Théorie et codage de l'information

Éléments d'algèbre discrète

- Chapitre 5 -

Algèbre discrète

Mise en oeuvre pour le codage de canal

D'après le second théorème de Shannon, le codage de canal permet de réduire arbitrairement les probabilités d'erreur de transmission. Cependant, aucune preuve constructive de celui-ci n'existe.

▷ **De multiples techniques de codage ont été proposées**

Les héritages d'algèbre discrète sont nombreux :

→ représentation vectorielle des mots

→ addition, produit

→ distance

→ ...

Structures algébriques

Groupes

Définition 1 (loi de composition interne). *On appelle* **loi de composition interne** *à un ensemble E une application $\top$ de $E \times E$ dans E :*

$$(x, y) \longmapsto z = x \top y.$$

On appelle **élément neutre** *de la loi $\top$ un élément e de E tel que :*

$$\forall x \in E, \quad x \top e = e \top x = x.$$

La loi $\top$ est **commutative** *si :*

$$\forall\, (x, y) \in E \times E, \quad x \top y = y \top x.$$

Structures algébriques

Groupes

Définition 2 (groupe). *Un ensemble G muni d'une loi de composition interne $\top$ est appelé* **groupe** *si :*

– *la loi $\top$ est* **associative**, *c'est-à-dire*

$$\forall\,(x,y,z)\in G^3,\quad (x\top y)\top z = x\top(y\top z)\,,$$

– *la loi $\top$ admet un* **élément neutre** *e dans G,*

– *tout élément de G admet un* **inverse** *pour la loi $\top$, c'est à dire*

$$\forall x\in G,\quad \exists x'\in G\quad :\quad x\top x' = x'\top x = e.$$

Notation. Lorsque la loi $\top$ est notée multiplicativement par $\times$, x' est souvent représenté par x^{-1} et e par 1. Lorsque la loi est notée additivement par $+$, x' est souvent représenté par $-x$ et e par 0.

Structures algébriques

Groupes

Définition 3. *On peut distinguer les différents types de groupes suivants.*

- *Si la loi $\top$ est commutative, le groupe $(G, \top)$ est dit* **abélien** *ou* **commutatif**.
- *S'il existe un élément x de G tel que*

$$\forall y \in G, \quad \exists i \in \mathbb{N} \quad : \quad y = x^i,$$

le groupe est dit **cyclique**. *On note $< x >$ le générateur du groupe. Ci-dessus, nous avons utilisé la notation $x^0 = e$ et, pour $i \neq 0$,*

$$x^i = \underbrace{x \top x \top \ldots \top x}_{i \text{ fois}}.$$

Définition 4. *Soit G un groupe fini et $x \in G$. On appelle* **ordre** *de x le plus petit entier positif n tel que $x^n = e$.*

Exemple. $(\mathbb{Z}, +)$ est un groupe abélien.

Exercice 1. Montrer que $\{0, 1, 2\}$ muni de la loi $+$ définie par

«$i + j$ = reste de la division par 3 de la somme $(i + j)$ calculée dans $\mathbb{Z}$»

est un groupe abélien fini de cardinal 3.

Structures algébriques

Anneaux

Définition 5 (anneau). *On appelle* **anneau** *un ensemble A muni de deux lois de composition interne $+$ et $\times$ telles que :*

- *$(A, +)$ est un* **groupe commutatif**,
- *la loi $\times$ est* **associative**,
- *la loi $\times$ est* **distributive** *par rapport à $+$, c'est à dire*

$$\forall\,(x, y, z) \in A^3,\ x \times (y + z) = x \times y + x \times z \text{ et } (x + y) \times z = x \times z + y \times z.$$

Vocabulaire.

- Si la loi $\times$ est commutative, l'anneau A est dit **commutatif**.
- S'il existe un élément neutre, noté 1, pour la loi $\times$, l'anneau A est dit **unitaire**.
- Si quels que soient x et y des éléments de A, on a

$$x \times y = 0 \quad \Rightarrow \quad x = 0 \text{ ou } y = 0,$$

l'anneau A est dit **intègre** ou **anneau d'intégrité**.

