductible sur $\mathbb{Z}_3[X]$?

$$1,\ 2,\ X,\ X+1,\ X+2,\ 2X,\ 2x+1,\ 2X+2$$

Les classes de l'anneau quotient sont de la forme

$$P+\langle X^2+1\rangle,\quad \deg P<2$$

car pour tous $P,Q\in\mathbb{K}[X]$, $P+\langle X^2+1\rangle=Q+\langle X^2+1\rangle$ SSI P et Q ont même reste après division par X^2+1.

Notons $P+\langle X^2+1\rangle$ simplement P.

Exemple

$\mathbb{Z}_3[X]$ quotienté par l'idéal $\langle X^2 + 1 \rangle$.

$X^2 + 1$ irréductible sur $\mathbb{Z}_3[X]$?

$$1,\ 2,\ X,\ X+1,\ X+2,\ 2X,\ 2x+1,\ 2X+2$$

Les classes de l'anneau quotient sont de la forme

$$P + \langle X^2 + 1 \rangle, \quad \deg P < 2$$

car pour tous $P, Q \in \mathbb{K}[X]$, $P + \langle X^2 + 1 \rangle = Q + \langle X^2 + 1 \rangle$
SSI P et Q ont même reste après division par $X^2 + 1$.

Notons $P + \langle X^2 + 1 \rangle$ simplement P.

Table de multiplication (sans 0) — version 1

$\cdot$	1	2	X	$X+1$	$X+2$	$2X$	$2X+1$	$2X+2$
1	1	2	X	$X+1$	$X+2$	$2X$	$2X+1$	$2X+2$
2	2	1	$2X$	$2X+2$	$2X+1$	X	$X+2$	$X+1$
X	X	$2X$	2	$X+2$	$2X+2$	1	$X+1$	$2X+1$
$X+1$	$X+1$	$2X+2$	$X+2$	$2X$	1	$2X+1$	2	X
$X+2$	$X+2$	$2X+1$	$2X+2$	1	X	$X+1$	$2X$	1
$2X$	$2X$	X	1	$2X+1$	$X+1$	2	$2X+2$	$X+2$
$2X+1$	$2X+1$	$X+2$	$X+1$	2	$2X$	$2X+2$	X	1
$2X+2$	$2X+2$	$X+1$	$2X+1$	X	2	$X+2$	1	$2X$

Table de multiplication (sans 0)

version 2 (liste des coefficients)

$\cdot$	$(0,1)$	$(0,2)$	$(1,0)$	$(1,1)$	$(1,2)$	$(2,0)$	$(2,1)$	$(2,2)$
$(0,1)$	$(0,1)$	$(0,2)$	$(1,0)$	$(1,1)$	$(1,2)$	$(2,0)$	$(2,1)$	$(2,2)$
$(0,2)$	$(0,2)$	$(0,1)$	$(2,0)$	$(2,2)$	$(2,1)$	$(1,0)$	$(1,2)$	$(1,1)$
$(1,0)$	$(1,0)$	$(2,0)$	$(0,2)$	$(1,2)$	$(2,2)$	$(0,1)$	$(1,1)$	$(2,1)$
$(1,1)$	$(1,1)$	$(2,2)$	$(1,2)$	$(2,0)$	$(0,1)$	$(2,1)$	$(0,2)$	$(1,0)$
$(1,2)$	$(1,2)$	$(2,1)$	$(2,2)$	$(0,1)$	$(1,0)$	$(1,1)$	$(2,0)$	$(0,1)$
$(2,0)$	$(2,0)$	$(1,0)$	$(0,1)$	$(2,1)$	$(1,1)$	$(0,2)$	$(2,2)$	$(1,2)$
$(2,1)$	$(2,1)$	$(1,2)$	$(1,1)$	$(0,2)$	$(2,0)$	$(2,2)$	$(1,0)$	$(0,1)$
$(2,2)$	$(2,2)$	$(1,1)$	$(2,1)$	$(1,0)$	$(0,2)$	$(1,2)$	$(0,1)$	$(2,0)$

