CRY 2024

Anneaux et Corps

Alexandre Duc

Retour sur $\mathbb{Z}_m$

- L'ensemble $\mathbb{Z}_m = \{0, 1, \ldots, m-1\}$ muni de l'addition modulo m forme un groupe additif.
- L'ensemble $\{1, \ldots, m-1\}$ muni de la multiplication modulo m ne forme **pas forcément** un groupe multiplicatif.
- Néanmoins, si l'on munit l'ensemble $\{0, 1, \ldots, m-1\}$ de l'addition modulo m **et** de la multiplication modulo m, on constate les propriétés suivantes pour tout $a, b, c \in \{0, 1, \ldots, m-1\}$:

$$\begin{aligned} a \cdot (b + c) &\equiv a \cdot b + a \cdot c \pmod{m} \\ (b + c) \cdot a &\equiv b \cdot a + c \cdot a \pmod{m} \end{aligned}$$

- Ces propriétés s'appellent **distributivité à gauche** et **à droite** de la multiplication par rapport à l'addition, respectivement.

Anneau

Un **anneau** $(\mathbb{A}, +, \times)$ est un ensemble $\mathbb{A}$ muni de deux opérations $+$ et $\times$ qui vérifient les propriétés suivantes :

- $(\mathbb{A}, +)$ est un groupe abélien.
- L'opération $\times$ est une loi de composition interne et associative sur $\mathbb{A}$.
- L'opération $\times$ est distributive à gauche et à droite par rapport à $+$.
- L'opération $\times$ admet un élément neutre dans $\mathbb{A}$.

Anneau

- Un anneau $(\mathbb{A}, +, \times)$ pour lequel $\times$ est également commutatif s'appelle un **anneau commutatif**.

☞ On remarque que $(\mathbb{A}\backslash\{0\}, \times)$ forme **presque** un groupe : il ne lui manque que l'exigence d'inverse !

☞ Ainsi, $\{0, 1, \ldots, m-1\}$ muni de l'addition et de la multiplication modulo m forme un anneau.

$\mathbb{Z}_m$: Résumé

- $\mathbb{Z}_m$ est toujours un **anneau** (muni de l'addition et de la multiplication modulo m).
- $\mathbb{Z}_m$ muni uniquement de l'addition modulo m est un **groupe additif**.
- $\mathbb{Z}_m^*$ muni uniquement de la multiplication modulo m est un **groupe multiplicatif**.

Retour sur $\mathbb{Z}_p$

- On remarque que $\mathbb{Z}_p \backslash \{0\} = \{1, \ldots, p-1\}$ muni de la multiplication modulo p forme **de plus** un groupe (abélien).
- On dit que $\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$ muni de l'addition et de la multiplication modulo p forme un **corps**.

Corps

Définition (Corps)

Un **corps** est un anneau dans lequel l'ensemble des éléments non nuls forme un groupe.

- ☞ En résumé, un corps est un ensemble muni d'une addition et d'une multiplication avec lequel il est possible de calculer (additioner, soustraire, multiplier, diviser) selon les règles habituelles de l'arithmétique.
- ☞ Exemples de corps : $\mathbb{Q}$ (les nombres rationnels), $\mathbb{R}$ (les nombres réels), $\mathbb{C}$ (les nombres complexes) munis de l'addition et de la multiplication.
- ☞ Un corps comportant un nombre fini d'éléments est appelé un **corps fini**.

Nombre d'Élements d'un Corps Fini

Théorème (Corps Fini)

- Si $\mathbb{F}$ est un corps fini, alors $\mathbb{F}$ contient p^m éléments, avec p premier et $m \geq 1$.
- Pour chaque puissance p^m d'un nombre premier, il existe un unique corps fini d'ordre p^m.

☞ Le corps à p^m éléments est noté $\mathrm{GF}(p^m)$, en honneur du mathématicien français **Évariste Galois** (1811-1832).

☞ Le nombre p est appelé **caractéristique** du corps $\mathrm{GF}(p^m)$.

☞ Le plus petit corps fini est $\mathrm{GF}(2)$. Il ne comporte que les éléments 0 et 1.

