ARITHMÉTIQUE ET ALGÈBRE POUR LES ÉLÈVES INGÉNIEURS

Formation HUGo

Table des matières

Chapitre 1

Propriétés des entiers

Ce chapitre aborde des notions que l'on rencontre avant d'entrer en école d'ingénieurs : notion de divisibilité, nombre premier, PGCD et PPCM ainsi que la notion d'idéal. Il introduit également une vision algorithmique. Comment effectuer la division euclidienne efficacement ? Comment calculer un PGCD ou un PPCM ? Ces rappels basiques sont utiles pour vous remémorer les définitions, la manière d'écrire une preuve et comprendre un algorithme.

L'ensemble des nombres entiers est noté $\mathbb{Z}$:

$$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\},$$

et celui des entiers $n \geq 0$ est noté $\mathbb{N}$.
Dans la suite, les lettres désigneront toujours des entiers quelconques, sauf précision : ainsi, $a > 0$ signifiera $\forall a \in \mathbb{Z}$ et $a > 0$, et « il existe a tel que... » fera référence à un entier a vérifiant une certaine condition.

1.1 Division entière

Soit $a, b \in \mathbb{Z}$, b divise a si il existe $c \in \mathbb{Z}$ tel que $a = bc$. L'élément b est alors un **diviseur** de a et on écrit $b|a$.
Exemple. $-6|30 \;\; 190|0 \;\; 11|759$
Notation. Il ne faut pas confondre la notation $b|a$ qui est un booléen (VRAI ou FAUX) de a et b/a qui est la valeur de la division de b par a. Par exemple, $3|6$ est vrai alors que $3|4$ est faux, et on a $3/6 = 0,5$ et $3/4 = 0,75$.

Théorème 1.1.1. *Quels que soient les entiers a, b, c, on a :*

a) $1|a$, $a|a$, $a|0$.

b) $0|a$ *SSI* $a = 0$.

c) Si $a|b$ *et* $b|c$, *alors* $a|c$.

d) Si $a|b$ *et* $a|c$*, alors* $a|(bx+cy)$*,* $\forall x, y \in \mathbb{Z}$*.*

e) $a|b$ *et* $b|a$ *SSI* $a = \pm b$*.*

Théorème 1.1.2. *(Division entière) Si* $a, b \in \mathbb{Z}$*,* $b \geq 1$*, alors il existe un unique couple* $(q, r) \in \mathbb{Z}^2$ *tel que*

$$a = bq + r \quad \textit{avec } 0 \leq r < b$$

q *est appelé le* **quotient** *et* r *le* **reste** *de la division de* a *par* b*.*

$$\begin{cases} r = a \mod b \\ q = \lfloor a/b \rfloor \end{cases}$$

Exemple. Si $a = 73$ et $b = 17$, alors :

$$\begin{cases} q = 4,\ r = 5, \\ \lfloor 73/17 \rfloor = 4, \\ 73 \mod 17 = 5\,. \end{cases}$$

Un entier c est un **diviseur commun** à a et b si $c|a$ et $c|b$.

1.1.1 Tests de divisibilité

1. Un nombre est divisible par 2^k si ses k derniers chiffres sont divisibles par 2^k.
2. Un nombre est divisible par 5^k si ses k derniers chiffres sont divisibles par 5^k.
3. Un nombre est divisible par 3 ou 9 si la somme de ses chiffres est divisible par 3 ou par 9.

Exemple. 2125 est divisible par 5^k, pour $k = 3$ et 1638 est divisible par 9.

1.2 Nombre premier

Un entier $p \geq 2$ est dit premier si ses seuls diviseurs positifs sont 1 et p. Sinon on dit que le nombre est composé.

Théorème 1.2.1. *(Théorème fondamental de l'arithmétique) Tout entier* $n \geq 2$ *admet une factorisation unique comme produit de puissances de nombres premiers.*

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$$

1.3 Idéaux, PGCD et PPCM

Un **idéal** de $\mathbb{Z}$ est un ensemble non vide d'entiers qui est clos par addition et par multiplication par un entier arbitraire .
Définition. Un ensemble $I \subseteq \mathbb{Z}$ non vide est un idéal si et seulement si pour tout $a, b \in I$ et pour tout $z \in \mathbb{Z}$, $a + b \in I$ et $az \in I$.
Remarques :

1. Si $a \in I$ alors $-a \in I$
2. $0 \in I$ car $a + (-a) \in I$
3. Si $1 \in I$ alors $I = \mathbb{Z}$.

Définition. $a\mathbb{Z} := \{az : z \in \mathbb{Z}\}$ est l'ensemble des multiples de a. $a\mathbb{Z}$ est un idéal engendré par a. Tous les idéaux de la forme $a\mathbb{Z}$ sont appelés **idéaux principaux**. Considérons maintenant $a_1\mathbb{Z}+a_2\mathbb{Z}+\cdots+a_k\mathbb{Z} := \{a_1z_1+\cdots+a_kz_k : z_1, \cdots, z_k \in \mathbb{Z}\}$. Cet objet est un idéal engendré par les a_i. C'est le plus petit idéal contenant les a_i.
Exemple.

— $a = 3,\ aZ = \{\ldots, -9, -6, -3, 0, 3, 6, \ldots\}$
— $a_1 = 3, a_2 = 5,\ a_1\mathbb{Z} + a_2\mathbb{Z} = \mathbb{Z}$ car $2a_1 - a_2 = 1$ (voir Remarque 3)
— $a_1 = 4, a_2 = 6,\ a_1\mathbb{Z} + a_2\mathbb{Z} = 2\mathbb{Z}$.

Théorème 1.3.1. *Pour tout idéal $I \subset \mathbb{Z}$, il existe un unique entier positif d tel que $I = d\mathbb{Z}$.*

Pour $a, b \in I$, on appelle $d \in \mathbb{Z}$ un diviseur commun de a et b si $d|a$ et $d|b$. L'élément d est le PGCD de a et b si $d \geq 0$ et tous les autres diviseurs communs de a et b divisent d.

Théorème 1.3.2. *Pour tout $a, b \in \mathbb{Z}$, il existe un unique PGCD d de a et b et de plus $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$.*

Remarque : $PGCD(a, 0) = |a|$.

Calcul du PGCD : En pratique, on utilise l'algorithme d'Euclide :
Calcul de $PGCD(a, b)$
$R0 := |a|$;
$R1 := |b|$; $\quad (b \neq 0)$
Tantque $R1 > 0$ Faire
$R := Reste\_Division(R0, R1)$;
$R0 := R1$;
$R1 := R$;
En sortie $R1 = 0$, et $R0 = pgcd(a, b)$.

Théorème 1.3.3. *(Bézout)*
$\forall a, b \in \mathbb{Z}, \exists s, t \in \mathbb{Z}$ *tel que* $as + bt = PGCD(a, b)$.
Si $PGCD(a, b) = 1$*,* a *et* b *sont dits premiers entre eux. Il existe* $s, t \in \mathbb{Z}$ *tel que* $as + bt = 1$.

Exemple. $PGCD(12, 42) = 6$ et on a
$(-3).12 + 1.42 = 6$
$4.12 + (-1).42 = 6$
Remarque : A partir d'un couple solution (x_0, y_0), il est possible d'obtenir toutes les autres solutions de la manière suivantes : $a(x_0 - k\frac{b}{d}) + b(y_0 + k\frac{a}{d}) = d$.

Théorème 1.3.4. *(Conséquence de la factorisation unique)*
Il existe une infinité de nombres premiers.