Version 3 : En base 3...
$(x_{f-1}, \ldots, x_0) \in (\mathbb{Z}_p)^f$ correspond à l'entier

$$\sum_{i=0}^{f-1} x_i\, p^i .$$

$\cdot$	1	2	3	4	5	6	7	8
1	1	2	3	4	5	6	7	8
2	2	1	6	8	7	3	5	4
3	3	6	2	5	8	1	4	7
4	4	8	5	6	1	7	2	3
5	5	7	8	1	3	4	6	1
6	6	3	1	7	4	2	8	5
7	7	5	4	2	6	8	3	1
8	8	4	7	3	2	5	1	6

"Mathematica crash course"

```
In[71]:= Table[i, {i, 1, 4}]

Out[71]= {1, 2, 3, 4}

In[72]:= Table[i + j^2, {i, 1, 3}, {j, 1, 2}]

Out[72]= {{2, 5}, {3, 6}, {4, 7}}

In[73]:= CoefficientList[X^3 + 2 X - 1, X]

Out[73]= {-1, 2, 0, 1}

In[74]:= Reverse[CoefficientList[X^3 + 2 X - 1, X]]

Out[74]= {1, 0, 2, -1}

In[86]:= PadLeft[{1, 2, 3}, 5]

Out[86]= {0, 0, 1, 2, 3}

In[87]:= IntegerDigits[1324, 3]

Out[87]= {1, 2, 1, 1, 0, 0, 1}

In[88]:= FromDigits[{1, 2, 1, 1, 0, 0, 1}, 3]

Out[88]= 1324

In[90]:= {1, 2, 1, 1, 0, 0, 1}.Reverse[Table[3^i, {i, 0, 6}]]

Out[90]= 1324
```

"Mathematica crash course"

```
In[81]:= PolynomialMod[4 X^3 + X - 1, X^2 - 1]

Out[81]= -1 + 5 X

In[82]:= PolynomialQuotient[4 X^3 + X - 1, X^2 - 1, X]

Out[82]= 4 X

In[83]:= Expand[4 X (X^2 - 1) + (-1 + 2 X)]
```

Out[83]= $-1-2X+4X^3$

```
In[84]:= PolynomialMod[4 X^3 + X - 1, X^2 - 1, Modulus → 3]

Out[84]= 2 + 2 X

In[85]:= PolynomialMod[4 X^3 + X - 1, X^2 - 1, Modulus → 2]

Out[85]= 1 + X
```

Avec Mathematica

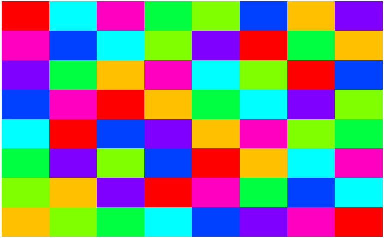
```
In[1]:=  t = {1, 2, X, X + 1, X + 2, 2 X, 2 X + 1, 2 X + 2}

Out[1]=  {1, 2, X, 1 + X, 2 + X, 2 X, 1 + 2 X, 2 + 2 X}

In[29]:=  tab = Table[
             PolynomialMod[t[[i]] t[[j]], X^2 + 1, Modulus → 3],
             {i, 1, 8}, {j, 1, 8}]

Out[29]=  {{1, 2, X, 1 + X, 2 + X, 2 X, 1 + 2 X, 2 + 2 X}, {2, 1, 2 X, 2 + 2 X, 1 + 2 X, X, 2 + X, 1 + X},
           {X, 2 X, 2, 2 + X, 2 + 2 X, 1, 1 + X, 1 + 2 X}, {1 + X, 2 + 2 X, 2 + X, 2 X, 1, 1 + 2 X, 2, X},
           {2 + X, 1 + 2 X, 2 + 2 X, 1, X, 1 + X, 2 X, 2}, {2 X, X, 1, 1 + 2 X, 1 + X, 2, 2 + 2 X, 2 + X},
           {1 + 2 X, 2 + X, 1 + X, 2, 2 X, 2 + 2 X, X, 1}, {2 + 2 X, 1 + X, 1 + 2 X, X, 2, 2 + X, 1, 2 X}}
```