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

Exercice 2. Reprenons l'exercice 1. Munissons $(\{0,1,2\}, +\}$ d'une loi «multiplicative» commutative définie par :

$$0 * i = 0,\ 1 * i = i,\ 2 * 2 = 1, \qquad i \in \{0,1,2\}$$

Montrer que $(\{0,1,2\}, +, *)$ est un anneau commutatif unitaire et intègre.

Structures algébriques

Corps

Définition 6 (corps). *On appelle corps un ensemble* $\mathbf{K}$ *muni de deux lois de composition interne* $+$ *et* $\times$ *telles que :*

- $(\mathbf{K}, +, \times)$ *est un anneau ;*
- *Si on note* e *l'élément neutre de la loi* $+$*, alors* $(\mathbf{K} \setminus \{e\}, \times)$ *est un groupe. Ceci implique que tout élément de* $\mathbf{K}$ *admet un inverse pour* $\times$*, à l'exception de* e*.*

▷ Un corps est donc un anneau dans lequel tout élément non-nul est inversible.

Vocabulaire.

- Un corps est dit **fini** s'il admet un nombre fini d'éléments. Un corps fini à q éléments sera noté $\mathbf{F}_q$.
- Le corps $\mathbf{K}$ est dit **commutatif** si la loi $\times$ est commutative.

Structures algébriques

Caractéristique d'un corps

Définition 7 (caractéristique). *Soit* $(\mathbf{K}, +, \times)$ *un corps. Soit* r *le plus petit entier* k *tel que*

$$0 = \underbrace{1 \ + \ \ldots \ + \ 1}_{k \text{ fois}}.$$

r *est appelé* **caractéristique** *du corps* $\mathbf{K}$.

Propriété 1. *La caractéristique d'un corps est zéro ou un nombre premier.*

L'anneau $\mathbb{Z}/n\mathbb{Z}$

Rappels sur les entiers relatifs

Théorème 1 (division euclidienne). *Soit $(a, b) \in \mathbb{Z} \times \mathbb{Z}$ tel que $b \neq 0$. Il existe un unique couple $(q, r) \in \mathbb{Z} \times \mathbb{Z}$ tel que $a = bq + r$ et $0 \leq r < |b|$, où $|b|$ désigne la valeur absolue de b.*
r est le **reste** *et q le* **quotient** *de la division de a par b dans $\mathbb{Z}$.*

Théorème 2 (Bezout). *Soient a et b deux éléments non nuls de $\mathbb{Z}$. Les éléments a et b sont premiers entre eux si et seulement s'il existe u et v de $\mathbb{Z}$ tels que*

$$ua + vb = 1.$$

L'anneau $\mathbb{Z}/n\mathbb{Z}$

La congruence

Définition 8 (congruence). *Soit n un entier relatif. Si a et b sont deux entiers relatifs tels que n divise $b-a$, ou $b-a$ est multiple de n, on dit que b est* **congru à** *a* **modulo** *n. On note :*

$$b \equiv a \ (mod\ n) \ \ ou\ b \equiv a\ [n].$$

La relation définie est une congruence modulo n.

L'anneau $\mathbb{Z}/n\mathbb{Z}$

La congruence

Proposition 1. *La relation de congruence est une* **relation d'équivalence**, *c'est-à-dire qu'elle est*

symétrique : $b \equiv a \ (mod\ n) \Longrightarrow a \equiv b \ (mod\ n)$

reflexive : $a \equiv a \ (mod\ n)$

transitive : $b \equiv a \ (mod\ n)$ *et* $c \equiv b \ (mod\ n) \Longrightarrow c \equiv a \ (mod\ n)$

Notation. La classe d'équivalence de a pour cette relation, i.e. l'ensemble des entiers congrus à a modulo n, est la classe de congruence de a modulo n. Elle sera éventuellement notée dans la suite $\bar{a}$.

