Université Mohammed Premier
Faculté Pluridisciplinaire de Nador
Département de Mathématiques
Nador

Troisième Année Universitaire
Semestre 6
Filière : SMA

ARITHMÉTIQUE 2
NOTES DE COURS

Professeur : Taoufik Serraj

Année universitaire : 2020-2021
Version : 1

Table des matières

“Les mathématiques sont la science des opérations habiles avec des concepts et des règles inventés uniquement à cette fin."

Eugene Wigner.

“Les mathématiques sont la reine des sciences et la théorie des nombres est la reine des mathématiques".

Gauss

Muhammad Ibn Musa al-Khuwarizmi, ou encore Al-Khwarizmin (vers 780–850), mathématicien musulman, son travail a permis d'introduire l'algèbre en Europe. Son nom est à l'origine du mot algorithme et son livre à l'origine du mot Algèbre où il montre comment résoudre les 6 équations canoniques du second degré et les méthodes pour s'y ramener.

1. Introduction

L'objectif de ce cours est de donner une introduction à la cryptographie et à la théorie des codes correcteurs d'erreurs. Ces disciplines se basent sur plusieurs théories de mathématiques, nous allons donc commencer par rappeler et completer quelques résultats de l'arithmétique et presenter les concepts de base de la théorie des corps finis.

Le lecteur est supposé connaître la théorie de base sur les groupes, les anneaux et les corps.

Le début du cours est consacré à l'étude de la congruence, dans $\mathbb{Z}$, modulo un entier naturel, et à une introduction à la théorie des groupes finis. Les premiers résultats de cette théorie sont indispensables dans la plupart des applications arithmétiques. Ensuite, nous insistons sur quelques points de l'arithmétique de $K[X]$, où K est un corps fini, à savoir la division euclidienne dans $K[X]$, le pgcd et le ppcm de deux polynômes. Après, nous traitons la théorie des corps finis. Enfin, nous abordons les notions de base la cryptographie.

J'espère que ce document vous sera utile et j'attends avec plaisir toute remarque, correction et suggestion que vous pouvez m'envoyer sur mon adresse email :

staoufik.fpn@gmail.com

Bonne lecture !

2. Arithmétique des congruences

2.1. **Rappel.**

On rappelle que si G est un groupe ayant un nombre fini d'éléments, alors son nombre d'éléments est dit cardinal ou ordre de G, il est noté par $\text{card}(G)$ ou $|G|$ ou $\#G$. Commençons par la définition d'un groupe cyclique.

Définition 1. On dit qu'un groupe G est monogène s'il est engendré par l'un de ses éléments, c'est-à-dire s'il existe a dans G tel que :

$$G = \langle a \rangle = \{a^k |\ k \in \mathbb{Z}\} \text{ si la loi est notée multiplicativement.}$$
$$G = \langle a \rangle = \{ka |\ k \in \mathbb{Z}\} \text{ si la loi est notée additivement.}$$

Dans le cas où G est monogène fini, G est dit cyclique. L'élément a est dit un générateur de G.

Remarques 1.

1. Un groupe monogène est nécessairement commutatif.
2. Un groupe cyclique engendré par un élément $g \neq e$ a au moins deux élément, e et g.

Exemples 1.

1. $(\mathbb{Z}, +)$ est monogène engendré par 1.
2. Les sous-groupes $(n\mathbb{Z}, +)$ de $(\mathbb{Z}, +)$, où $n \geq 0$, sont tous monogènes engendré par n.

Déterminons les sous-groupes de $\mathbb{Z}$.

Proposition 1. *Pour tout $n \in \mathbb{Z}$, $n\mathbb{Z}$ est un sous-groupe commutatif de $(\mathbb{Z}, +)$.*

Preuve. Soit n un entier relatif. Montrons que $n\mathbb{Z}$ est un sous-groupe commutatif de $(\mathbb{Z}, +)$.

1. $n \in \mathbb{Z} \neq \emptyset$, car $0 \in n\mathbb{Z}$.
2. Soient a et b dans $n\mathbb{Z}$, alors $a + b \in n\mathbb{Z}$. En effet, on a : $a = nk$ et $b = nh$, donc $a + b = n(k + h) \in n\mathbb{Z}$. De plus il est simple de voir que $a + b = b + a$.
3. Soit a dans $n\mathbb{Z}$, donc $-a \in n\mathbb{Z}$, car $-a = -nk = n(-k)$.