1.4 Algorithme d'Euclide étendu

Soit a er b deux entiers positifs et d leur PGCD. Le théorème de Bézout dit qu'il existe des entiers s et t tels que $as + bt = 1$. Ces entiers s et t peuvent être efficacement calculés grâce à l'algorithme d'Euclide étendu :
Algorithme d'Euclide étendu
Entrée : $a,\ b$ entiers positif
Sortie : d entier positif et $s,\ t$ entiers tels que $d = pgcd(a, b)$ et $d = as + bt$
$d := a, d' := b, s := 1, t := 0, s' := 0, t' := 1$
tant que $(d' \neq 0)$ faire
$q := d \div d'$
$x := d, y := s, z := t$
$d := d', s := s', t := t'$
$d' := x - q * d', s' = y - q * s', t' = z - q * t'$
Renvoyer (d, s, t)

Exemple. Calculer s et t tels que $53.s + 39.t = 1$. Le déroulement de l'algorithme donne

q	d	s	t	d'	s'	t'	x	y	z
	53	1	0	39	0	1			
1	39	0	1	14	1	-1	53	1	0
2	14	1	-1	11	-2	3	39	0	1
1	11	-2	3	3	3	-4	14	1	-1
3	3	3	-4	2	-11	15	11	-2	3
1	2	-11	15	1	14	-19	3	3	-4
2	**1**	**14**	**-19**	0	-39	53	2	-11	15

En pratique, on peut aussi exécuter l'algorithme d'Euclide pour calculer le PGCD de 39 et 53, puis réécrire les restes en fonction de ces deux nombres.

$$
\begin{array}{lcl}
53 = 1.39 + 14 & \Rightarrow & 14 = 53 - 39 \\
39 = 2.14 + 11 & \Rightarrow & 11 = 39 - 2.14 = -2.53 + 3.39 \\
14 = 1.11 + 3 & \Rightarrow & 3 = 14 - 1.11 = 3.53 - 4.39 \\
11 = 3.3 + 2 & \Rightarrow & 2 = 11 - 3.3 = -11.53 + 15.39 \\
3 = 1.2 + 1 & \Rightarrow & 1 = 3 - 1.2 = 14.53 - 19.39 \\
2 = 2.1 + 0 &&
\end{array}
$$

On obtient $14.53 - 19.39 = 1$
Le nombre de boucles de l'algorithme est le même que celui de l'algorithme d'Euclide simple. Par contre, le nombre d'opérations est plus important dans chaque boucle, puisqu'il faut calculer les restes en fonction de 39 et 53.

Chapitre 2

Congruences

2.1 Classes d'équivalence

Soit n un entier positif.

Définition. Rappelons la relation entre les entiers a et b : a est congru à b modulo n, ce qui s'écrit $a \equiv b \pmod{n}$, si $n|(a-b)$; n est le **module** de la congruence.

Exemples.

$$\begin{array}{rlll} 24 \equiv 9 \pmod{5} & \text{puisque} & 24-9 &= 3\,.\,5\,. \\ -11 \equiv 17 \pmod{7} & \text{puisque} & -11-17 &= -4\,.\,7\,. \end{array}$$

Propriétés de la congruence. $\forall\, a, a_1, b, b_1, c \in \mathbb{Z}$:

- $a \equiv b \pmod{n} \iff a$ et b ont le même reste dans la division par n.
- $a \equiv a \pmod{n}$ (réflexivité).
- $a \equiv b \pmod{n} \iff b \equiv a \pmod{n}$ (symétrie).
- $a \equiv b \pmod{n}$ et $b \equiv c \pmod{n} \Rightarrow a \equiv c \pmod{n}$ (transitivité).
- $a \equiv a_1 \pmod{n}$ et $b \equiv b_1 \pmod{n} \Rightarrow \begin{cases} a+b \equiv a_1+b_1 \pmod{n}\,, \\ ab \equiv a_1 b_1 \pmod{n}\,. \end{cases}$

Exemple : Résoudre $3x + 4 \equiv 6 \mod 7$.
On peut écrire $3x \equiv 2 \mod 7$ puis multiplier l'équation par 5 pour obtenir $x \equiv 3 \mod 7$.

Remarque : $a \equiv b \mod n$ si et seulement si il existe c tel que $a = b + cn$.

2.2 Résoudre les congruences linéaires

Soit $n > 0, a \in \mathbb{Z}$, $a' \in \mathbb{Z}$ est l'inverse multiplicatif de $a \mod n$ si $a.a' \equiv 1 \mod n$. On note $a^{-1} \mod n$ l'inverse de a modulo n.

Théorème 2.2.1. *L'entier a admet un inverse multiplicatif modulo n si et seulement si $PGCD(a, n) = 1$*

En pratique, pour calculer l'inverse d'un élément, on utilise l'algorithme d'Euclide étendu.

Théorème 2.2.2. *Soit $a, n, z, z' \in \mathbb{Z}$, $n > 0$. Si $PGCD(a, n) = 1$ alors*

$$az \equiv az' \mod n \Leftrightarrow z \equiv z' \mod n$$

et si $PGCD(a, n) = d$ alors

$$az \equiv az' \mod n \Leftrightarrow z \equiv z' \mod n/d$$

Exemples :
a) $5.2 \equiv 5.(-4) \mod 6$.
On peut simplifier par 5 des deux cotés car $PGCD(5, 6) = 1$. On obtient $2 \equiv -4 \mod 6$.
b) $3.5 \equiv 3.3 \mod 6$.
On ne peut pas simplifier par 3 car $PGCD(3, 6) \neq 1$, mais on peut écrire $5 \equiv 3 \mod 2$.

Théorème 2.2.3. *Soit $a, b, n \in \mathbb{Z}$, $n > 0$ et $PGCD(a, n) = d$. Si $d|b$, $az \equiv b \mod n$ admet une solution z et tout z' est aussi solution si et seulement si $z \equiv z' \mod n/d$. Si $d \nmid b$, la congruence n'admet pas de solution.*

Exercices : Résoudre les équations suivantes
$2z \equiv 3 \mod 15$,
$3z \equiv 4 \mod 15$,
$3z \equiv 12 \mod 15$.
Dans le premier cas, $PGCD(2, 15) = 1$. L'inverse de 2 modulo 15 existe, c'est 8. En multipliant les termes de l'équation par 8, on obtient $z \equiv 9 \mod 15$.
Dans le deuxième cas, $PGCD(3, 15) = 3$. Donc 3 n'admet pas d'inverse et 4 n'est pas divisible par 3. L'équation n'admet pas de solution.
Dans le troisième cas, 12 étant divisible par 3, on peut diviser par 3 et on obtient $z \equiv 4 \mod 5$. L'ensemble des solutions est $S = \{4 + 5k,\ k \in \mathbb{Z}\}$.

Théorème 2.2.4. *Soit $n_1, n_2, \ldots, n_k \in \mathbb{Z}$ et des entiers arbitraires $a_1, a_2, \ldots, a_k \in \mathbb{Z}$. Si les entiers $n_1, n_2, \ldots, n_k$ sont deux à deux premiers entre eux, alors le système :*

$$\begin{cases} x \equiv a_1 \pmod{n_1} \\ x \equiv a_2 \pmod{n_2} \\ \quad \vdots \\ x \equiv a_k \pmod{n_k} \end{cases}$$

a une solution unique modulo $n = n_1 n_2 \ldots n_k$.

