"Ecole sur les Codes Correcteurs d'Erreurs" (Algérie)

Codes et anneaux

Dr. Joël KABORE

Laboratoire de Mathématiques et Informatique (LAMI)
Université Joseph KI-ZERBO
Burkina-Faso

Septembre 2025

Objectifs

- Décomposition d'un anneau fini via le Théorème des Reste Chinois
- Propriétés des polynômes sur un anneau
- Caractérisation des anneaux à chaînes finis

Rappels sur les codes

Soit $\mathcal{A}$(alphabet) un ensemble fini.

- Code en bloc de longueur n sur $\mathcal{A}$: $(\emptyset \neq)\mathcal{C} \subseteq \mathcal{A}^n$
- Distance de Hamming : $d(a,b) = |\{i : a_i \neq b_i\}|$,, où $a = (a_1, ..., a_n)$ et $b = (b_1, ..., b_n)$ deux mots de codes.
- Distance minimale : $d(\mathcal{C}) = min\{d(a,b) : a, b \in \mathcal{C}, a \neq b\}$
- (n, M, d)-code sur $\mathcal{A}$: code de longueur n, de taille M, de distance minimale d.
- $\mathcal{C}$ corrige l-erreurs si $\forall\ a\ \in \mathcal{A}^n$, il existe au plus un mot de code c tel que $d(a,c) \leq l$.
  Capacité de correction e : nombre maximal d' erreurs que $\mathcal{C}$ peut corriger.
  Pour un code $\mathcal{C}$ de distance minimale d, $e = \left[\frac{d-1}{2}\right]$.

Rappels sur les codes

Soit $\mathcal{A}$(alphabet) un ensemble fini.

- Code en bloc de longueur n sur $\mathcal{A}$: $(\emptyset \neq)\mathcal{C} \subseteq \mathcal{A}^n$
- Distance de Hamming : $d(a,b) = |\{i : a_i \neq b_i\}|$,, où $a = (a_1, ..., a_n)$ et $b = (b_1, ..., b_n)$ deux mots de codes.
- Distance minimale : $d(\mathcal{C}) = min\{d(a,b) : a, b \in \mathcal{C}, a \neq b\}$
- (n, M, d)-code sur $\mathcal{A}$: code de longueur n, de taille M, de distance minimale d.
- $\mathcal{C}$ corrige l-erreurs si $\forall\ a\ \in \mathcal{A}^n$, il existe au plus un mot de code c tel que $d(a,c) \leq l$.
  Capacité de correction e : nombre maximal d' erreurs que $\mathcal{C}$ peut corriger.
  Pour un code $\mathcal{C}$ de distance minimale d, $e = \left[\frac{d-1}{2}\right]$.
- $\mathcal{A}$ comme structure algébrique : corps finis et anneaux finis.

Corps finis vs anneaux finis

- Diviseur de zéros
  ▷ polynômes non constant inversibles
  Exemple : $f(X) = (1 + 2X + 2X^2) \in \mathbb{Z}_4[X]$ est inversible.

Corps finis vs anneaux finis

- Diviseur de zéros
  ▷ polynômes non constant inversibles
  Exemple : $f(X) = (1 + 2X + 2X^2) \in \mathbb{Z}_4[X]$ est inversible.
  ▷ Unicité de factorisation
  Exemple :
  $X^4 - 1 = (X - 1)(X + 1)\left(X^2 + 1\right) = (X + 1)^2\left(X^2 + 2X - 1\right)$ dans $\mathbb{Z}_4[X]$.

Idéaux particuliers

Soit $\mathcal{A}$ un anneau commutatif unitaire et $U(\mathcal{A})$ le groupe multiplicatif des éléments inversibles de $\mathcal{A}$.

- $a \in \mathcal{A} \setminus 0$ est un diviseur de zéro si $\exists b(\neq 0) \in \mathcal{A}$ tel que $ab = 0$. $\mathcal{Z}(\mathcal{A})$ désignera l'ensemble des diviseurs de zéro de $\mathcal{A}$.
- $\mathrm{Ann}(I) := \{x \in \mathcal{A} / xI = (0)\}$ est un idéal de $\mathcal{A}$ (exercice) appelé annulateur de I.

Idéaux particuliers

Soit $\mathcal{A}$ un anneau commutatif unitaire et $U(\mathcal{A})$ le groupe multiplicatif des éléments inversibles de $\mathcal{A}$.