□

La réciproque de ce résultat, qui est conséquence de la division euclidienne dans $\mathbb{Z}$, est vraie ; elle concerne la forme spécifique des sous-groupes de $\mathbb{Z}$.

Théorème 1. *Les sous-groupes de $(\mathbb{Z}, +)$ sont les ensembles $n\mathbb{Z}$, avec $n \in \mathbb{Z}$.*

Preuve. Soit H un sous-groupe de $\mathbb{Z}$. Si $H = \{0\}$, alors $H = 0\mathbb{Z}$.
Supposons que $H \neq \{0\}$, donc il existe un entier $a \in H$ tel que $a \neq 0$. Alors l'un des entiers a ou $-a$ est dans $H^+ = H \cap \mathbb{N}^*$. L'ensemble H^+ est donc une partie non vide de $\mathbb{N}^*$ et en conséquence admet un plus petit élément $n \geq 1$. Comme $n \in H$ et H est un groupe additif, alors $n\mathbb{Z} \subset H$.

D'autre part, pour tout $x \in H$, la division euclidienne par n donne

$$x = qn + r \text{ avec } r = x - nq \in H^+ \text{ et } r \leq n - 1,$$

ceci impose $r = 0$ par définition de n. On a donc $H \subset n\mathbb{Z}$ et $H = n\mathbb{Z}$.

L'unicité provient du fait que $n\mathbb{Z} = m\mathbb{Z}$ si, et seulement si, $n = \mp m$; et pour n et m positifs, on a nécessairement $n = m$. □

Cette démonstration nous permet de dire que :

Corollaire 1. *Si H est un sous-groupe de $(\mathbb{Z}, +)$, alors il existe un unique $n \in \mathbb{N}$ tel que $H = n\mathbb{Z}$.*

Corollaire 2. *Les idéaux de $\mathbb{Z}$ sont les sous-groupes de $\mathbb{Z}$.*

Preuve. Tout idéal d'un anneau en est par définition un sous-groupe. Réciproquement, pour tout entier naturel n, il est clair que $n\mathbb{Z}$ est un idéal de $\mathbb{Z}$. □

Corollaire 3. *Soient a et b deux entiers relatifs non tous deux nuls. Il existe un unique entier naturel δ tel que :*

$$a\mathbb{Z} + b\mathbb{Z} = \delta\mathbb{Z}.$$

Cet entier s'écrit $\delta = au + bv$ avec $(u, v) \in \mathbb{Z}^2$ et c'est le pgcd de a et b.

Preuve. $a\mathbb{Z} + b\mathbb{Z} = \{au + bv \in \mathbb{Z} \mid u, v \in \mathbb{Z}\}$ est un sous-groupe de $(\mathbb{Z}, +)$, le corollaire 1 nous dit qu'il existe un unique entier naturel δ tel que $a\mathbb{Z} + b\mathbb{Z} = \delta\mathbb{Z}$.

Comme $\delta \in \delta\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}$, il existe $(u, v) \in \mathbb{Z}^2$ tel que $\delta = au + bv$. De $a\mathbb{Z} \subset \delta\mathbb{Z}$ et $b\mathbb{Z} \subset \delta\mathbb{Z}$, on déduit que δ un diviseur commun à a et b. Si $d \in \mathbb{N}$ est un diviseur commun à a et b, il divise aussi $\delta = au + bv$ et $d \leq \delta$ (a et b n'étant pas tous les deux nuls, on a $\delta \neq 0$). Donc δ est bien le plus grand entier naturel qui divise a et b. □

Corollaire 4. *Soient a_1, a_2, $\cdots$, a_n n entiers relatifs non tous nuls. Il existe un unique entier naturel δ tel que :*

$$a_1\mathbb{Z} + a_2\mathbb{Z} + \cdots + a_n\mathbb{Z} = \delta\mathbb{Z}.$$

Cet entier s'écrit $\delta = \sum_{i=1}^{n} a_i u_i$ avec $u_i \in \mathbb{Z}^2$ et c'est le pgcd de a_1, a_2, $\cdots$, a_{n-1} et a_n.

Preuve. Par récurrence sur n. □

Corollaire 5. *Soient a et b deux entiers relatifs. Il existe un unique entier naturel μ tel que :*

$$a\mathbb{Z} \cap b\mathbb{Z} = \mu\mathbb{Z}.$$

Si $a = 0$ ou $b = 0$, alors $\mu = 0$, et si $a \neq 0$ et $b \neq 0$, alors μ est le ppcm de a et b.