Avec Mathematica

```
In[28]:= Table[
          PadLeft[
           Reverse[CoefficientList[
             PolynomialMod[t[[i]] t[[j]], X^2 + 1, Modulus → 3]
             , X]]
           , 2],
          {i, 1, 8}, {j, 1, 8}]

Out[28]= {{{0, 1}, {0, 2}, {1, 0}, {1, 1}, {1, 2}, {2, 0}, {2, 1}, {2, 2}},
          {{0, 2}, {0, 1}, {2, 0}, {2, 2}, {2, 1}, {1, 0}, {1, 2}, {1, 1}},
          {{1, 0}, {2, 0}, {0, 2}, {1, 2}, {2, 2}, {0, 1}, {1, 1}, {2, 1}},
          {{1, 1}, {2, 2}, {1, 2}, {2, 0}, {0, 1}, {2, 1}, {0, 2}, {1, 0}},
          {{1, 2}, {2, 1}, {2, 2}, {0, 1}, {1, 0}, {1, 1}, {2, 0}, {0, 2}},
          {{2, 0}, {1, 0}, {0, 1}, {2, 1}, {1, 1}, {0, 2}, {2, 2}, {1, 2}},
          {{2, 1}, {1, 2}, {1, 1}, {0, 2}, {2, 0}, {2, 2}, {1, 0}, {0, 1}},
          {{2, 2}, {1, 1}, {2, 1}, {1, 0}, {0, 2}, {1, 2}, {0, 1}, {2, 0}}}

In[30]:= Table[
          FromDigits[
           Reverse[CoefficientList[PolynomialMod[t[[i]] t[[j]], X^2 + 1, Modulus → 3], X]]
           , 3],
          {i, 1, 8}, {j, 1, 8}]

Out[30]= {{1, 2, 3, 4, 5, 6, 7, 8}, {2, 1, 6, 8, 7, 3, 5, 4},
          {3, 6, 2, 5, 8, 1, 4, 7}, {4, 8, 5, 6, 1, 7, 2, 3}, {5, 7, 8, 1, 3, 4, 6, 2},
          {6, 3, 1, 7, 4, 2, 8, 5}, {7, 5, 4, 2, 6, 8, 3, 1}, {8, 4, 7, 3, 2, 5, 1, 6}}
```

Avec Mathematica

```
In[31]:= m = Table[Hue[
             FromDigits[Reverse[
                CoefficientList[PolynomialMod[t[[i]] t[[j]], X^2 + 1, Modulus → 3], X]], 3]
               / 8],
            {i, 1, 8}, {j, 1, 8}];

In[32]:= Show[Graphics[RasterArray[m]]]
```



```
Out[32]= - Graphics -
```

“Mathematica crash course”

```
In[16]:= Table[IntegerDigits[n, 2], {n, 1, 10}]

Out[16]= {{1}, {1, 0}, {1, 1}, {1, 0, 0}, {1, 0, 1},
          {1, 1, 0}, {1, 1, 1}, {1, 0, 0, 0}, {1, 0, 0, 1}, {1, 0, 1, 0}}

In[17]:= TableForm[%]

Out[17]//TableForm=
      1
      1    0
      1    1
      1    0    0
      1    0    1
      1    1    0
      1    1    1
      1    0    0    0
      1    0    0    1
      1    0    1    0

In[18]:= Table[PadLeft[IntegerDigits[n, 2], 5], {n, 1, 10}]

Out[18]= {{0, 0, 0, 0, 1}, {0, 0, 0, 1, 0}, {0, 0, 0, 1, 1}, {0, 0, 1, 0, 0}, {0, 0, 1, 0, 1},
          {0, 0, 1, 1, 0}, {0, 0, 1, 1, 1}, {0, 1, 0, 0, 0}, {0, 1, 0, 0, 1}, {0, 1, 0, 1, 0}}

In[19]:= Table[PadLeft[IntegerDigits[n, 2], 5].{X^4, X^3, X^2, X, 1}, {n, 1, 10}]
```