Algorithme de Gauss. La solution x du système précédent peut s'écrire :

$$x = \sum_{i=1}^{k} a_i N_i M_i \mod n$$

avec $N_i = n/n_i$, $M_i = N_i^{-1} \mod n_i$.
Exemple. La solution unique du système :

$$\begin{cases} x \equiv 3 \mod 7 \\ x \equiv 7 \mod 13 \end{cases}$$

est $x \equiv 59 \mod 91$.
Remarque : Le logiciel magma permet de calculer de tels systèmes.
Voir $http : //magma.maths.edu.au/calc/$ et taper l'exemple précédent : $CRT([3, 7], [7, 13])$;

2.3 Classes résiduelles

Soit n un entier positif. La relation binaire $\equiv \mod n$ est une relation d'équivalence. La **classe d'équivalence** de $a \in \mathbb{Z}$ est l'ensemble des entiers congrus à a modulo n. Notons-la $[a]_n$.

$$[a]_n = \{a + nz \ : z \in \mathbb{Z}\} = a + n\mathbb{Z}.$$

Les classes d'équivalence sont disjointes et forment une partition de $\mathbb{Z}$ en n sous-ensembles. Si $a = qn + r$, $0 \leq r < n$, alors $a \equiv r \pmod{n}$, r est son **résidu** modulo n, $[a]_n = [r]_n$. Ce résidu est utilisé pour représenter la classe d'équivalence $[a]_n$ de a.
On a $[1]_n = [1 + n]_n$.
Définition. L'ensemble des **entiers modulo n**, noté $\mathbb{Z}_n$ ou $\mathbb{Z}/n\mathbb{Z}$, est l'ensemble des n classes d'équivalence

$$\mathbb{Z}_n = \{[0]_n, [1]_n, [2]_n, \ldots, [n-1]_n\}.$$

L'addition et la multiplication respectant l'équivalence (donc aussi la soustraction, la division et l'exponentiation), elles induisent des opérations sur $\mathbb{Z}_n$: la somme des classes de a et b est la classe de $a+b$, leur produit est la classe de ab :
$[a]_n + [b]_n = [a+b]_n$,
$[a]_n[b]_n = [ab]_n$.
De plus,
$-[a]_n = [-1]_n.[a]_n = [-a]_n$
et
$[a]_n - [b]_n = [a]_n + (-[b]_n) = [a-b]_n$.
Exemple : Les quatre classes modulo 4 sont
$[0]_n = \{\ldots, -4, 0, 4, 8, \ldots\}$
$[1]_n = \{\ldots, -3, 1, 5, 9, \ldots\}$
$[2]_n = \{\ldots, -2, 2, 6, 10, \ldots\}$
$[3]_n = \{\ldots, -1, 3, 7, 11, \ldots\}$
On a par exemple $[1]_n + [3]_n = [0]_n$, $[2]_n.[2]_n = [0]_n$, $[2]_n.[3]_n = [2]_n$.

Définitions. Soit $[a]_n \in \mathbb{Z}_n$. L'**inverse** de $[a]_n$ est, s'il existe, $[x]_n \in \mathbb{Z}_n$ tel que $[ax]_n = [1]_n$. Il est unique, noté $[a]_n^{-1}$, et $[a]_n$ est dit **inversible**. La **division** de $[a]_n$ par $[b]_n \in \mathbb{Z}_n$, si $[b]_n$ est inversible, est égale à $[a]_n \left([b]_n\right)^{-1}$.

Proposition 2.3.1. *$[a]_n \in \mathbb{Z}_n$ est inversible* $\iff PGCD(a,n) = 1$.

Exemple. Les éléments inversibles de $\mathbb{Z}_9$ sont les classes de $1, 2, 4, 5, 7$ et 8. Ainsi $\left([4]_9\right)^{-1} = [7]_9$ car $7\,.\,4 = 3\,.\,9 + 1$.

On a vu qu'on pouvait faire des additions et des multiplications dans $\mathbb{Z}_n$. En fait $(\mathbb{Z}_n, +, .)$ est une structure algébrique avec les propriétés suivantes : pour tout $\alpha, \beta, \gamma \in \mathbb{Z}_n$
$\alpha + \beta = \beta + \alpha$ (commutativité de $+$)
$(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$ (associativité de $+$)
$\alpha + [0]_n = \alpha$ (neutre pour $+$)
$\alpha - \alpha = [0]_n$ (α est l'inverse additif de lui-même) $\alpha.\beta = \beta.\alpha$ (commutativité de .)
$(\alpha.\beta).\gamma = \alpha.(\beta.\gamma)$ (associativité de .)
$\alpha.(\beta + \gamma) = \alpha\beta + \alpha.\gamma$ (distributivité de .)
$\alpha.[1]_n = \alpha$ (existence du neutre de .)

Cette structure est appelée un **anneau commutatif**, sera développée plus tard.
Remarque : Dans $\mathbb{Z}_n$, tous les éléments ont un inverse additif mais pas forcément d'inverse multiplicatif. Si un élément possède un inverse multiplicatif, celui-ci est unique.

Définitions. $\mathbb{Z}_n^*$ est l'ensemble des classes qui admettent un inverse multiplicatif.
Exemple. $\mathbb{Z}_6^* = \{[1]_6, [5]_6\}$

Soit $\alpha \in \mathbb{Z}_n^*$ et $k > 0$, alors $\alpha^k = \alpha \dots \alpha$ (k fois), $\alpha^0 = [1]_n$.

Remarque : Il est équivalent de travailler avec les congruences modulaires ou avec la structure algébrique $\mathbb{Z}_n$.

Par abus de notation, on écrira pour simplifier :
$\mathbb{Z}_n = \{0, 1, 2, \dots, n-1\}$ au lieu de $\mathbb{Z}_n = \{[0]_n, [1]_n, [2]_n, \dots, [n-1]_n\}$. On peut alors voir $\mathbb{Z}_n^*$ comme l'ensemble des entiers premiers avec n et inférieurs à n. Par exemple $\mathbb{Z}_4^* = \{1, 3\}$.

Chapitre 3

Propriétés des entiers modulaires

3.1 Fonction d'Euler

La fonction **indicatrice d'Euler**[1] fait correspondre à un entier positif n le nombre $\Phi(n)$ des entiers compris entre 1 et $n-1$ premiers avec n. On pose $\Phi(1) = 1$.

— Si p est premier, $\Phi(p) = p - 1$ et, si $n \geq 1$, $\Phi(p^n) = (p-1)\, p^{n-1}$.
— Si m et n sont premiers entre eux, $\Phi(mn) = \Phi(m)\, \Phi(n)$.
— Si les p_i sont les facteurs premiers de n, $\Phi(n) = n \prod_{i=1}^{k} (1 - 1/p_i)$.

3.2 Théorème d'Euler et petit théorème de Fermat

Soit $\alpha \in \mathbb{Z}_n^*$. On considère les puissances successives de α : $\alpha^0, \alpha^1, \alpha^2, \ldots$. Tous ces éléments appartiennent à $\mathbb{Z}_n^*$ et comme $\mathbb{Z}_n^*$ est fini, il existe des entiers $k, i > 0$ tels que

$$\alpha^k \equiv \alpha^i \mod n$$

soit $\alpha^{k-i} \equiv 1 \mod n$.
L'ordre multiplicatif de α est le plus petit entier positif t tel que $\alpha^t \equiv 1 \mod n$.

1. Leonhard Euler (1707-1783), immense mathématicien suisse.

Exemple. $n = 7$

i		1	2	3	4	5	6
1^i	mod 7	$\boxed{1}$	1	1	1	1	1
2^i	mod 7	2	4	$\boxed{1}$	2	4	1
3^i	mod 7	3	2	6	4	5	$\boxed{1}$
4^i	mod 7	4	2	$\boxed{1}$	4	2	1
5^i	mod 7	5	4	6	2	3	$\boxed{1}$
6^i	mod 7	6	$\boxed{1}$	6	1	6	1

Ainsi 3 et 5 sont d'ordre 6, 2 et 4 sont d'ordre 3, 6 est d'ordre 2 et 1 est d'ordre 1. On remarque que tous les ordres des éléments divisent 6 qui est le nombre d'éléments dans $\mathbb{Z}_7^* = \Phi(7)$.

Théorème 3.2.1 (d'Euler)**.** *Si $n \geq 2$ et $a \in \mathbb{Z}_n^*$, alors $a^{\Phi(n)} \equiv 1 \pmod{n}$.*

Théorème 3.2.2 (Petit théorème de Fermat [2])**.** *Soit p un nombre premier. Quel que soit a premier avec p, c'est-à-dire non multiple de p, on a : $a^{p-1} \equiv 1 \mod p$.*

Le petit théorème de Fermat est un cas particulier du théorème d'Euler.