Polynômes sur un Corps

Définition (Anneau des Polynômes sur un Corps)

On note $\mathbb{Z}_p[x]$ **l'anneau** formé de l'ensemble des polynômes en x possédant des cœfficients dans $\mathbb{Z}_p$.

- $x^5 + x^2 + x + 1 \in \mathbb{Z}_2[x]$,
- $3x^5 + 2x^2 + x \in \mathbb{Z}_5[x]$,

☞ On appelle $0 \in \mathbb{Z}_p[x]$ le **polynôme nul**.

☞ Un polynôme dont le monôme de plus haut degré possède un cœfficient égal à 1 s'appelle un polynôme **unitaire**.

☞ Il est possible d'additionner et de multiplier des polynômes entre eux, le calcul sur les cœfficients se faisant dans le corps sous-jacent.

Polynômes sur un Corps

Question

- Sur $\mathbb{Z}_2[x]$, que vaut $(x+1)^2$?
- Sur $\mathbb{Z}_2[x]$, que vaut $(x^2+x+1)\cdot(x^8+x+1)$?
- Sur $\mathbb{Z}_5[x]$, que vaut $(x^5+4)^2$?

Division Euclidienne de Polynômes

Définition (Division Euclidienne de Polynômes)

Soit $a(x), b(x) \in \mathbb{Z}_p[x]$, avec $b(x) \neq 0$. La division euclidienne de $a(x)$ par $b(x)$ consiste à écrire $a(x) = q(x)b(x) + r(x)$, où le degré de $r(x)$ est strictement inférieur au degré de $b(x)$.

- On note $a(x) \equiv r(x) \pmod{b(x)}$, ou $r(x) = a(x) \bmod b(x)$.
- Par exemple, sur $\mathbb{Z}_2$:

$$x^4 + x + 1 = (x + 1)(x^3 + x^2 + x) + 1$$
$$x^2 + 1 = (x + 1)^2$$
$$x^4 + x + 1 = (x^2 + 1)(x^2 + 1) + x$$

Polynômes Irréductibles

Polynômes Irréductibles

Un polynôme $p(x) \in \mathbb{Z}_p[x]$ est **irréductible** s'il est **non-constant** et si ses seuls diviseurs sont des polynômes constants et de polynômes de la forme $\alpha p(x)$, pour $\alpha \in \mathbb{Z}_p$.

Factorisation de Polynômes

- $x^2 + x + 1$ est **irréductible** dans $\mathbb{Z}_2[x]$: on ne peut pas l'écrire sous forme de produits de polynômes de degrés inférieurs à 2.

Théorème (Factorisation de Polyômes)

Tout polynôme $a(x) \in \mathbb{Z}_p[x]$ non-nul est, à l'ordre près, le produit unique de $\alpha \in \mathbb{Z}_p$ et de polynômes unitaires irréductibles.

☞ Les polynômes irréductibles jouent un rôle similaire aux nombres premiers.

Irréductibilité des Polynômes

- Un polynôme **de degré deux ou trois** est irréductible si et seulement si il n'a pas de racine.
- **Exemple :** $x^2 + 1$ est irréductible dans $\mathbb{Z}_3[x]$ mais pas dans $\mathbb{Z}_2[x]$.
- **Attention :** Contrairement à la factorisation des entiers, il existe des algorithmes efficaces pour factoriser un polynôme (algorithme de Cantor–Zassenhaus).
- A la main, pour des degrés $k > 2$, la solution la plus facile est de tester si le polynôme est divisible par tous les polynômes irréductible de degrés $\leq k/2$.

PGCD de Polynômes

Définition (PGCD de Polynômes)

Le $\mathrm{pgcd}(a(x), b(x))$, avec $a(x), b(x) \in \mathbb{Z}_p[x]$ est défini comme étant l'unique polynôme **unitaire** de degré maximal qui divise $a(x)$ et $b(x)$.