Out[19]= $\{1, X, 1+X, X^2, 1+X^2, X+X^2, 1+X+X^2, X^3, 1+X^3, X+X^3\}$

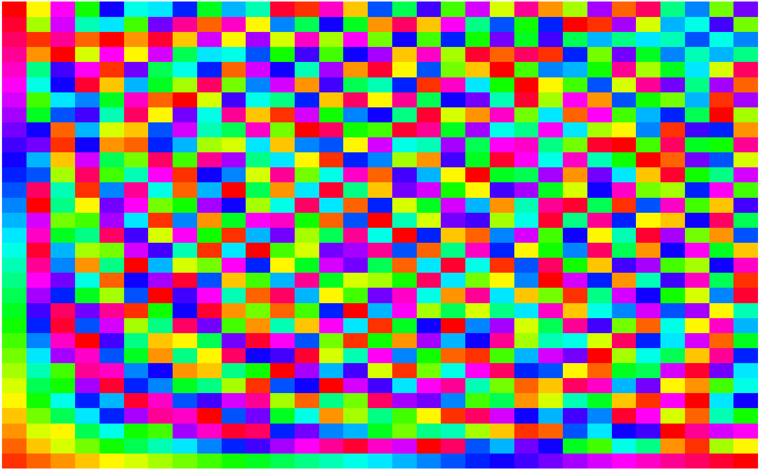
UN AUTRE EXEMPLE

$1 + X + X^3 + X^4 + X^5$ irréductible sur $\mathbb{Z}_2[X]$

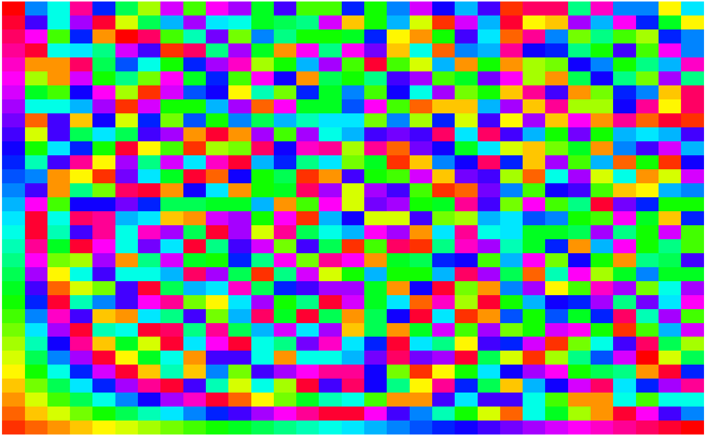
$$\mathbb{Z}_2[X]/\langle 1 + X + X^3 + X^4 + X^5 \rangle$$

```
In[64]:= t = Table[PadLeft[IntegerDigits[n, 2], 5].{X^4, X^3, X^2, X, 1}, {n, 1, 31}]

Out[64]= {1, X, 1 + X, X^2, 1 + X^2, X + X^2, 1 + X + X^2, X^3, 1 + X^3, X + X^3, 1 + X + X^3,
  X^2 + X^3, 1 + X^2 + X^3, X + X^2 + X^3, 1 + X + X^2 + X^3, X^4, 1 + X^4, X + X^4, 1 + X + X^4,
  X^2 + X^4, 1 + X^2 + X^4, X + X^2 + X^4, 1 + X + X^2 + X^4, X^3 + X^4, 1 + X^3 + X^4, X + X^3 + X^4,
  1 + X + X^3 + X^4, X^2 + X^3 + X^4, 1 + X^2 + X^3 + X^4, X + X^2 + X^3 + X^4, 1 + X + X^2 + X^3 + X^4}

In[65]:= tab = Table[
   PolynomialMod[t[[i]] t[[j]], 1 + X + X^3 + X^4 + X^5, Modulus → 2],
   {i, 1, 31}, {j, 1, 31}]
```