Corollaire : Dans $\mathbb{F}_p$, c'est à dire lorsqu'on travaille modulo p, on travaille modulo $p-1$ sur les exposants. ▽

Théorème 3.2.3. *Quel que soit a, $a^p \equiv a \mod p$.*

Soit $n \in \mathbb{Z}^+, a \in \mathbb{Z},\ PGCD(a,n) = 1$, a est un élément **primitif** modulo n si l'ordre multiplicatif de $a \mod n$ est $\Phi(n)$.
Les seuls entiers positifs n pour qui il existe une racine primitive sont

$$n = 1, 2, 4p, 2p^e, \quad p \text{ premier }, e \geq 1.$$

Exercices Déterminer l'ordre de 2 dans $\mathbb{Z}_{21}^*$. Idem avec $\mathbb{Z}_{14}^*$.
L'ensemble des 12 éléments de $\mathbb{Z}_{21}^*$ est $\{1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20\}$. L'élément 2 fait bien partie de $\mathbb{Z}_{21}^*$. Nous savons qu'il n'existe pas d'élément primitif. Cela signifie qu'aucun élément n'est d'ordre 12. Pour calculer l'ordre de 2 il faut calculer 2^i pour $i = 1, 2, \ldots$ jusqu'à obtenir 1. $2^2 = 4,\ 2^3 = 8,\ 2^4 = 16,\ 2^5 = 11,\ 2^6 = 22 = 1$. Donc l'ordre de 2 est 6. Attention, ce n'est pas parce que $a^6 = 1$ que a est d'ordre 6. Par exemple 20 est d'ordre 2 car $20 = -1$ et $-1^2 = 1$. Mais $-1^6 = 1$. D'ailleurs, pour tout $a \in \mathbb{Z}_{21}^*$, on a $a^6 = 1$.
L'ensemble des 6 éléments de $\mathbb{Z}_{14}^*$ est $\{1, 3, 5, 9, 11, 13\}$ et on voit que 2 ne fait pas partie de l'ensemble. Par contre, il existe un élément primitif (d'ordre 6). Essayons de le déterminer. On sait que 1 est d'ordre 1. L'élément 3 est-il d'ordre 6 ? $3^2 = 9,\ 3^3 = 13 = -1$. Or -1 est d'ordre 2. Donc 3 est d'ordre 6. Nous verrons

2. Pierre de Fermat (1601-1665), mathématicien français.

plus tard qu'il existe $\phi(6) = 2$ éléments primitifs.
Exercices Calculer $8^{11} \mod 11, 5^8 \mod 7, 7^8 \mod 30$.
Pour calculer la première valeur, il faut utiliser le petit théorème de Fermat. On sait que $8^{10} \mod 11 \equiv 1$ donc $8^{11} \mod 11 \equiv 8$. Le deuxième calcul fait intervenir le même théorème. $5^6 \mod 7 \equiv 1$, donc $5^8 \mod 7 \equiv 25 \mod 7 \equiv 4 \mod 7$. Le troisième calcul fait intervenir le théorème d'Euler car le modulo n'est pas premier et $PGCD(7, 30) = 1$. Puisque $\phi(30) = 8$, on a $7^8 \mod 30 \equiv 1$.

3.3 Application du théorème d'Euler : le cryptosystème RSA

Le théorème d'Euler est utilisé dans le chiffrement RSA (1977). Bob souhaite chiffrer un message pour Alice. Alice choisit des paramètres entiers premiers p et q et pose $n = pq$. Notons que connaissant p et q, il est facile de calculer n mais si n est grand, il est difficile de retrouver p et q à partir de n. Il n'existe en effet pas d'algorithme rapide de factorisation.
Alice choisit alors un entier $d < n$ puis calcule e tel que $ed \equiv 1 \mod \Phi(n)$. Ces deux valeurs s'appellent des clés. La première clé est privée (d) et la seconde (e) est publique. Connaissant e il est facile de calculer d si on connaît $\Phi(n)$ en utilisant l'algorithme d'Euclide étendu. Mais si on ne connaît pas $\Phi(n)$, le calcul de d est difficile. Or si n est suffisamment grand, le calcul de $\Phi(n)$ est un problème difficile lorsqu'on ne connaît pas la factorisation de n.
Alice rend publique n, e. Pour chiffrer un message $m < n$ (le message est codé en un nombre inférieur à n), Bob utilise la clé publique e, calcule $c = m^e \mod n$ et envoie la valeur à Alice. Alice reçoit c et retrouve la valeur du message m en utilisant la clé privée d. Elle calcule $c^d \mod n = (m^e)^d \mod n = m^{e.d \mod \Phi(n)} \mod n = m$. Bien sur, il faut que $PGCD(m, n) = 1$ pour pouvoir réduire les exposants modulo $\Phi(n)$.
Application numérique
Alice choisit $p = 3, q = 11, d = 7$. Calculer la clé publique. Si $m = 15$, qu'elle est la valeur de c ? Comment Alice va-t-elle déchiffrer le message chiffré par Bob ?
La pratique : Dans la pratique, les paramètres sont à choisir avec précaution. Par exemple, p et q doivent être très grands (supérieurs à 1024 bits) et pour obtenir une sécurité satisfaisante, le cryptosystème ne peut pas être utilisé en l'état car il est déterministe (pour plus de détail, voir http ://www.rsa.com/rsalabs/).

Chapitre 4

Structures algébriques

Une structure algébrique est un ensemble muni d'une ou plusieurs opérations. Certaines structures se rencontrent fréquemment dans notre environnement. Par exemple, l'ensemble des nombres entiers muni de $+$ ou l'ensemble des nombres réels muni de $+$ et . forme une structure qui admet certaines propriétés (associativité, commutativité, inversibilité, distributivité, etc).
Nous allons nous intéresser aux trois structures mathématiques les plus importantes : les structures de groupe, d'anneau et de corps. Chaque structure admet des propriétés qui induisent des méthodes de calcul spécifiques.

4.1 Groupes

Un ensemble G muni d'une opération $*$ associative possédant un élément e, dit **neutre** ($\forall g \in G \; e * g = g * e = g$) tel que, quel que soit $g \in G$, il existe un élément y de G vérifiant : $x * y = e$ est un **groupe**. L'élément y est l'**inverse** de x, et il est noté x^{-1}. Ceci est la notation multiplicative, pour laquelle e est aussi noté 1_G, voire 1, et $a * b$ est souvent noté $a.b$, ou encore ab.
Si l'opération $*$ est commutative, le groupe est dit **commutatif**.
On utilise aussi la notation additive (équivalente) $a + b$, pour laquelle le neutre est noté 0_G, ou simplement 0. L'inverse, s'appelle alors l'**opposé**, noté $-x$. Le choix entre ces deux notations est justifié par le contexte.
Le nombre d'éléments d'un groupe fini G, son cardinal, est son **ordre** $|G|$ (noté aussi $\#G$).
Un groupe se note comme un couple $(G, *)$ (ou un triplet $(G, *, e)$, e étant l'élément neutre) où le premier élément est l'ensemble et le second la loi qui agit sur les éléments. Lorsqu'il n'y a pas d'ambiguïté sur la loi, le groupe se note simplement G.
Exemple de groupes : $(\mathbb{Z}, +)$, $(n\mathbb{Z}, +)$, $(\mathbb{Z}_n, +)$, $(\{\pm 1\}, *)$ et $(\mathbb{Z}_n^*, *)$ appelé

le groupe multiplicatif de $\mathbb{Z}_n$. Notons que $(\mathbb{Z}, *)$ ne forme pas un groupe car les éléments différent de ± 1 n'ont pas d'inverse.