- $a \in \mathcal{A} \setminus 0$ est un diviseur de zéro si $\exists b(\neq 0) \in \mathcal{A}$ tel que $ab = 0$.
  $\mathcal{Z}(\mathcal{A})$ désignera l'ensemble des diviseurs de zéro de $\mathcal{A}$.
- $\mathrm{Ann}(I) := \{x \in \mathcal{A} / xI = (0)\}$ est un idéal de $\mathcal{A}$ (exercice) appelé annulateur de I.
  $\mathcal{Z}(\mathcal{A}) = \bigcup_{a \in \mathcal{A}} \mathrm{Ann}(a)$.
- $a \in \mathcal{A} \setminus 0$ est dit nilpotent si $a^n = 0$ pour un certain $n \in \mathbb{N}^*$.
- Nilradical de $\mathcal{A}$ (noté $\mathcal{N}(\mathcal{A})$) : ensemble des éléments nilpotents de $\mathcal{A}$ est un idéal de $\mathcal{A}$(exercice).

Idéaux particuliers

Soit $\mathcal{A}$ un anneau commutatif unitaire et $U(\mathcal{A})$ le groupe multiplicatif des éléments inversibles de $\mathcal{A}$.

- $a \in \mathcal{A} \setminus 0$ est un diviseur de zéro si $\exists b(\neq 0) \in \mathcal{A}$ tel que $ab = 0$.
  $\mathcal{Z}(\mathcal{A})$ désignera l'ensemble des diviseurs de zéro de $\mathcal{A}$.
- $\mathrm{Ann}(I) := \{x \in \mathcal{A} / xI = (0)\}$ est un idéal de $\mathcal{A}$ (exercice) appelé annulateur de I.
  $\mathcal{Z}(\mathcal{A}) = \bigcup_{a \in \mathcal{A}} \mathrm{Ann}(a)$.
- $a \in \mathcal{A} \setminus 0$ est dit nilpotent si $a^n = 0$ pour un certain $n \in \mathbb{N}^*$.
- Nilradical de $\mathcal{A}$ (noté $\mathcal{N}(\mathcal{A})$) : ensemble des éléments nilpotents de $\mathcal{A}$ est un idéal de $\mathcal{A}$(exercice).
  $\mathcal{N}(\mathcal{A}) = \bigcap_{P \text{ ideal premier}} P$.

Idéaux particuliers

- $\mathcal{A}$ admet au moins un idéal maximal
- Radical de Jacobson : $\mathcal{J}(\mathcal{A}) = \bigcap_{\mathfrak{m}\ \text{idealmaximal}} \mathfrak{m}$.
- $a \in \mathcal{J}(\mathcal{A}) \iff 1 - ab \in U(\mathcal{A}), \forall b \in \mathcal{A}$
- Tout idéal est contenu dans au moins un idéal maximal
- A est dit local s'il possède un seul idéal maximal
- Un idéal I de $\mathcal{A}$ est dit primaire si $I \neq A$ et si $\forall a, b \in \mathcal{A}$: $ab \in I \Rightarrow a \in I$ ou $\exists n \in \mathbb{N} \mid b^n \in I$.

Théorème des Restes Chinois

- Deux idéaux I et J de $\mathcal{A}$ sont dits étrangers (ou comaximaux) si $I + J = \mathcal{A}$.
  - ▷ Si I et J sont étrangers alors $I + J = IJ$
  - ▷ **Exemple :** $\mathfrak{m}_1 + \mathfrak{m}_2 = A$ où $\mathfrak{m}_1$ et $\mathfrak{m}_2$ sont deux idéaux maximaux distincts de $\mathcal{A}$.

Théorème des Restes Chinois

- Deux idéaux I et J de $\mathcal{A}$ sont dits étrangers (ou comaximaux) si $I + J = \mathcal{A}$.
  ▷ Si I et J sont étrangers alors $I + J = IJ$
  ▷ **Exemple :** $\mathfrak{m}_1 + \mathfrak{m}_2 = A$ où $\mathfrak{m}_1$ et $\mathfrak{m}_2$ sont deux idéaux maximaux distincts de $\mathcal{A}$.
  ▷ **Exercice :** Montrer que $\mathfrak{m}_1^{e_1} + \mathfrak{m}_2^{e_2} = \mathcal{A}$ où $\mathfrak{m}_1$ et $\mathfrak{m}_2$ sont deux idéaux maximaux distincts de $\mathcal{A}$, e_1, e_2 des entiers naturels non nuls.

Théorème des Restes Chinois

- Deux idéaux I et J de $\mathcal{A}$ sont dits étrangers (ou comaximaux) si $I + J = \mathcal{A}$.
  ▷ Si I et J sont étrangers alors $I + J = IJ$
  ▷ **Exemple :** $\mathfrak{m}_1 + \mathfrak{m}_2 = A$ où $\mathfrak{m}_1$ et $\mathfrak{m}_2$ sont deux idéaux maximaux distincts de $\mathcal{A}$.
  ▷ **Exercice :** Montrer que $\mathfrak{m}_1^{e_1} + \mathfrak{m}_2^{e_2} = \mathcal{A}$ où $\mathfrak{m}_1$ et $\mathfrak{m}_2$ sont deux idéaux maximaux distincts de $\mathcal{A}$, e_1, e_2 des entiers naturels non nuls.
- Soient $I_1, ..., I_l$ des idéaux de $\mathcal{A}$ étrangers deux à deux et $\psi : \mathcal{A} \longrightarrow \prod_{i=1}^{l} \mathcal{A}/I_i$, la surjection canonique défini par : $\psi(x) = (x + I_1, ..., x + I_l)$.