Remarque. L'ensemble des classes de congruence forme une partition de $\mathbb{Z}$.

L'anneau $\mathbb{Z}/n\mathbb{Z}$

La congruence

Proposition 2. *Les éléments a et b sont congrus modulo n si et seulement s'ils ont même reste dans la division euclidienne par n.*

Proposition 3. $(0, 1, \ldots, n-1)$ *constitue un système de représentants de la congruence modulo n, chacun de ces entiers représentant une classe.*

Proposition 4. *La relation de congruence est compatible avec les opérations de $\mathbb{Z}$. Si $a \equiv b \ (mod\ n)$ et $a' \equiv b' \ (mod\ n)$, alors*

$$\begin{aligned} a + a' &\equiv b + b' \ (mod\ n) \\ aa' &\equiv bb' \ (mod\ n) \end{aligned}$$

L'anneau $\mathbb{Z}/n\mathbb{Z}$

Définition

Définition 9. *$\mathbb{Z}/n\mathbb{Z}$ est l'ensemble des* **classes de congruence** *modulo n.*

Notation. La classe d'un entier a sera notée $\overline{a}$. Dans ces conditions, l'ensemble des éléments de $\mathbb{Z}/n\mathbb{Z}$ peut être écrit sous la forme $\overline{0}$, $\overline{1}$, $\ldots$, $\overline{n-1}$.

Définition 10 (opérations). *Soient $\overline{a}$ et $\overline{b}$ deux classes de $\mathbb{Z}/n\mathbb{Z}$. On définit l'addition et la multiplication dans $\mathbb{Z}/n\mathbb{Z}$ ainsi :*

$$\begin{aligned} \overline{a}+\overline{b} &= \overline{a+b} \\ \overline{a}\overline{b} &= \overline{ab} \end{aligned}$$

L'anneau $\mathbb{Z}/n\mathbb{Z}$

Propriété

Proposition 5. *Muni des deux opérations définies précédemment, $\mathbb{Z}/n\mathbb{Z}$ est un anneau commutatif unitaire.*

Exemple. Les tables d'addition et de multiplication de $\mathbb{Z}/5\mathbb{Z}$ sont données par :

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\times$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Exercice 3. Dans $\mathbb{Z}/13\mathbb{Z}$, par quoi peut-on remplacer $\overline{9}$, $\overline{29}$ et $\overline{-10}$?

L'anneau $\mathbb{Z}/n\mathbb{Z}$

Corps premier

Proposition 6. *Un élément $\overline{a}$ de l'anneau $\mathbb{Z}/n\mathbb{Z}$ est inversible si et seulement si $pgcd(a, n) = 1$, c'est à dire a premier avec n.*

Proposition 7. *$\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est premier.*

Notation. Si $p \in \mathbb{N}$ est un nombre premier, le corps $\mathbb{Z}/p\mathbb{Z}$ est noté $\mathbf{F}_p$. On dit qu'il est un **corps premier**.

Polynômes

Rappels

Notation. Soit $\mathbf{K}$ un corps commutatif. On note $\mathbf{K}[X]$ l'anneau des polynômes à coefficients dans $\mathbf{K}$.

Proposition 8. $\mathbf{K}[X]$ *est un anneau commutatif intègre.*

Remarque. $\mathbf{K}$ peut être identifié à l'ensemble des polynômes constants de $\mathbf{K}[X]$.

Polynômes

Rappels

Théorème 3 (division euclidienne). *Soient $A \in \mathbf{K}[X]$ et $B \in \mathbf{K}[X]$, $B \neq 0$. Il existe un unique couple (Q, R) de $\mathbf{K}[X] \times \mathbf{K}[X]$ tel que*

$$A = BQ + R$$

avec $d^\circ(R) < d^\circ(B)$ ou $R = 0$. Le polynôme Q est appelé le quotient et R le reste de la division euclidienne de A par B.