Proposition 4.1.1. *Un groupe G n'admet qu'un seul élément neutre.*

Proposition 4.1.2. *L'inverse d'un élément de G est unique.*

Autres exemples de groupes :
- L'ensemble des chaînes de n bits avec XOR
- Les permutations sur trois éléments S_3 (groupe non commutatif)
- $\mathbb{Z}_{15}^* = \{1, 2, 4, 7, 8, 11, 13, 14\}$.

Définition. L'ordre d'un élément g de G est le plus petit entier non nul n tq $g^n = e$. Si n n'existe pas, g est d'ordre infini.

Proposition 4.1.3. *Soit $g \in G$ un élément d'ordre n, alors g^{-1} est aussi d'ordre n.*

4.1.1 Groupes cycliques

Un groupe fini G est **cyclique** s'il est constitué des puissances successives de l'un de ses éléments, g, appelé alors **générateur** :

$$G = \{g, g^2, \ldots, g^{|G|} = e\}.$$

Exemple : $\mathbb{Z}_{14}^* = \{1, 3, 5, 9, 11, 13\} = \{3^6, 3, 3^5, 3^2, 3^4, 3^3\}$. $\mathbb{Z}_{14}^*$ est donc un groupe cyclique et 3 est un générateur du groupe (aussi appelé élément primitif).

Le nombre de générateurs dans un groupe cyclique d'ordre n est $\Phi(n)$.

Exemples :
- $(\mathbb{Z}, +)$ est engendré par 1
- $(\mathbb{Z}_n, +)$ est engendré par 1 (en fait il s'agit de $[1]_n$)

4.2 Sous-groupe

Un sous ensemble H de G est un sous-groupe de G s'il est non vide et si on a
- pour tout $g, h \in H,\ g * h \in H$ ou $*$ est la loi de G
- pour tout $g \in H,\ \ g^{-1} \in H$.

Attention, il faut bien vérifier que la loi est bien la même. Par exemple, $(\mathbb{Z}_3, +_3)$ n'est pas un sous groupe de $(\mathbb{Z}_{15}, +_{15})$ car le premier groupe est muni de l'addition modulo 3 alors que le deuxième groupe est muni de l'addition modulo 15.
Si H est l'ensemble des puissances d'un élément h d'un groupe cyclique fini G.

Cet ensemble étant fini, il existe un couple d'entiers distincts (r, s) tel que $a^r = a^s$, et alors $a^{r-s} = e$; H est donc un groupe cyclique pour la même opération que G et avec le même neutre : c'est un sous-groupe de G, différent de G si h n'est pas un générateur de G. L'ordre d'un élément de G est l'ordre du groupe cyclique qu'il engendre (ses puissances).
Remarque : Dans un groupe cyclique fini, l'ordre d'un générateur est égal à l'ordre du groupe.

Théorème 4.2.1 (Lagrange)**.** *Soit G fini, $H \subset G$ un sous groupe, alors l'ordre de H divise l'ordre de G.*

Proposition 4.2.1. *Soit $g \in G$, l'ordre de g divise $|G|$. En particulier*

$$|H| \mid |G|, \quad \textit{avec } < g >= H$$

En conséquence, $g^{|G|} = e$, pour tout $g \in G$. En particulier si $a \in \mathbb{Z}_n^*$, alors

$$a^{\Phi(n)} \equiv 1 \mod n.$$

4.3 Homomorphismes de groupes

Considérons deux groupes $(G, \perp)$ et $(H, \top)$ et leur neutre respectif e_G et e_H.
Définition Une application $f : G \to H$ est un homomorphisme de groupe si :
- $f(e_G) = e_H$
- Si x et y sont éléments de G, $f(x \perp y) = f(x) \top f(y)$.

De plus :
- Si $G = H$, f est un **endomorphisme**.
- Si f est bijective, f est un **isomorphisme**. Si il existe un isomorphisme entre G et H, G et H sont isomorphes et on note $G \simeq H$
- Si f est à la fois un isomorphisme et un endomorphisme,f est un **automorphisme**.

L'image de f est

$$Im(f) := \{f(a) \ : \ a \in G\}$$

et le noyau de f est

$$Ker(f) := \{a \in G \ : \ f(a) = e_H\}.$$

On peut montrer que $Im(f)$ et $Ker(f)$ sont des sous groupes de respectivement G et H.

Proposition 4.3.1. *Soit f un homomorphisme. f est injective si et seulement si $Ker(f) = \{e_G\}$. f est surjective si et seulement si $Im(f) = H$.*

Exemples :

1. Soit $f : (\mathbb{Z}_6, +, 0) \to (\mathbb{Z}_{12}, +, 0)$, définie par $f([1]_6) = [4]_{12}$. f est bien définie car $[1]_6$ est générateur de $\mathbb{Z}_6$ et $[4]_{12}$ est d'ordre 3.
   Par la suite, on simplifie les notations en écrivant des entiers au lieu de classes.
   $f(1) = 4, f(2) = 8, f(3) = 0, f(4) = 4, f(5) = 8, f(0) = 0$.
   $Ker(f) = \{0, 3\}$, donc f n'est pas injective.
   $Im(f) = \{0, 4, 8\}$. $Im(f)$ est un sous-groupe de $(\mathbb{Z}_{12}, +, 0)$.
2. $(\mathbb{Z}_6, +, 0)$ et $(\mathbb{Z}_7^*, ., 1)$ sont isomorphe. L'isomorphisme est $f : \ i \to 3^i$.

4.4 Corps et anneaux

On a souvent besoin d'avoir deux opérations binaires distinctes : l'addition et la multiplication. On peut alors construire des structures algébriques plus complexes comme les corps ou les anneaux. Ce sont ces structures qui nous intéressent maintenant.
Un corps F est un ensemble d'éléments dans lequel il est possible de faire des additions, soustractions, multiplications et divisions (à l'exception de zero !).
$+$ et $*$ doivent satisfaire les lois de commutativité, associativité et distributivité.
De plus, pour tout $\alpha \in F$, il doit exister $0,\ 1,\ -\alpha,\ \alpha^{-1}$ tel que

$$\begin{array}{cc} 0 + \alpha = \alpha & (-\alpha) + \alpha = 0 \\ 1 * \alpha = \alpha & 0 * \alpha = 0 \\ \text{et si } \alpha \neq 0 & (\alpha^{-1}) * \alpha = 1 \end{array}$$

Un corps fini contient un nombre fini d'éléments : C'est son **ordre**. Les corps finis sont appelés **Corps de Galois**.
Un anneau $(F, +, \cdot)$ admet une structure semblable au corps à ceci près que les éléments de $F^\star$ n'admettent pas forcément un inverse multiplicatif. L'ensemble des inversibles d'un anneau forme un groupe (multiplicatif) appelé le groupe des inversible de R.

Exemple 4.4.1. *L'anneau des entiers modulo n avec $n \in \mathbb{N}$:*

$$\mathbb{Z}_n = \{0, 1, \ldots,\ n - 1\}.$$

0 est l'élément neutre additif et 1 l'élément neutre multiplicatif. L'ordre de $\mathbb{Z}_n$ est n puisque $\mathbb{Z}_n$ contient n éléments.

La caractéristique d'un anneau est le plus petit entier n tel que $n.1 = 0$. La caractéristique de $\mathbb{Z}_p$ est donc p. Si la caractéristique m d'un corps est non nulle, alors m est premier.

On a vu que $(\mathbb{Z}_n, +, 0)$ et $(\mathbb{Z}_p^\star, *, 1)$ forment des groupes commutatifs pour tout n et tout p premier. On a donc

Proposition 4.4.1. *$(\mathbb{Z}_p, +, \cdot)$ est un corps si p est premier. On le note $\mathbb{F}_p$.*
Si n n'est pas premier, $(\mathbb{Z}_n, +, \cdot)$ est un anneau.