Théorème des Restes Chinois

- Deux idéaux I et J de $\mathcal{A}$ sont dits étrangers (ou comaximaux) si $I + J = \mathcal{A}$.
  ▷ Si I et J sont étrangers alors $I + J = IJ$
  ▷ **Exemple :** $\mathfrak{m}_1 + \mathfrak{m}_2 = A$ où $\mathfrak{m}_1$ et $\mathfrak{m}_2$ sont deux idéaux maximaux distincts de $\mathcal{A}$.
  ▷ **Exercice :** Montrer que $\mathfrak{m}_1^{e_1} + \mathfrak{m}_2^{e_2} = \mathcal{A}$ où $\mathfrak{m}_1$ et $\mathfrak{m}_2$ sont deux idéaux maximaux distincts de $\mathcal{A}$, e_1, e_2 des entiers naturels non nuls.
- Soient $I_1, ..., I_l$ des idéaux de $\mathcal{A}$ étrangers deux à deux et $\psi : \mathcal{A} \longrightarrow \prod_{i=1}^{l} \mathcal{A}/I_i$, la surjection canonique défini par : $\psi(x) = (x + I_1, ..., x + I_l)$.
  ▷ $\ker(\psi) = \cap_{i=1}^{l} I_i$
  ▷ $\frac{\mathcal{A}}{\cap_{i=1}^{l} I_i} \cong \prod_{i=1}^{l} \mathcal{A}/I_i$. (1er théorème d'isomorphisme)

Module

Définition

Un groupe abélien $(M, +)$ est dit $\mathcal{A}$-module s'il est muni d'une application (modulation) : $\mathcal{A} \times M \longrightarrow M$ telle que : $\forall x, y \in M,\ \forall a, b \in \mathcal{A}$

1. $a(x + y) = ax + ay$
2. $(ab)x = a(bx)$
3. $(a + b)x = ax + bx$
4. $1x = x$

Module

Définition

Un groupe abélien $(M, +)$ est dit $\mathcal{A}$-module s'il est muni d'une application (modulation) : $\mathcal{A} \times M \longrightarrow M$ telle que : $\forall x, y \in M,\ \forall a, b \in \mathcal{A}$

1. $a(x + y) = ax + ay$
2. $(ab)x = a(bx)$
3. $(a + b)x = ax + bx$
4. $1x = x$

▷ Si $\mathcal{A}$ est un corps, $\mathcal{A}$-module $\equiv$ $\mathcal{A}$-espace vectoriel

▷ Tout groupe abélien est un $\mathbb{Z}$-module

▷ Un idéal de $\mathcal{A}$ est un $\mathcal{A}$-module.

Module

- Soit M un $\mathcal{A}$-module. On dit que N est un sous module de M si :
  - $(N, +)$ est un sous groupe de M
  - $ax \in N \ \forall \ (x, a) \in N \times \mathcal{A}$.

Module

- Soit M un $\mathcal{A}$-module. On dit que N est un sous module de M si :
  - $(N, +)$ est un sous groupe de M
  - $ax \in N \ \forall \ (x, a) \in N \times \mathcal{A}$.
- Le groupe quotient $(M/N, +)$ est un $\mathcal{A}$-module (module quotient).
- Les sous-modules du $\mathcal{A}$-module $\mathcal{A}$ sont les idéaux de $\mathcal{A}$.

Module

- Soit M un $\mathcal{A}$-module. On dit que N est un sous module de M si :
  - ▷ $(N, +)$ est un sous groupe de M
  - ▷ $ax \in N \ \forall \ (x, a) \in N \times \mathcal{A}$.
- Le groupe quotient $(M/N, +)$ est un $\mathcal{A}$-module (module quotient).
- Les sous-modules du $\mathcal{A}$-module $\mathcal{A}$ sont les idéaux de $\mathcal{A}$.
- M est dit de type fini s'il existe $\{x_1, \ldots, x_n\} \subseteq M$ tel que $M = \langle x_1, \ldots, x_n \rangle = M$; i.e $M = \sum_{i=1}^{n} \mathcal{A}x_i$.
  - ▷ Si $M =< x >$, on dit qu'il est cyclique.