Rappels - mise à niveau en algèbre

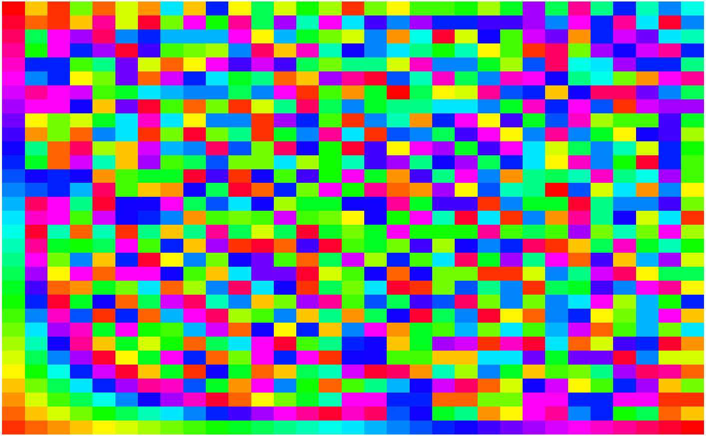


Isomorphisme avec $\mathbb{Z}_2[X]/\langle 1 + X + X^2 + X^3 + X^5 \rangle$?



Patience... (Structure des corps finis)

ou encore isomorphisme avec $\mathbb{Z}_2[X]/\langle 1+X^2+X^3+X^4+X^5 \rangle$?

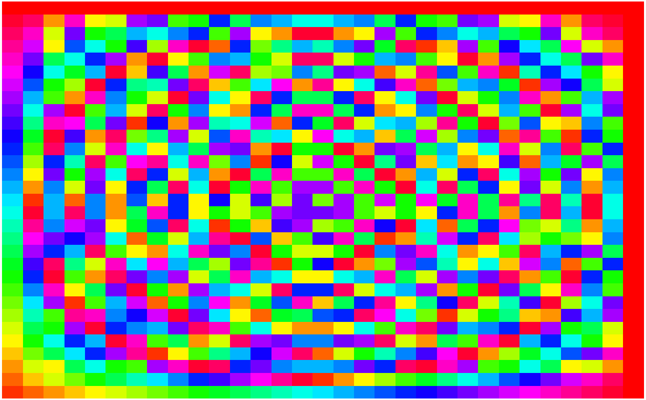


Rappels - mise à niveau en algèbre

Et si on considère un polynôme réductible ?

Exemple

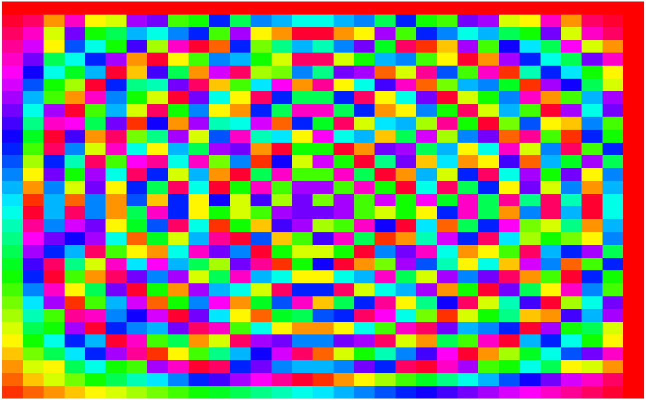
Dans $\mathbb{Z}_2[X]$, $\quad X^5 + 1 = (X^4 + X^3 + X^2 + X + 1)(X + 1)$



Et si on considère un polynôme réductible ?