Remarque. D'un point de vue pratique, on pose la division suivant les puissances décroissantes. La division euclidienne dans $\mathbf{K}[X]$ est alors analogue à celle de $\mathbb{Z}$.

Polynômes

Rappels

Exercice 4. Effectuer dans $\mathbb{R}[X]$ la division euclidienne de $A(X) = 3X^5 + 2X^4 - 2X^3 - X^2 + 1$ et $B(X) = X^2 - 1$.

Exercice 5. Effectuer dans $\mathbf{F}_{31} = \mathbb{Z}/31\mathbb{Z}$ la division euclidienne de $A(X) = 12X^7 + 5X^3 - 21X^2$ et $B(X) = X^4 + X + 1$.

Polynômes

Rappels

Définition 11. *Soient A et B deux éléments de $\mathbf{K}[X]$ et D un polynôme unitaire $\mathbf{K}[X]$, i.e. dont le coefficient du terme de plus haut degré est égal à l'unité. On dit que D est* **le plus grand commun diviseur** *des polynômes A et B si*
– *D divise A et D divise B,*
– *$G \in \mathbf{K}[X]$ divise A et B entraîne G divise D.*

Définition 12. *Un polynôme P non nul de $\mathbf{K}[X]$ est dit* **irréductible** *ou* **premier** *sur $\mathbf{K}$ si, dans $\mathbf{K}[X]$, ses seuls diviseurs sont les polynômes constants non nuls et les produits de P par des constantes non nulles.*

Définition 13. *Deux éléments non nuls de $\mathbf{K}[X]$ sont premiers entre eux si et seulement si leur pgcd vaut 1.*

Polynômes

Rappels

Calcul pratique du pgcd. A l'aide de la division euclidienne, on effectue les divisions successives

$$A = BQ_1 + R_1 \text{ avec } d^\circ(R_1) < d^\circ(B)$$
$$B = R_1Q_2 + R_2 \quad \dots$$

Le pgcd est le dernier reste unitaire non nul.

Exercice 6. Dans $\mathbf{F}_2[X]$, calculer le PGCD des polynômes suivants :
$A(X) = X^{16} + X^{12} + X^{11} + X^8 + X^4 + X + 1$
$B(X) = X^{13} + X^9 + X^8 + X^5 + X + 1.$

Polynômes

L'anneau des polynômes modulo P

Nous allons dans un premier temps définir une sous-structure particulière de la structure d'anneau appelée *idéal*.

Définition 14 (Idéal). *Soit A un anneau et $\mathcal{I}$ une partie non vide de A. On dit que $\mathcal{I}$ est* **un idéal** *de A si :*
– *x et $y \in \mathcal{I} \Rightarrow x - y \in \mathcal{I}$, c'est à dire $(\mathcal{I}, +)$ constitue un sous-groupe de $(A, +)$.*
– *$\forall a \in A, \forall x \in \mathcal{I}$, $a \times x \in \mathcal{I}$ et $x \times a \in \mathcal{I}$ (idéal bilatère).*

Exemple. Soit A un anneau commutatif et $x \in A$. L'ensemble des multiples de x, noté $< x >$ ou xA, est un idéal.

Polynômes

L'anneau des polynômes modulo P

De même que nous avons défini les $\mathbb{Z}/n\mathbb{Z}$, nous allons définir des *anneaux quotients* de polynômes.

Théorème 4. *Toute* **relation d'équivalence** *sur un anneau A, compatible avec les opérations, est du type $(x - y) \in \mathcal{I}$ où $\mathcal{I}$ est un idéal. Ceci signifie que $\mathcal{I}$ est en fait la classe de l'élément nul de A.*

Remarque. Par **compatible avec les opérations**, nous entendons

$$x\mathcal{R}y \text{ et } x'\mathcal{R}y' \Longrightarrow (x + x')\mathcal{R}(y + y') \text{ et } xx'\mathcal{R}yy',$$

où $\mathcal{R}$ désigne la relation d'équivalence.