Modules

Lemme de Nakayama

Soient I un idéal de $\mathcal{A}$, $\mathcal{J}(\mathcal{A})$ le radical de Jacobson de l'anneau A et M un module de type fini de $\mathcal{A}$. Alors

$$I \subseteq \mathcal{J}(\mathcal{A})$$
$$\Updownarrow$$
$$(IM = M \Rightarrow M = 0)$$

- Un $\mathcal{A}$-module M est dit libre s'il possède une base (i.e. une famille libre et génératrice).

Modules

Lemme de Nakayama

Soient I un idéal de $\mathcal{A}$, $\mathcal{J}(\mathcal{A})$ le radical de Jacobson de l'anneau A et M un module de type fini de $\mathcal{A}$. Alors

$$I \subseteq \mathcal{J}(\mathcal{A})$$
$$\Updownarrow$$
$$(IM = M \Rightarrow M = 0)$$

- Un $\mathcal{A}$-module M est dit libre s'il possède une base (i.e. une famille libre et génératrice).
  ▷ Tout $\mathbb{K}$-espace vectoriel possède une base, mais un module peut ne pas avoir de base.

Modules

Lemme de Nakayama

Soient I un idéal de $\mathcal{A}$, $\mathcal{J}(\mathcal{A})$ le radical de Jacobson de l'anneau A et M un module de type fini de $\mathcal{A}$. Alors

$$I \subseteq \mathcal{J}(\mathcal{A})$$
$$\Updownarrow$$
$$(IM = M \Rightarrow M = 0)$$

- Un $\mathcal{A}$-module M est dit libre s'il possède une base (i.e. une famille libre et génératrice).
  ▷ Tout $\mathbb{K}$-espace vectoriel possède une base, mais un module peut ne pas avoir de base.
  Exemple : Le $\mathbb{Z}$-module $\mathbb{Z}_n$.

Anneau non local

On suppose que $\mathcal{A}$ est un anneau fini non local. Soient $\mathfrak{m}_1, \mathfrak{m}_2$ deux idéaux maximaux de $\mathcal{A}$.

- $\exists e_1 \in \mathbb{N}^* \mid \mathfrak{m}_1^{e_1} = \mathfrak{m}_1^{e_1+1} \neq \{0\}$;
  e_1 est appelé **index de stabilité** de $\mathfrak{m}_1$.

Anneau non local

On suppose que $\mathcal{A}$ est un anneau fini non local. Soient $\mathfrak{m}_1, \mathfrak{m}_2$ deux idéaux maximaux de $\mathcal{A}$.

- $\exists e_1 \in \mathbb{N}^* \mid \mathfrak{m}_1^{e_1} = \mathfrak{m}_1^{e_1+1} \neq \{0\}$;
  e_1 est appelé **index de stabilité** de $\mathfrak{m}_1$.
  ▷ Puisque $\mathcal{A}$ est fini, la suite décroissante suivante est stationnaire $\mathcal{A} \supsetneq \mathfrak{m}_1 \supsetneq \cdots \supsetneq \mathfrak{m}_1^{e_1} \supsetneq \mathfrak{m}_1^{e_1+1} \supsetneq \cdots$. De plus $\mathfrak{m}_1^{e_1} \neq \{0\}$ car $\mathfrak{m}_1^{e_1} + \mathfrak{m}_2 = \mathcal{A}$.

Anneau non local

On suppose que $\mathcal{A}$ est un anneau fini non local. Soient $\mathfrak{m}_1, \mathfrak{m}_2$ deux idéaux maximaux de $\mathcal{A}$.

- $\exists e_1 \in \mathbb{N}^* \mid \mathfrak{m}_1^{e_1} = \mathfrak{m}_1^{e_1+1} \neq \{0\}$;
  e_1 est appelé **index de stabilité** de $\mathfrak{m}_1$.
  ▷ Puisque $\mathcal{A}$ est fini, la suite décroissante suivante est stationnaire $\mathcal{A} \supsetneq \mathfrak{m}_1 \supsetneq \cdots \supsetneq \mathfrak{m}_1^{e_1} \supsetneq \mathfrak{m}_1^{e_1+1} \supsetneq \cdots$. De plus $\mathfrak{m}_1^{e_1} \neq \{0\}$ car $\mathfrak{m}_1^{e_1} + \mathfrak{m}_2 = \mathcal{A}$.
  ▷ Que devient e_1 si $\mathcal{A}$ est local ? (Conséquence du Lemme de Nakayama).

Anneau non local

On suppose que $\mathcal{A}$ est un anneau fini non local. Soient $\mathfrak{m}_1, \mathfrak{m}_2$ deux idéaux maximaux de $\mathcal{A}$.