EXEMPLE

Dans $\mathbb{Z}_2[X]$, $\quad X^5 + 1 = (X^4 + X^3 + X^2 + X + 1)(X + 1)$



RAPPELS - MISE À NIVEAU EN ALGÈBRE

Dans la table de multiplication d'un corps

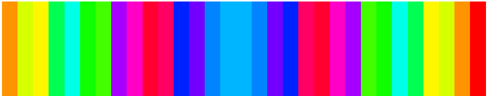
sur chaque ligne/colonne, permutation des éléments

$$x.y = x.z \Rightarrow y = z$$

```
In[79]:= Table[
          FromDigits[
           Reverse[CoefficientList[PolynomialMod[t[[i]] t[[j]], X^5 + 1, Modulus → 2], X]]
           , 2],
          {i, 3, 3}, {j, 1, 31}]

Out[79]= {{3, 6, 5, 12, 15, 10, 9, 24, 27, 30, 29, 20, 23,
          18, 17, 17, 18, 23, 20, 29, 30, 27, 24, 9, 10, 15, 12, 5, 6, 3, 0}}

In[80]:= m = Map[Hue[# / 31] &, %, {2}]
```

Out[80]= $\{\{\mathrm{Hue}[\frac{3}{31}], \mathrm{Hue}[\frac{6}{31}], \mathrm{Hue}[\frac{5}{31}], \mathrm{Hue}[\frac{12}{31}], \mathrm{Hue}[\frac{15}{31}], \mathrm{Hue}[\frac{10}{31}], \mathrm{Hue}[\frac{9}{31}], \mathrm{Hue}[\frac{24}{31}],$
$\mathrm{Hue}[\frac{27}{31}], \mathrm{Hue}[\frac{30}{31}], \mathrm{Hue}[\frac{29}{31}], \mathrm{Hue}[\frac{20}{31}], \mathrm{Hue}[\frac{23}{31}], \mathrm{Hue}[\frac{18}{31}], \mathrm{Hue}[\frac{17}{31}], \mathrm{Hue}[\frac{17}{31}],$
$\mathrm{Hue}[\frac{18}{31}], \mathrm{Hue}[\frac{23}{31}], \mathrm{Hue}[\frac{20}{31}], \mathrm{Hue}[\frac{29}{31}], \mathrm{Hue}[\frac{30}{31}], \mathrm{Hue}[\frac{27}{31}], \mathrm{Hue}[\frac{24}{31}],$
$\mathrm{Hue}[\frac{9}{31}], \mathrm{Hue}[\frac{10}{31}], \mathrm{Hue}[\frac{15}{31}], \mathrm{Hue}[\frac{12}{31}], \mathrm{Hue}[\frac{5}{31}], \mathrm{Hue}[\frac{6}{31}], \mathrm{Hue}[\frac{3}{31}], \mathrm{Hue}[0]\}\}$

```
In[78]:= Show[Graphics[RasterArray[m]]]
```



EN RÉSUMÉ

Si p est un nombre premier et si P un polynôme irréductible de degré f de $\mathbb{Z}_p[X]$, alors

$$\boxed{\mathbb{Z}_p[X]/\langle P\rangle}$$

est un champ à p^f éléments.

Questions :

- existence de polynômes irréductibles ?
- nombre d'éléments d'un champ fini quelconque ?

Nous devons encore démontrer le résultat suivant :

COROLLAIRE

Soient $\mathbb{K}$ un champ et $P \in \mathbb{K}[X]$. L'idéal $\langle P \rangle$ est un idéal maximal si et seulement si P est irréductible.

$\Rightarrow$ Supposons $\langle P \rangle$ idéal maximal avec $P \neq 0$.

P ne peut pas être constant.
P.A. Supposons qu'il le soit. $P = k \in \mathbb{K} \setminus \{0\}$ et $k^{-1}.k = 1$ doit appartenir à $\langle k \rangle$ d'où $\langle P \rangle = \mathbb{K}[X]$, impossible !