- L'algorithme d'Euclide s'applique également aux polynômes : $\mathrm{pgcd}(a(x), b(x)) = \mathrm{pgcd}(b(x), a(x) \bmod b(x))$, si le degré de $a(x)$ est supérieur au degré de $b(x)$.
- De manière similaire, on peut calculer l'identité de Bézout sur les polynômes au moyen de l'algorithme d'Euclide étendu.

Opération Polynômes

Question

- Sur $\mathbb{Z}_2[x]$, que vaut $\mathrm{pgcd}(x^4 + x^2 + 1, x^3 + 1)$?
- Sur $\mathbb{Z}_2[x]$, donnez l'identité de Bézout entre x^4+x+1 et x^2+1.
- Sur $\mathbb{Z}_3[x]$, donnez l'identité de Bézout entre x^4+x^2 et x^3+2x^2.

Anneau $\mathbb{F}[x]/(m(x))$

- Étant donné un corps $\mathbb{F}$ et un polynôme $m(x) \in \mathbb{F}[x]$, on peut définir l'anneau $\mathbb{F}[x]/(m(x))$:
  - Les éléments de l'anneau sont les polynômes de degré inférieur à $m(x)$ possédant des cœfficients dans $\mathbb{F}$.
  - Les deux opérations de l'anneau sont l'addition et la multiplication modulo $m(x)$, respectivement.

Corps $\mathbb{F}[x]/(m(x))$

- Étant donné un anneau $\mathbb{F}[x]/(m(x))$, et en exigeant que $m(x)$ soit **irréductible** sur $\mathbb{F}$, on obtient une structure de **corps**.
- En effet, il est possible de calculer un inverse modulo $m(x)$ pour tout élément de l'anneau (à part 0) en utilisant l'algorithme d'Euclide étendu.
- Par exemple, $\mathbb{Z}_2[x]/(x^8 + x^4 + x^3 + x^2 + 1)$ forme un corps possédant 256 éléments, qui sont les polynômes de degré au plus 7 avec des cœfficients égaux à 0 ou à 1.

Corps $\mathbb{F}[x]/(m(x))$

Question

Listez tous les éléments du corps $\mathbb{Z}_3[x]/(x^2 + 2x + 2)$. Combien d'éléments possède-t-il ?

Construction d'un Corps de Galois (premier)

Pour un corps de Galois **de type $\mathbf{GF}(p)$, avec p premier** :

- On utilise simplement le corps $\mathbb{Z}_p$, i.e., les entiers modulo p.
- Exemple : $\mathrm{GF}(3)$ peut être construit comme les entiers modulo 3.

$\mathrm{GF}(2)$

- $\mathrm{GF}(2)$ consiste en l'ensemble $\{0, 1\}$ avec l'addition et la multiplication modulo 2.
- Sur $\mathrm{GF}(2)$, $a - b = a + b$ pour tout $a, b \in \mathrm{GF}(2)$.

☞ On peut remplacer les soustractions par des additions !

- Sur $\mathrm{GF}(2)$, $a + a = 0$.

☞ On a donc $(2k) \cdot a = 0$ pour tout $a \in \mathrm{GF}(2)$ et $k \in \mathbb{Z}$.

Construction d'un Corps de Galois (non premier)

Pour un corps de Galois **de type $\mathbf{GF}(p^m)$, avec p premier et $m > 1$** :

- On choisit un polynôme $p(x)$ de degré m irréductible sur $\mathbb{Z}_p$.
- Les éléments de $\mathrm{GF}(p^m)$ sont les polynômes de degrés au plus $m-1$ possédant des cœfficients dans $\mathbb{Z}_p$.
- Nous travaillons donc dans $\mathbb{Z}_p[x]$ et les multiplications sont faites modulo $p(x)$.

Corps de Galois de Type $\mathrm{GF}(p^k)$ – Exemples

- Le corps à 9 éléments peut être construit au moyen d'un polynôme de degré 2 irréductible sur $\mathbb{Z}_3$.
- Le corps à 81 éléments peut être construit au moyen d'un polynôme de degré 4 irréductible sur $\mathbb{Z}_3$.
- Le corps à 65536 éléments peut être construit au moyen d'un polynôme de degré 16 irréductible sur $\mathbb{Z}_2$.