- $\exists e_1 \in \mathbb{N}^* \mid \mathfrak{m}_1^{e_1} = \mathfrak{m}_1^{e_1+1} \neq \{0\}$;
  e_1 est appelé **index de stabilité** de $\mathfrak{m}_1$.
  ▷ Puisque $\mathcal{A}$ est fini, la suite décroissante suivante est stationnaire $\mathcal{A} \supsetneq \mathfrak{m}_1 \supsetneq \cdots \supsetneq \mathfrak{m}_1^{e_1} \supsetneq \mathfrak{m}_1^{e_1+1} \supsetneq \cdots$. De plus $\mathfrak{m}_1^{e_1} \neq \{0\}$ car $\mathfrak{m}_1^{e_1} + \mathfrak{m}_2 = \mathcal{A}$.
  ▷ Que devient e_1 si $\mathcal{A}$ est local ? (Conséquence du Lemme de Nakayama).
- $\mathcal{A}/\mathfrak{m}_1^{e_1}$ est local d'idéal maximal $\mathfrak{m}/\mathfrak{m}^{e_1}$.

Décomposition d'anneaux

Théorème

$\mathcal{A}$ est isomorphe à un produit finis d'anneaux locaux. De plus cette décomposition est unique à permutation près des facteurs directs.

Décomposition d'anneaux

Théorème

$\mathcal{A}$ est isomorphe à un produit finis d'anneaux locaux. De plus cette décomposition est unique à permutation près des facteurs directs.

Preuve : Si $\mathcal{A}$ n'est pas local, soient $\mathfrak{m}_1, \mathfrak{m}_2, \cdots, \mathfrak{m}_l$ les idéaux maximaux de A d' indices de stabilité respectives $e_1, e_2, \cdots, e_l$.

▷ les idéaux $\mathfrak{m}_1^{e_1}, \mathfrak{m}_2^{e_2}, \cdots, \mathfrak{m}_l^{e_l}$ sont étrangers deux à deux.

Décomposition d'anneaux

Théorème

$\mathcal{A}$ est isomorphe à un produit finis d'anneaux locaux. De plus cette décomposition est unique à permutation près des facteurs directs.

Preuve : Si $\mathcal{A}$ n'est pas local, soient $\mathfrak{m}_1, \mathfrak{m}_2, \cdots, \mathfrak{m}_l$ les idéaux maximaux de A d' indices de stabilité respectives $e_1, e_2, \cdots, e_l$.

▷ les idéaux $\mathfrak{m}_1^{e_1}, \mathfrak{m}_2^{e_2}, \cdots, \mathfrak{m}_l^{e_l}$ sont étrangers deux à deux.

▷ $\cap_{i=1}^{l} \mathfrak{m}_i^{e_i} = \prod_{i=1}^{l} \mathfrak{m}_i^{e_i} = 0$. (Conséquence Lemme de Nakayama)

Décomposition d'anneaux

Théorème

$\mathcal{A}$ est isomorphe à un produit finis d'anneaux locaux. De plus cette décomposition est unique à permutation près des facteurs directs.

Preuve : Si $\mathcal{A}$ n'est pas local, soient $\mathfrak{m}_1, \mathfrak{m}_2, \cdots, \mathfrak{m}_l$ les idéaux maximaux de A d' indices de stabilité respectives $e_1, e_2, \cdots, e_l$.

- ▷ les idéaux $\mathfrak{m}_1^{e_1}, \mathfrak{m}_2^{e_2}, \cdots, \mathfrak{m}_l^{e_l}$ sont étrangers deux à deux.
- ▷ $\cap_{i=1}^{l} \mathfrak{m}_i^{e_i} = \prod_{i=1}^{l} \mathfrak{m}_i^{e_i} = 0$. (Conséquence Lemme de Nakayama)
- ▷ D'après le Théorème des Restes Chinois $\mathcal{A} \cong \prod_{i=1}^{l} \mathcal{A}/\mathfrak{m}_i^{e_i}$ □.

Anneau de polynômes

Soit $\mathcal{A}$ un anneau local fini, d'idéal maximal $\mathfrak{m}$ et de corps résiduel $k = \mathcal{A}/\mathfrak{m}$. Soit $\bar{}$ le morphisme canonique $\bar{}: \mathcal{A}[X] \to k[X]$. Soient f un polynôme de $\mathcal{A}[X]$ et $< f >$ l'idéal engendré par f.

Anneau de polynômes

Soit $\mathcal{A}$ un anneau local fini, d'idéal maximal $\mathfrak{m}$ et de corps résiduel $k = \mathcal{A}/\mathfrak{m}$. Soit $\bar{}$ le morphisme canonique $\bar{}: \mathcal{A}[X] \to k[X]$. Soient f un polynôme de $\mathcal{A}[X]$ et $< f >$ l'idéal engendré par f.