Supposons à présent que P est un polynôme non constant qui se factorise en $P = Q.R$.

$\langle P \rangle \subseteq \langle Q \rangle$. Si $\langle P \rangle = \langle Q \rangle$, alors R est constant. Sinon, $\langle P \rangle \subsetneq \langle Q \rangle$ et puisque $\langle P \rangle$ est maximal, $\langle Q \rangle = \mathbb{K}[X]$ donc Q est constant.

$\Leftarrow$ si P est un polynôme irréductible,
montrer que l'anneau $\mathbb{K}[X]/\langle P\rangle$ est un champ
(d'où conclusion, par thm...).

Thèse : tout élément non nul $\pi(Q) = Q + \langle P\rangle$ du quotient $\mathbb{K}[X]/\langle P\rangle$ est inversible.

REM : $\pi(Q)$ est non nul SSI $Q \notin \langle P\rangle$.

Partie 1. Montrons que $\langle P, Q\rangle = \mathbb{K}[X]$.

Puisque $\mathbb{K}[X]$ est principal, $\exists T$ t.q. $\langle P, Q\rangle = \langle T\rangle$.

$\exists$ U et V t.q. $P = U.T$ et $Q = V.T$.

Par hypothèse, P irréductible, donc U ou T est constant.

Si T constant, alors $\langle P, Q\rangle = \langle T\rangle = \mathbb{K}[X]$.
Si U constant, $U = k \in \mathbb{K}$, $k \neq 0$, U inversible dans $\mathbb{K}[X]$
P et T sont associés, $\langle P\rangle = \langle T\rangle = \langle P, Q\rangle$, $Q \in \langle P\rangle$, impossible !

Partie 2. Nous savons que $\langle P, Q\rangle = \mathbb{K}[X]$.

$\langle P, Q\rangle = \mathbb{K}[X] \ni 1$. $\exists\, A, B \in \mathbb{K}[X]$ t.q.

$$1 = A.P + B.Q.$$

Dans l'anneau quotient $\mathbb{K}[X]/\langle P\rangle$,

$$(B + \langle P\rangle).(Q + \langle P\rangle) = 1 + \langle P\rangle$$

et donc, $\pi(Q)$ est inversible d'inverse $B + \langle P\rangle$. **QED**

PROPOSITION

Tout polynôme de $\mathbb{K}[X]$ se décompose de manière unique comme produit de polynômes irréductibles (à des facteurs constants et à l'ordre des facteurs près).

$\deg P.Q = \deg P + \deg Q \Rightarrow$ existence de la décomposition
si un polynôme n'est pas irréductible,
il se factorise en un produit de 2 polynômes de degré <
la procédure s'arrête.

L'unicité de la décomposition découle du lemme suivant.

LEMME

Si $P \in \mathbb{K}[X]$ est irréductible et si P divise $F.G$,
alors P divise F ou G.

Lemme

Si $P \in \mathbb{K}[X]$ est irréductible et si P divise $F.G$,
alors P divise F ou G.

Si P ne divise pas F. $F \notin \langle P \rangle$

$\langle P \rangle$ inclus strictement dans $\langle P, F \rangle$.

Puisque P irréductible, $\langle P \rangle$ est maximal.

Donc, $\langle P, F \rangle = \mathbb{K}[X]$ contient 1
$\exists$ S et T t.q. $1 = S.P + T.F$.

$$G = SPG + TFG$$

P divise chacun des deux termes de la somme, P divise G.
QED

REMARQUE

les polynômes irréductibles jouent, dans $\mathbb{K}[X]$, le même rôle que les nombres premiers, dans l'ensemble des entiers.

A SUIVRE...

moyen commode pour générer des champs finis à p^f éléments pour tout $p \geq 2$ premier,

s'il existe au moins un polynôme irréductible de degré f sur $\mathbb{Z}_p$.

Dans la suite, construction alternative en considérant l'extension d'un champ $\mathbb{K}$ par un élément algébrique