Construction de $\mathrm{GF}(2^2)$

- Le corps à 4 éléments peut être construit au moyen du polynôme irréductible $p(x) = x^2 + x + 1$ sur $\mathbb{Z}_2$.
- Les éléments de $\mathrm{GF}(4)$ sont les polynômes de la forme $ax + b$, avec $a, b \in \{0, 1\}$.
- L'addition et la multiplication s'effectuent modulo $x^2 + x + 1$.

Construction de $\mathrm{GF}(3^2)$

- Le corps à 9 éléments peut être construit au moyen du polynôme irréductible $p(x) = x^2 + 2x + 2$ sur $\mathbb{Z}_3$.
- Les éléments de $\mathrm{GF}(9)$ sont les polynômes de la forme $ax + b$, avec $a, b \in \{0, 1, 2\}$.
- L'addition et la multiplication s'effectuent modulo $x^2 + 2x + 2$.

Corps de Galois

Question

Effectuez les tables d'addition et de multiplication pour le corps $\mathbb{Z}_2[x]/(x^2 + x + 1)$. Vérifiez l'existence d'un inverse multiplicatif pour chaque élément.

Solutions

Polynômes sur un Corps

Solution

- $(x+1)^2 = x^2 + 2x + 1 = x^2 + 1$
- $$(x^2 + x + 1) \cdot (x^8 + x + 1) = x^{10} + x^9 + x^8 + x^3 + 2x^2 + 2x + 1 = x^{10} + x^9 + x^8 + x^3 + 1$$
- $$(x^5 + 4)^2 = x^{10} + 8x^5 + 16 = x^{10} + 3x^5 + 1$$

Opérations Polynômes

- Sur $\mathbb{Z}_2[x]$, $\mathrm{pgcd}(x^4 + x^2 + 1, x^3 + 1) = x^2 + x + 1$.
- Sur $\mathbb{Z}_2[x]$, l'algorithme d'Euclide étendu entre $x^4 + x + 1$ et $x^2 + 1$ donne

		q
$(x^4 + x + 1, 1, 0)$	$(x^2 + 1, 0, 1)$	$x^2 + 1$
$(x^2 + 1, 0, 1)$	$(x, 1, x^2 + 1)$	x
$(x, 1, x^2 + 1)$	$(1, x, x^3 + x + 1)$	x
$(1, x, x^3 + x + 1)$	$(0, \dots)$	

On a donc $1 = (x^4 + x + 1)x + (x^2 + 1)(x^3 + x + 1)$.

Opérations Polynômes (suite)

- Sur $\mathbb{Z}_3[x]$, l'algorithme d'Euclide étendu entre $x^4 + x^2$ et $x^3 + 2x^2$ donne

		q
$(x^4 + x^2, 1, 0)$	$(x^3 + 2x^2, 0, 1)$	$x + 1$
$(x^3 + 2x^2, 0, 1)$	$(2x^2, 1, 2x + 2)$	$2x + 1$
$(2x^2, 1, 2x + 2)$	$(0, \dots)$	

On a donc $2x^2 = (x^4 + x^2) \cdot 1 + (x^3 + 2x^2)(2x + 2)$.

$2x^2$ n'est pas unitaire. Ce n'est donc pas le pgcd. On peut diviser par 2 et on obtient :

$$x^2 = (x^4 + x^2) \cdot 2 + (x^3 + 2x^2)(x + 1)\ .$$

Corps $\mathbb{F}[x]/(m(x))$

Solution

$$0, 1, 2, x, x+1, x+2, 2x, 2x+1, 2x+2.$$

Il a donc 9 éléments. Il s'agit d'une représentation de GF(9).

Corps de Galois

$+$	0	1	x	$x+1$
0	0	1	x	$x+1$
1	1	0	$x+1$	x
x	x	$x+1$	0	1
$x+1$	$x+1$	x	1	0

$\times$	1	x	$x+1$
1	1	x	$x+1$
x	x	$x+1$	1
$x+1$	$x+1$	1	x