- f est dit primaire si $< f >$ est un idéal primaire.
- f est dit régulier si f n'est pas un diviseur de zéro.
- f est dit résiduellement irréductible (respectivement résiduellement primaire) si $\bar{f}$ est irréductible (respectivement primaire) dans $k[X]$.
- Deux polynômes f et g de $\mathcal{A}[X]$ sont dits étrangers si $< f >$ et $< g >$ sont étrangers dans $\mathcal{A}[X]$; c'est-à-dire s'il existe u et v dans $R[X]$ tel que $fu + gv = 1$ (Identité de Bezout).

Anneaux de polynômes

Soit $f = a_0 + a_1X + ... + a_nX^n \in \mathcal{A}[X]$

- f **inversible** dans $\mathcal{A}[X] \Leftrightarrow \bar{f}$ est inversible dans $k[X] \Leftrightarrow a_0$ est inversible et $a_1, ..., a_n$ sont nilpotents.
- f est **nilpotent** $\Leftrightarrow \bar{f} = 0 \Leftrightarrow a_0, ..., a_n$ sont nilpotents $\Leftrightarrow f$ est un diviseur de zéro.
- f est **régulier** $\Leftrightarrow < a_0, a_1, ..., a_n >= \mathcal{A} \Leftrightarrow \exists\ i \in \{0, ..., n\}$ tel que a_i soit inversible dans $\mathcal{A} \Leftrightarrow \bar{f} \neq 0$.

Anneau de polynômes

Lemme de Hensel

Soient $\mathcal{A}$ un anneau fini local et $f \in \mathcal{A}[X]$. On suppose que $\overline{f} = g_1 g_2 ... g_r$, où $g_1, g_2, ..., g_r$ sont étrangers deux à deux dans $k[X]$. Alors, il existe des polynômes $f_1, f_2, ..., f_r$ à coefficients dans $\mathcal{A}$, étrangers deux à deux tels que :
$f = f_1 f_2 ... f_r$, et $\overline{f_i} = g_i, \forall\ i = 1, 2, ...r$.

Anneau de polynômes

Lemme de Hensel

Soient $\mathcal{A}$ un anneau fini local et $f \in \mathcal{A}[X]$. On suppose que $\overline{f} = g_1 g_2 ... g_r$, où $g_1, g_2, ..., g_r$ sont étrangers deux à deux dans $k[X]$. Alors, il existe des polynômes $f_1, f_2, ..., f_r$ à coefficients dans $\mathcal{A}$, étrangers deux à deux tels que :
$f = f_1 f_2 ... f_r$, et $\overline{f_i} = g_i, \forall\ i = 1, 2, ...r$.

Proposition

Soit $\mathcal{A}$ est local et f un polynôme régulier dans $\mathcal{A}[X]$.

1. f est résiduellement irréductible $\Rightarrow$ f est irréductible.
2. f est irréductible $\Rightarrow$ $\overline{f} = g^l$, où l est un entier positif et g est irréductible dans $k[X]$.

Décomposition

Proposition

Soit f un polynôme unitaire défini sur un anneau fini local $\mathcal{A}$ tel que $\overline{f}$ est sans facteur carré. Alors f se décompose en un produit de facteurs unitaires résiduellement irréductibles étrangers deux à deux. De plus cette décomposition est unique à permutation près des facteurs.

Anneau de Galois

Les anneaux de Galois sont les extensions de Galois de l'anneau des entiers modulo puissance d'un nombre premier.

Anneau de Galois

Les anneaux de Galois sont les extensions de Galois de l'anneau des entiers modulo puissance d'un nombre premier.
Soient p un nombre premier, n un entier naturel et $\mathbb{Z}_{p^n} := \mathbb{Z}/p^n\mathbb{Z}$.

- $GR(p^n, r) \cong \mathbb{Z}_{p^n}[X]/ < f >= \mathbb{Z}_{p^n}[x]$ où f est un polynôme unitaire résiduellement irréductible de degré r sur $\mathbb{Z}_{p^n}$ et $x = X+ < f >$ est la classe de X dans $\mathbb{Z}_{p^n}[X]/ < f >$.

Anneau de Galois

Les anneaux de Galois sont les extensions de Galois de l'anneau des entiers modulo puissance d'un nombre premier.
Soient p un nombre premier, n un entier naturel et $\mathbb{Z}_{p^n} := \mathbb{Z}/p^n\mathbb{Z}$.

- $GR(p^n, r) \cong \mathbb{Z}_{p^n}[X]/ < f >= \mathbb{Z}_{p^n}[x]$ où f est un polynôme unitaire résiduellement irréductible de degré r sur $\mathbb{Z}_{p^n}$ et $x = X + < f >$ est la classe de X dans $\mathbb{Z}_{p^n}[X]/ < f >$.
- $GR(p^n, r)$ est un $\mathbb{Z}_{p^n}$-module libre de base $\{1, x, \cdots, x^{r-1}\}$
- Il est de caractéristique p^n et d'idéal maximal $pGR(p^n, r)$.
- $|GR(p^n, r)| = p^{nr}$.