Polynômes

L'anneau des polynômes modulo P

Les notations utilisées ici sont les mêmes que celles introduites pour $\mathbb{Z}/n\mathbb{Z}$.

Notations.

- Toute relation de ce type s'appelle une congruence modulo $\mathcal{I}$.
- $x - y \in \mathcal{I}$ se note $x \equiv y \ (mod\, \mathcal{I})$ et se lit x **congru à** y **modulo** $\mathcal{I}$.
- L'ensemble des classes d'équivalence de A pour cette relation ou **ensemble quotient** est noté $A/\mathcal{I}$.
- La classe de x est notée $\overline{x}$. On peut remarquer que $\overline{x}$ est donnée par $x + \mathcal{I} = \{z = x + y \ : \ y \in \mathcal{I}\}$.

Polynômes

L'anneau des polynômes modulo P

Théorème 5. *Soit* $\mathbf{K}$ *un corps commutatif. Soit* $\mathcal{I}$ *un sous-ensemble de* $\mathbf{K}[X]$*. Les 2 assertions suivantes sont équivalentes :*

- *L'ensemble* $\mathcal{I}$ *est un idéal de* $\mathbf{K}[X]$*.*
- *Il existe un polynôme* P *de* $\mathbf{K}[X]$ *tel que* $\mathcal{I}$ *est l'ensemble des multiples de* P *dans* $\mathbf{K}[X]$*.*

Définition 15 (équivalence modulo P). *Soit* P *un élément de* $\mathbf{K}[X]$*. Deux polynômes* A *et* B *de* $\mathbf{K}[X]$ *sont dit équivalents modulo* P *si et seulement si* $A - B$ *est un multiple de* P*.*

Notation. On note $A \equiv B \pmod{P}$.

Polynômes

L'anneau des polynômes modulo P

Proposition 9. *On a $A \equiv B \,(mod\, P)$ si et seulement si les polynômes A et B ont le même reste dans la division par le polynôme P. Dans ces conditions, pour tout C de $\mathbf{K}[X]$, les équivalences suivantes sont satisfaites :*

$$\begin{aligned} A + C &\equiv B + C \,(mod\, P) \\ AC &\equiv BC \,(mod\, P). \end{aligned}$$

Polynômes

L'anneau des polynômes modulo P

Corollaire 1. *Soit S un polynôme non nul de $\mathbf{K}[X]$ de degré n, et soit $\mathcal{I} =< S >$ l'idéal engendré par S. Soit $\mathcal{P}_n$ l'ensemble des polynômes non nuls de degré strictement inférieur à n c'est-à-dire l'ensemble des polynômes sur $\mathbf{K}$ de la forme $a_0 + a_1X + \ldots + a_{n-1}X^{n-1}$. Alors :*

- *La classe de A pour l'équivalence modulo S est $A + \mathcal{I}$. C'est aussi $R + \mathcal{I}$ où R est le reste de la division de A par S.*
- *L'application $\phi : \mathbf{K}[X]/\mathcal{I} \longrightarrow \mathcal{P}_n$ définie par $\phi(A + \mathcal{I}) = R$ où R est le reste de la division de A par S est une bijection.*
- *Le cardinal de $\mathbf{K}[X]/\mathcal{I}$ est $|\mathbf{K}|^n$.*

$\triangleright$ On définit ainsi un anneau commutatif qui sera noté $\mathbf{K}[X]/ < S >$.

Polynômes

L'anneau des polynômes modulo P

En pratique, dans $\mathbf{K}[X]/ < S >$, les polynômes et les résultats des opérations ordinaires sont remplacés par leurs restes dans la division par S.