Définition 4.4.1. *Un sous-ensemble F d'un corps E est un sous-corps de E si F est un corps pour les lois de E. Dans ce cas, E est une extension de F.*

4.4.1 Polynômes

Soit A un anneau, un polynôme f est une expression de la forme

$$f(x) = \sum_{i=0}^{n} a_i x^i = a_0 + a_1 x + \cdots + a_n x^n,$$

où n est un entier positif, les coefficients $a_i,\ 0 \leq i \leq n$ sont des éléments de A et x un symbole appelé une indeterminée.

Définition 4.4.2. *Soit $f = \sum_{i=0}^{n} a_i x^i$ un polynôme tel que $a_n \neq 0$. Alors f est de degré n (on note $\deg(f) = n$), a_0 est le terme constant et a_n le coefficient de plus haut degré (leading coefficient en anglais).*

On peut définir la somme et le produit de deux polynômes $f = \sum_{i=0}^{n} a_i x^i$ et $g = \sum_{i=0}^{m} b_i x^i$ $(m \leq n)$:

$$f(x) + g(x) = \sum_{i=0}^{n} (a_i + b_i) x^i,$$

et

$$f(x)g(x) = \sum_{k=0}^{n+m} c_k x^k, \text{ où } c_k = \sum_{i+j=k} a_i b_j,$$

où $0 \leq i \leq n$ et $0 \leq j \leq m$.
L'ensemble des polynômes sur A muni de ces deux opérations admet une structure d'anneau noté $A[x]$.
On montre facilement que pour tout $f, g \in F[x]$ (F étant un corps)

$$\deg(f+g) \leq max\{\deg(f), \deg(g)\}, \text{ et } \deg(fg) = \deg(f) + \deg(g).$$

Le polynôme g divise le polynôme f si il existe un polynôme h tel que $f = gh$.
Pour éviter tout problème, on ne considère ici que des polynômes à coefficients dans un corps.

Exemple 4.4.2. *Dans* $\mathbf{F}_2[x]$*, considérons les deux polynômes*
$f = x^7 + x^6 + x^3 + x^2 + x + 1$ *et*
$g = x^4 + x^3 + x^2 + 1$.
Le polynôme g *divise* f *car* $f = gh$ *avec* $h = x^3 + x + 1$.

Théorème 4.4.1. *Soit* g *un polynôme non nul dans* $F[x]$*. Alors pour tout* $f \in F[x]$ *il existe deux polynômes* q *et* r *de* $F[x]$ *tels que*

$$f = qg + r, \text{ où } \deg(r) < \deg(q).$$

Toujours dans $F[x]$, si d divise f et g et si tout polynôme divisant f et g divise aussi d, alors d est le plus grand diviseur commun de f et g. On note $d = pgcd(f, g)$. Si $pgcd(f, g) = 1$, on dit que f et g sont premiers entre eux.

Exemple 4.4.3. *Les polynômes de* $\mathbf{F}_2[x]$
$f = x^2 + x + 1$ *et* $g = x^5 - 1$ *sont-ils premiers entre eux ?*

Théorème 4.4.2. *Avec les mêmes notations, il existe* $u, v \in F[x]$ *tels que*

$$d(x) = u(x)f(x) + g(x)v(x), \text{ avec } u, v \in F[x].$$

Exemple 4.4.4. *Prenons* $f := x^6 + x^5 + 2\,x^4 + 2\,x^2 + 2$*, et* $g := x^2 + 2\,x + 1$*, deux polynômes sur* $\mathbf{F}_3$*. Alors, on a*

$$f = q_1 g + r_1 \text{ avec } q_1 = x^4 + 2\,x^3 + x \text{ et } r_1 = 2x + 2$$
$$g = q_2 r_1 + r_2 \text{ avec } q_2 = 2x + 2 \text{ et } r_2 = 0.$$

On trouve, $d = 2f + q_1 g = x + 1$.

Définition 4.4.3. *un polynôme non constant* $f \in F[x]$ *est dit irréductible sur* F *si les seuls polynômes* ($\neq f$) *qui le divisent sont constants. Sinon, le polynôme* f *est réductible.*

Par exemple, le polynôme $x^2 - 2$ est irréductible sur Q. Par contre, si on construit un corps contenant Q et $\sqrt{2}$, alors le polynôme sera réductible sur ce corps car $x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$. On note $Q(\sqrt{2})$ le plus petit corps contenant Q et $\sqrt{2}$.

Exemple 4.4.5. *Le polynôme de* $\mathbf{F}_2[x]$
$f = x^4 - 1$ *est-il irreductible ? même question avec* $f = x^3 - 1$.

Théorème 4.4.3. *Tout polynôme* $f \in F[x]$ *peut s'écrire*

$$f = a f_1^{e_1} f_2^{e_2} \dots f_k^{e_k},$$

où $a \in F$*, les* f_i *sont des polynômes irréductibles unitaires de* $F[x]$ *et les exposants* e_i *des entiers positifs. Cette factorisation est unique.*

Rappelons qu'un polynôme unitaire a son coefficient de plus haut degré égal à 1.

Définition 4.4.4. *Un élément a est une racine (ou un zéro) du polynôme f si $f(a) = 0$.*

4.5 Construction d'un corps fini

Jusqu'à présent, nous n'avons introduit qu'un corps ayant p éléments (p premier). Il s'agit de $\mathbf{F}_p$. Dans $\mathbf{F}_p$ les opérations ($+$ et $\cdot$) sont effectuées modulo p.
Comment construire un corps qui admet p^m éléments ? En fait, construire un corps qui contient peu d'éléments n'est pas difficile : il suffit de construire les tables de multiplication et d'addition en respectant les contraintes déjà vues. Par exemple, dans la table de multiplication, chaque ligne doit avoir l'élément neutre. Cela traduit l'existance d'un inverse pour tout élément non nul.
Dans ce qui suit, nous donnons une méthode générale de construction. Nous allons construire le corps $\mathbf{F}_{p^m}$ qui admet p^m éléments.
Soit m un entier positif et $f(x)$ un polynôme irréductible sur $\mathbf{F}_p$ de degré m. On considère un élément α satisfaisant $f(\alpha) = 0$. Posons

$$\mathbf{F}_{p^m} = \{a_0 + a_1\alpha + \cdots + a_{m-1}\alpha^{m-1} \mid a_i \in \mathbf{F}_p\},$$

l'ensemble de tous les polynômes en α de degrés inférieurs à m et à coefficients dans F_p. On peut alors munir cet ensemble des opérations $+$ et $\cdot$.
L'opération $+$ est définie comme l'addition de polynômes dans $\mathbf{F}_p$.
L'opération multiplicative se fait en deux étapes : supposons que l'on veuille calculer $g_1 \cdot g_2$, on va d'abord effectuer une multiplication de polynômes usuelle

$$g_1(\alpha) \cdot g_2(\alpha) = h(\alpha)$$

puis, si le degré de h est supérieur à m, on va le réduire en effectuant une division par f et en considérant le reste r de cette division. Si $\deg(r) < m$ alors $g_1(\alpha) \cdot g_1(\alpha) = r(\alpha)$ sinon on redivise $r(\alpha)$ jusqu'à obtenir un reste dont le degré est inférieur à m. En d'autres termes, on fait les caluls "modulo" le polynôme f, modulo p.

Remarque 1. *Il est important de voir que puisque f est irréductible sur F_p, la racine α n'est pas un élément de F_p. Rappelez-vous de la construction du corps des complexes : l'élément i, racine de $x^2 + 1$, n'est pas un réel.*

Remarque 2. *Pour simplifier, on note souvent $f \cdot g$ par fg.*

Exemple 4.5.1. *Calculer* $f * g \mod h$ *dans* $\mathbf{F}_2$ *avec* $f = x^3 + x^2 + 1$, $g = x^4 + x + 1$ *et* $h = x^5 + x + 1$.