▷ pour $n = 1$, on a $GR(p, r) \cong F_{p^r}$.
▷ pour $r = 1$, on a $GR(p^n, 1) \cong \mathbb{Z}_{p^n}$.

Anneaux de Galois

Soient $\bar{}$ le morphisme surjectif défini par :

$$\begin{array}{rccc} \bar{}: & GR(p^n, r) & \longrightarrow & \mathbb{F}_{p^r} \\ & u & \longmapsto & u + pGR(p^n, r). \end{array}$$

et $\mathbb{F}_{p^r} = \{0, 1, \alpha, ..., \alpha^{p^r-2}\}$ où α est un élément primitif de $\mathbb{F}_{p^r}$.
$\triangleright$ $\alpha = \xi + pGR(p^n, r)$; $T = \{0, 1, \xi, ..., \xi^{p^r-2}\}$ est un ensemble (de Teichmuller) de représentants des classes dans $\mathbb{F}_{p^r}$.

Anneaux de Galois

Soient $\bar{}$ le morphisme surjectif défini par :

$$\begin{array}{rccc} \bar{}: & GR(p^n, r) & \longrightarrow & \mathbb{F}_{p^r} \\ & u & \longmapsto & u + pGR(p^n, r). \end{array}$$

et $\mathbb{F}_{p^r} = \{0, 1, \alpha, ..., \alpha^{p^r-2}\}$ où α est un élément primitif de $\mathbb{F}_{p^r}$.
▷ $\alpha = \xi + pGR(p^n, r)$; $T = \{0, 1, \xi, ..., \xi^{p^r-2}\}$ est un ensemble (de Teichmuller) de représentants des classes dans $\mathbb{F}_{p^r}$.
▷ Si u un élément de $GR(p^n, r)$, alors il existe un unique élément s_0 de T tel que $\bar{u} = \bar{s_0}$, i.e. $u - s_0 \in pGR(p^n, r)$. Il existe donc $u_1 \in GR(p^n, r)$ tel que $u = s_0 + pu_1$. De même, il existe un unique $s_1 \in T$ et $u_2 \in GR(p^n, r)$ tels que $u_1 = s_1 + pu_2$. On obtient alors : $u = s_0 + ps_1 + p^2u_2$. En continuant ce même procédé qui est fini puisque $p^n = 0$ dans $GR(p^n, r)$, on peut écrire u sous la forme suivante :

$$u = s_0 + ps_1 + ...p^{n-1}s_{n-1},$$

avec $s_i \in T$. Cette représentation est unique et est appelée représentation p-adique des éléments de $GR(p^n, r)$.

Propriétés

- Les idéaux de l'anneau $GR(p^n, r)$ sont de la forme $p^k GR(p^n, r)$, avec $0 \leq k \leq n$.
- $GR(p^n, r)$ est un anneau local d' idéal maximal $pGR(p^n, r)$
- $R \subseteq GR(p^n, r) \Rightarrow R = GR(p^n, s)$, où s divise r.
- Si s divise r, alors $GR(p^n, s) \subseteq GR(p^n, r)$

Anneaux à chaînes finis

Un anneau R est appelé anneau à chaîne si l'ensemble de ses idéaux est totalement ordonné par l'inclusion.

Caractérisation

Les ASSE :

1. R est un anneau à chaîne fini
2. R est un anneau local et son idéal maximal est principal,
3. R est local et principal.

Preuve :

- x et y générateurs de $\mathfrak{m}$, alors $x \notin < y >$ et $y \notin < x >$ et donc $< x > \nsubseteq < y >$ et $< y > \nsubseteq < x >$.
- R est un anneau fini et local, $\exists e \in \mathbb{N} \setminus \{0\}$ tel que $\mathfrak{m}^e =< \gamma^e >= 0$. I étant un idéal propre non-nul de R, : $I \subseteq < \gamma^k >$ et $I \nsubseteq < \gamma^{k+1} >$.
  Cela entraîne $< \gamma^{k+1} > \subsetneq I + < \gamma^{k+1} > \subseteq < \gamma^k >$ i.e.
  $I + < \gamma^{k+1} >=< \gamma^k >$.
  Lemme de Nakayama $\Rightarrow I =< \gamma^k >$.

□

Soit $(R, \gamma, e, \mathbb{F}_q)$ un anneau à chaîne fini.

- $< 0 >=< \gamma^e > \subsetneq < \gamma^{e-1} > \subsetneq \ldots \subsetneq < \gamma^0 >= R.$

Soit $(R, \gamma, e, \mathbb{F}_q)$ un anneau à chaîne fini.