Exemple. Prenons le cas $\mathbf{K} = \mathbb{Z}/2\mathbb{Z}$ et considérons le polynôme $S = X^2 + X + 1$. Les différents restes possibles de la division par S sont 0, 1, $A = X$ et $B = X + 1$. Les tables des opérations pour $\mathbf{K}[X] / < X^2 + X + 1 >$ sont les suivantes :

$+$	0	1	A	B
0	0	1	A	B
1	1	0	B	A
A	A	B	0	1
B	B	A	1	0

$\times$	0	1	A	B
0	0	0	0	0
1	0	1	A	B
A	0	A	B	1
B	0	B	1	A

Polynômes

L'anneau des polynômes modulo P

Théorème 6. *L'anneau* $\mathbf{K}[X] / < S >$ *est* **un corps** *si et seulement si le polynôme* S *est irréductible sur* $\mathbf{K}$*, c'est-à-dire si et seulement si les seuls diviseurs de* S *à coefficients dans* $\mathbf{K}$ *sont les constantes non nulles et lui même.*

$\triangleright$ **on parle alors de corps quotient**

Remarque. Si s est le degré de S et q le cardinal de $\mathbf{K}$ (en supposant $\mathbf{K}$ fini), alors $\mathbf{K}[X] / < S >$ contient q^s éléments.

Les corps finis

Propriétés générales

Proposition 10. *Tout corps fini est isomorphe à un corps* $\mathbf{K}[X]/ < S >$ *où* $\mathbf{K} = \mathbb{Z}/p\mathbb{Z}$ *avec* p *premier et* S *irréductible sur* $\mathbf{K}$.

Notation. Un corps fini à q éléments est tel que $q = p^r$, avec p premier. On le note $\mathbf{F}_q$ ou $CG(q)$ (Corps de Galois à q éléments).

Les corps finis

Construction d'un corps fini

Afin de construire un corps fini, on utilise les propriétés suivantes :

Propriété 2 (corps finis). *Soit $\mathbf{F}_q$ un corps fini à $q = p^r$ éléments. On a :*

- *Si $\mathbf{F}_q = \mathbf{F}_p[X]/ < S >$, avec p premier et S irréductible sur $\mathbf{F}_p$, alors le polynôme S possède au moins une racine dans $\mathbf{F}_q$.*
- *Le groupe $(\mathbf{F}_q, \times)$ est un groupe cyclique, c'est-à-dire que les éléments non nuls de $\mathbf{F}_q$ sont les puissances d'un même élément générateur. Un tel élément s'appelle élément primitif.*
- *Soit α un élément primitif de $\mathbf{F}_q$, avec $q = p^r$. Alors, tout élément de $\mathbf{F}_q$ s'écrit de manière unique comme une combinaison linéaire de $1, \alpha, \alpha^2, \ldots, \alpha^{r-1}$. Autrement dit, si l'on considère $\mathbf{F}_q$ comme un $\mathbf{F}_p$ espace vectoriel, alors $\{1, \alpha, \alpha^2, \ldots, \alpha^{r-1}\}$ en est une base.*

Les corps finis

Construction d'un corps fini

Soit S un polynôme irréductible sur $\mathbf{F}_p$, unitaire et de degré r :

$$S = x^r + a_{r-1}x^{r-1} + \cdots + a_1 x + a_0.$$

Supposons que S possède comme racine dans $\mathbf{F}_q$ un élément primitif α de $\mathbf{F}_q$. Puisque $f(\alpha) = 0$, il vient :

$$\alpha^r = -a_{r-1}\alpha^{r-1} - \cdots - a_1\alpha - a_0.$$

En multipliant l'égalité précédente par α, puis en remplaçant α^r par son expression, on obtient α^{n+1} sous la forme :

$$\alpha^{r+1} = -b_{r-1}\alpha^{r-1} - \cdots - b_1\alpha - b_0,$$

puis $\alpha^{r+2}, \ldots, \alpha^{p^r-2}$ comme combinaisons linéaires des éléments de la base $1, \alpha, \ldots, \alpha^{r-1}$. On obtient ainsi une expression de tous les éléments de $\mathbf{F}_q$ permettant d'effectuer les calculs.