Théorème 4.5.1. $(\mathbf{F}_{p^m}, +, \cdot)$ *est un corps de taille* p^m

Preuve Il est facile de montrer que $(\mathbf{F}_{p^m}, +, \cdot)$ est un anneau contenant p^m éléments. Il reste à montrer que tout élément non nul admet un inverse. Puisque g appartient à $\mathbf{F}_{p^m}$, son degré est inférieur ou égal à $m - 1$. Et puisque f est irréductible, les deux polynômes f et g sont premiers entre eux. On peut donc utiliser Bezout : il existe deux polynômes $u(x)$ et $v(x)$ de $\mathbf{F}_{p^m}[x]$ tels que

$$u(x)f(x) + v(x)g(x) = 1.$$

Si l'on écrit cette égalité en α, puisque $f(\alpha) = 0$, on obtient

$$v(\alpha)g(\alpha) = 1,$$

et en supposant que $\deg(v(\alpha)) < m$ (sinon on réduit modulo f comme précédemment) on a $g^{-1} = v(\alpha)$. □

Le corps $\mathbf{F}_{p^m}$ est appelé une extension finie de $\mathbf{F}_p$ et $\mathbf{F}_p$ est le corps de base. Le corps se note aussi $\mathbf{F}_p[x]/(f(x))$. Si f est réductible, il existe deux polynômes non nuls f_1 et f_2 de $\mathbf{F}_p[x]$ tels que $f = f_1 f_2$. Cela signifie que f_1 et f_2 sont des diviseurs de zéro (donc non inversibles) et $\mathbf{F}_p[x]/(f(x))$ n'est pas un corps.

Exemple 4.5.2. *Soit* $p = 2$ *et* $f(x) = x^3 + x + 1$ *un polynôme irréductible sur* $\mathbf{F}_2$. *Soit* β *une racine de* $f(x)$. *Le corps fini* $\mathbf{F}_{2^3}$ *est défini par*

$$\mathbf{F}_{2^3} = \{a_0 + a_1\beta + a_2\beta^2 | a_i \in \mathbf{F}_2\}.$$

Les éléments de $\mathbf{F}_{2^3}$ *peuvent donc s'écrire comme des triplets* (a_0, a_1, a_2) *ou des polynômes. De plus, puisque* $\mathbf{F}_{2^3}$ *est un corps,* $\mathbf{F}_{2^3}^\star$ *forme un groupe multiplicatif.*

On peut montrer que tout corps fini peut être construit comme nous venons de le voir. Cela signifie que tout corps fini F de caractéristique p admet p^m éléments (m étant un entier strictement positif).

Exemple 4.5.3. *On veut construire le corps à quatre éléments. On sait que* $4 = 2^2$ *donc le corps de base est* $\mathbf{F}_2$ *et pour construire le corps, il suffit d'obtenir un polynôme irreductible de degré* $m = 2$ *sur* $\mathbf{F}_2$ *(pour cela il existe des tables de polynômes irreductibles dans la littérature).*
Soit $f(x) = x^2 + x + 1$ *un polynôme irréductible sur* $\mathbf{F}_2$ *et soit* β *une racine de* $f(x)$. *La caractéristique du corps est égale à* 2, *c'est la caractéristique du corps de base. Les éléments de* F_4 *peuvent être représentés par les polynômes de la forme* $a_1 + a_2\beta$, a_1 *et* a_2 *étant binaires. On obtient :* $F_4 = \{0, 1, \beta, \beta + 1\}$. *Le*

corps est totalement défini par sa table d'addition et de multiplication que nous construisons maintenant en notant $\beta + 1 = \overline{\beta}$

$+$	0	1	β	$\overline{\beta}$
0	0	1	β	$\overline{\beta}$
1	1	0	$\overline{\beta}$	β
β	β	$\overline{\beta}$	0	1
$\overline{\beta}$	$\overline{\beta}$	β	1	0

$\cdot$	0	1	β	$\overline{\beta}$
0	0	1	0	0
1	0	1	β	$\overline{\beta}$
β	0	β	$\overline{\beta}$	1
$\overline{\beta}$	0	$\overline{\beta}$	1	β

Considérons maintenant un corps fini F muni de p^m éléments et $\beta \in F^\star = F \setminus \{0\}$. Alors toute puissance de β appartient aussi à $F^\star$ et comme F est fini, il existe un k et un l tel que $\beta^k = \beta^l$. Cela signifie que $\beta^{k-l} = 1$.

Exemple 4.5.4. $F = \mathbb{Z}_{11},\ \beta = 2$. *$F^\star$ s'écrit*

2^0	2^1	2^2	2^3	2^4	2^5	2^6	2^7	2^8	2^9	2^{10}	2^{11}
1	2	4	8	5	10	9	7	3	6	1	2

Donc $\beta^{10} = 1$ *: β est une racine dixième de l'unité.*

Définition 4.5.1. *L'***ordre** *d'un élément β non nul dans un corps fini est le plus petit entier $r \geq 1$ tel que $\beta^r = 1$.*

Théorème 4.5.2. *(de l'élément primitif) Tout corps fini F de taille p^m contient un élément β d'ordre $p^m - 1$, appelé* **élément primitif** *de F.*

Preuve On sait que puisque F est un corps, $F^\star$ est un groupe multiplicatif d'ordre $p^m - 1$. On va montrer plus précisément que c'est un groupe cyclique engendré par un élément β.
Soit $\beta \in F^\star$ un élément dont l'ordre r est le plus grand parmi tous les éléments du groupe. On a trivialement $r < p^m$. Il est facile de montrer que l'ordre l de tout élément b du groupe divise r. Ainsi, puisque β est racine de l'equation $x^r - 1$, tous les éléments du groupe sont aussi racines de cette même equation et $\prod_{\alpha \in F^\star}(x - \alpha)$ divise $x^r - 1$. Ce qui signifie que $r \geq p^m - 1$. Comme on sait que $r \leq p^m - 1$ on a $r = p^m - 1$. Donc β est d'ordre $p^m - 1$ qui est la taille du groupe multiplicatif $F^\star$ et $F^\star = \{1, \beta, \beta^2, \ldots, \beta^{p^m - 2}\}$. □

Corollaire 4.5.1. *Tout corps fini de taille p^m est de la forme*

$$F = \{0\} \cup \{1, \beta, \beta^2, \ldots, \beta^{p^m - 2}\},\ \beta \in F.$$

Exemple 4.5.5. $F = \mathbb{Z}_{11} = \{0\} \cup \{1, 2, 2^2, 2^3, 2^4, 2^5, 2^6, 2^7, 2^8, 2^9\}$.

Un polynôme primitif est un polynôme qui contient une racine primitive. Il faut noter que tous les polynômes irréductibles ne sont pas primitifs. Par exemple dans $\mathbf{F}_2[x]$, $P = x^{11}+x^9+x^7+x^6+x^5+x+1$ est irréductible de degré 11 et racine de $x^{23}-1$. Soit β une racine de P, β est d'ordre 23 et non $2^{11}-1 = 2047$ donc β n'est pas une racine primitive de $\mathbf{F}_{2^{11}}$. La donnée de P permet de construire le corps : c'est l'ensemble des polynômes de $\mathbf{F}_2[x]$ "modulo" $P(x)$.
Cependant, d'après le théorème précédent, il existe un élément α d'ordre $2^{11}-1 = 2047$ dont les puissances forment $\mathbf{F}^{\star}_{2^{11}}$. On sait que l'ordre de β divise l'ordre de α. On a $\beta = \alpha^{89}$ car $89 * 23 = 2047$. En résumé, voici deux représentations du corps en fonction de β ou α :

$$\begin{aligned}\mathbf{F}_{2^{11}} &= \{\textstyle\sum_{i=1}^{11} a_i\beta^i,\ a_i \in \mathbf{F}_2\} \\ &= \{0\} \cup \{1, \alpha, \alpha^2, \ldots, \alpha^{2^{11}-2}\}.\end{aligned}$$