- $< 0 >=< \gamma^e > \subsetneq < \gamma^{e-1} > \subsetneq \ldots \subsetneq < \gamma^0 >= R$.
- $r = \sum_{i=0}^{e-1} r_i \gamma^i$ où $r_i \in T_R = \{0, 1, \xi, ..., \xi^{p^r-2}\}$ et ξ l'antécédent par $\bar{}$ de l' élément primitif de $\mathbb{F}_q$.
- $|\gamma^j R| = |T_R|^{e-j} = p^{r(e-j)}$.
- $| < \gamma^i > | = |\mathbb{F}_{p^r}|^{e-i} = p^{r(e-i)}, \ \forall\ 0 \leq i \leq e$.
- $|R| = p^{re}$.

Soit $(R, \gamma, e, \mathbb{F}_q)$ un anneau à chaîne fini.

- $< 0 >=< \gamma^e > \subsetneq < \gamma^{e-1} > \subsetneq \ldots \subsetneq < \gamma^0 >= R$.
- $r = \sum_{i=0}^{e-1} r_i \gamma^i$ où $r_i \in T_R = \{0, 1, \xi, ..., \xi^{p^r-2}\}$ et ξ l'antécédent par $\bar{}$ de l' élément primitif de $\mathbb{F}_q$.
- $|\gamma^j R| = |T_R|^{e-j} = p^{r(e-j)}$.
- $| < \gamma^i > | = |\mathbb{F}_{p^r}|^{e-i} = p^{r(e-i)}, \ \forall\ 0 \leq i \leq e$.
- $|R| = p^{re}$.
- $U(R) = T_R^* \times (1 + \gamma R)$, où $T_R^* =< \xi >$ est un sous groupe de $U(R)$ d'ordre $p^r - 1$.

Extension de $GR(p^n, r)$

Théorème

Soient R un anneau à chaîne fini, de caractéristique p^n, et e l'indice de nilpotence de l'idéal maximal $< \gamma >$ de R. Alors il existe des entiers t et s tels que :

$$R \cong GR(p^n, r)[X]/(g(X), p^{n-1}X^t),$$

où $t = e - (n-1)s > 0$ et $g(X)$ est un polynôme de Eisensten de degré s sur $GR(p^n, r)$, i.e. : $g(X) = X^s + p(a_{s-1}X^{s-1} + ... + a_1X + a_0)$ avec a_0 inversible dans $GR(p^n, r)$.

▷ Un anneau principal est isomorphe à un produit fini d'anneaux à chaine finis.

Méthode de Graeffe

On souhaite factoriser $x^n - 1 \in \mathbb{Z}_4[x]$. Soit $h(x)$ un facteur irreductible de $x^n + 1 \in \mathbb{F}_2[x]$.

1. On pose $h(x) = e(x) + o(x)$, où $e(X)$ est un polynôme ne contenant que des puissances paires et $o(X)$ que des puissances impaires.
2. Alors $g(x)$ est un facteur irréductible de $x^n - 1 \in \mathbb{Z}_4[x]$ tel que $\mu(g(x)) = h(x)$ et $g\left(x^2\right) = \pm\left(e(x)^2 - o(x)^2\right)$.
   Alors $h\left(X^2\right) = \pm\left(e^2(X) - d^2(X)\right)$.

Anneaux de Frobenius

- Socle de $\mathcal{A}$: la somme de tous les $\mathcal{A}$-sous-modules (idéaux) minimaux de $\mathcal{A}$. On le note $Soc(\mathcal{A})$.
- On dit que $\mathcal{A}$ est un anneau de **Frobenius** si $R/J(\mathcal{A}) \cong Soc(\mathcal{A})$ (comme $\mathcal{A}$-modules)

Anneaux de Frobenius

- Socle de $\mathcal{A}$: la somme de tous les $\mathcal{A}$-sous-modules (idéaux) minimaux de $\mathcal{A}$. On le note $Soc(\mathcal{A})$.
- On dit que $\mathcal{A}$ est un anneau de **Frobenius** si $R/J(\mathcal{A}) \cong Soc(\mathcal{A})$ (comme $\mathcal{A}$-modules)

▷ Les corps finis, les anneaux à chaines finis sont des anneaux de Frobenius.

▷ La classe des anneaux de Frobenius finis est la classe d'anneaux finis la mieux indiquée pour la théorie algébrique des codes.

- McDonald, Bernard R. *Finite Rings with Identity*, Dekker, New York, 1974.
- Wan, Zhe-Xian *Lectures on finite fields and Galois Rings*, World Scientific , 2003.
- Bini, G. AND Flamini, F. *Finite Commutative Rings and Their Applications*, Springer, 2002.
- Huffman, W. C. AND Pless, V. , *Fundamentals of Error-Correcting Codes*, Cambridge University Press, New-York, 2003.
- Wood, Jay A. *Duality for modules over finite rings and applications to coding theory*, Amer. J. Math, 121 (1999), pp 555-575.