Théorème 4.5.1. *(Fermat) Tout élément β d'un corps F d'ordre p^m satisfait $\beta^{p^m} = \beta$. Ainsi, β est racine de $x^{p^m} = x$ et*

$$x^{p^m} - x = \prod_{\beta \in F}(x - \beta).$$

Définition 4.5.2. *Le polynôme minimal sur $\mathbf{F}_p$ de β est le polynôme unitaire de plus bas degré $M(x)$ dont les coefficients sont dans $\mathbf{F}_p$ tel que $M(\beta) = 0$.*

Exemple 4.5.6. *Construction du corps $F_8 = F_{2^3}$. Le corps admet huit éléments donc il contient un élément β d'ordre 7 qui est une racine primitive de l'unité. $F_8 = \{0\} \cup \{1, \beta, \beta^2, \ldots, \beta^6\}$, et β est racine du polynôme $(x^7 - 1) \mod 2$. On a $x^7 - 1 = \prod_{i=1}^{7}(x - \beta^i) = (x^3 + x + 1)(x^3 + x^2 + 1)(x + 1)$. Notons P_1 le polynôme $x^3 + x + 1$ et P_2 son réciproque et choisissons comme générateur β une racine de P_1. Cela veut dire que $P_1(\beta) = 0$ et $\beta^3 = \beta + 1$. Tout élément du corps peut être représenté par un triplet (s'il est vu comme un espace vectoriel de dimension 3 sur F_2) ou un polynôme de degré (au plus) 2 avec $\beta^3 = \beta + 1$.*

triplet $(\beta^2, \beta, 1)$	*polynôme*	*puissance de* β
$(0,0,0)$	0	0
$(0,0,1)$	1	1
$(0,1,0)$	β	β
$(1,0,0)$	β^2	β^2
$(0,1,1)$	$1+\beta$	β^3
$(1,1,0)$	$\beta+\beta^2$	β^4
$(1,1,1)$	$1+\beta+\beta^2$	β^5
$(1,0,1)$	$1+\beta^2$	β^6
$(0,0,1)$	1	$\beta^7 = 1$

En choisissant β racine de P_2, on aurait obtenu un corps isomorphe. Rappelons que deux corps sont dits isomorphes si il existe une application bijective ϕ de E dans F qui preserve l'arithmétique du corps (c.a.d. $\phi(a+b) = \phi(a) + \phi(b)$ et $\phi(ab) = \phi(a)\phi(b)$, $a,\ b \in E$).

Exemple 4.5.7. *Construction du corps $F_{16} = F_{2^4}$.*
On sait que F_{16} peut s'écrire $F_{16} = \{0\} \cup \{1, \beta, \beta^2, \ldots, \beta^{14}\}$, où β est un élément primitif de F_{16}.

4.5.1 Logarithme de Zech

Lorsque l'on fait des calculs dans les corps finis, il est facile de calculer $\alpha^i \alpha^j$. Il suffit d'additionner les puissances. Par contre, $\alpha^i + \alpha^j$ est plus difficile à déterminer. On peut alors utiliser le logarithme de Zech.
Supposons que $i < j$. Alors

$$\alpha^i + \alpha^j = \alpha^i(1 + \alpha^{j-i}).$$

Posons $r = j - i$. On veut calculer $(1 + \alpha^r) = \alpha^s$.
L'entier s est appelé le logarithme de Zech de r, noté $Zech(r)$:

$$\alpha^{Zech(r)} = \alpha^r + 1.$$

Il existe bien sur des tables de logarithmes pour les corps finis les plus utilisés.

Exercice 4.5.1. *Calculer les tables pour $\mathbf{F}_8$ et $\mathbf{F}_{16}$.*

Par cette méthode, il suffit de stocker les $p^m - 2$ logarithmes de Zech pour pouvoir effectuer toutes les additions nécessaires.

4.5.2 Classes cyclotomiques

Les classes cyclotomiques (cyclotomic cosets en anglais) permettent de déterminer le nombre de facteurs irréductibles de $x^{p^m-1} - 1$ sur F. Connaissant le polynôme minimal d'une racine de $x^{p^m-1} - 1$, elles permettent de trouver tous les polynômes minimaux des racines de $x^{p^m-1} - 1$, c'est à dire tous les facteurs de $x^{p^m-1} - 1$.

Théorème 4.5.3. *$\beta \in F_{p^m}$ et β^p ont le même polynôme minimal.*

Preuve Soit $M_\beta(x)$ le polynôme minimal de β. $M_\beta(x) = \sum_{i=0}^{d} a_i x^i$, où $d = \deg(M_\beta(x))$ et $a_i \in F_p$. Notons que $a_i = a_i^p$ car a_i est racine de $x^p - x = 0$. On a $M_\beta(\beta) = 0$ et $M_\beta(\beta) = \sum_{i=0}^{d} a_i \beta^i = (\sum_{i=0}^{d} a_i \beta^i)^p = \sum_{i=0}^{d} a_i^p (\beta^p)^i = M(\beta^p)$. Donc β^p est une racine de M_β. Puisque M_β est irreductible, $M_\beta = M_{\beta^p}$. □

Définition 4.5.3. *Soit $\beta \in F_{p^m}$. Alors les éléments $\beta,\ \beta^p, \ldots,\ \beta^{p^{m-1}}$ sont appelés les conjugués de β pour le corps F_p.*

Tous les conjugués de β ont donc le même polynôme minimal.

Exemple 4.5.8. *On considère le corps F_{16} avec $p = 2$, $m = 4$ et β admettant pour polynôme minimal $\beta^4 + \beta + 1$. Alors*

$$\left.\begin{array}{ll} \beta & \text{est un zéro de } x^4 + x + 1 \\ \beta^2 & \text{idem} \\ \beta^4 & \text{idem} \\ \beta^8 & \text{idem} \\ \beta^{16} = \beta & \end{array}\right\} \text{4 racines distinctes}$$

Finalement, on peut vérifier par le calcul que

$$x^4 + x + 1 = (x - \beta)(x - \beta^2)(x - \beta^4)(x - \beta^8).$$

Trouver l'ensemble des conjugués de toutes les racines revient à partitionner l'ensemble des puissances de β. Le corps F s'écrit $F = \{0\} \cup \{1, \beta, \beta^2, \ldots, \beta^{p^m-2}\}$ et l'ensemble des puissances de β est tout simplement Z_{p^m-1}.

Définition 4.5.4. *Soit $a,\ b \in Z_{p^m-1}$. a et b sont dits equivalents (notés $a \equiv b$) si $b = p^i a \mod (p^m - 1)$.*

La relation d'equivalence est reflexive, symétrique et transitive. C_s représente une classe cyclotomique où s est le plus petit entier de la classe :

$$\{s,\ sp,\ sp^2, \ldots,\ sp^{m_s-1}\},$$

où m_s est l'entier le plus petit tel que $p^{m_s} = s \pmod{p^m - 1}$. L'entier s est quelquefois appelé le chef de classe ou en anglais coset leader.

Exemple 4.5.9. *Quelles sont les classes cyclotomiques modulo 15 pour $p = 2$?*

$$\begin{array}{l} C_0 = \{0\} \\ C_1 = \{1, 2, 4, 8\} \\ C_3 = \{3, 6, 12, 9\} \\ C_5 = \{5, 10\} \\ C_7 = \{7, 14, 13, 11\}. \end{array}$$

Théorème 4.5.4. *Soit $\alpha \in \mathbf{F}_{p^m}$ un élément primitif.*

$$M(\alpha^s)(x) = \prod_{i \in C_s} (x - \alpha^i)$$

Preuve Ce résultat est admis. □

Exercice 4.5.2. *Soit α une racine primitive de $x^4 + x + 1$ sur $\mathbf{F}_{16}$.*
Déterminer les polynômes minimaux de $1, 3, 5, 7$.