Preuve. $a\mathbb{Z} \cap b\mathbb{Z}$ est un sous-groupe de $(\mathbb{Z}, +)$, l'unicité et l'existence de μ se déduit du corollaire 1.

Si $a = 0$ ou $b = 0$, alors $\mu\mathbb{Z} \subset 0\mathbb{Z} = \{0\}$; d'où $\mu = 0$.

Si $a \neq 0$ et $b \neq 0$, alors $\mu\mathbb{Z} \subset a\mathbb{Z}$ et $\mu\mathbb{Z} \subset b\mathbb{Z}$, on déduit que μ est multiple de a et b. Si $m \in \mathbb{N}$ est un multiple commun à a et b ; il est dans $a\mathbb{Z} \cap b\mathbb{Z} = \mu\mathbb{Z}$, et c'est donc un multiple de μ ; ce qui implique $m \geq \mu$. Donc, μ est bien le plus petit entier naturel non nul multiple de a et de b. □

Corollaire 6. *Soient a_1, a_2, $\cdots$, a_n n entiers relatifs non tous nuls. Il existe un unique entier naturel μ tel que :*

$$a_1\mathbb{Z} \cap a_2\mathbb{Z} \cap \cdots \cap a_n\mathbb{Z} = \mu\mathbb{Z}.$$

μ est le ppmc de a_1, a_2, $\cdots$, a_{n-1} et a_n.

Preuve. Par récurrence sur n. □

2.2. **La congruence dans $\mathbb{Z}$.**

La notion de congruence est ancienne, Les congruences modulo 2 et 4 ont été utilisées par les Grecs, mais la mise en forme de cette notion est due à Legendre et Gauss.

2.2.1. **La congruence modulo un entier.**

Définition 2. Soit n un entier naturel, et soient a, b deux entiers relatifs quelconques. On dit que a et b sont congrus modulo n, et on écrit $a \equiv b\ [n]$ ou $a \equiv b\ (\text{mod } n)$, si $b - a$ est dans $n\mathbb{Z}$, c'est-à-dire $b - a$ est un multiple de n.

$$a \equiv b\ [n] \Longleftrightarrow \exists k \in \mathbb{Z},\ b - a = kn.$$

On définit ainsi une relation sur $\mathbb{Z}$, appelée relation de congruence modulo n.
(La notion de congruence modulo n a été introduite par Gauss.)

Remarques 2.

- La congruence modulo $-n$ est la même que la congruence modulo n.

- On a l'équivalence : $a \equiv b \ \ [n] \Leftrightarrow (\exists k \in \mathbb{Z}, a = b + kn)$.
- $a \equiv b\ [n]$ équivaut à «a et b ont le même reste dans la division euclidienne par n».
- Pour $n = 0$, on a $0\mathbb{Z} = 0$ et $a \equiv b\ [0]$ revient à dire que $a = b$, c'est-à-dire la congruence modulo 0 ce n'est que l'égalité.
- Pour $n = 1$, on a $1\mathbb{Z} = \mathbb{Z}$, et la relation $a \equiv b\ [1]$ est toujours vérifiée.

Proposition 2. *Soit n un entier naturel. La relation de congruence modulo n est une relation d'équivalence sur $\mathbb{Z}$.*

Preuve. C'est la la relation d'équivalence associée au sous-groupe $H = n\mathbb{Z}$ de $\mathbb{Z}$, $a \equiv b \pmod{n} \Longleftrightarrow a - b \in n\mathbb{Z}$. □

2.2.2. **Classes d'équivalences.** Soit n un entier strictement positif fixé. On note souvent $\overline{a}$ la classe d'équivalence de a pour la relation de congruence modulo n, c'est-à-dire l'ensemble des b de $\mathbb{Z}$ tels que $b \equiv a\ [n]$,

$$\overline{a} = \{b \in \mathbb{Z} |\ b \equiv a[n]\} = \{b \in \mathbb{Z} |\ b = a + kn, k \in \mathbb{Z}\} = \{a + kn |\ k \in \mathbb{Z}\} = a + n\mathbb{Z}.$$

Tout élément x de $\overline{a}$ est dit *un représentant* de $\overline{a}$, de plus, pour tout $a \in \mathbb{Z}$, il existe un unique entier $0 \leq r \leq n - 1$ tel que $\overline{a} = \overline{r}$. En effet, la division euclidienne de a par n donne

$$a = nq + r \text{ avec } 0 \leq r \leq n - 1,$$

d'où le résultat.
Alors tout entier relatif a est congru, modulo n, à un unique entier r de $\{0, ..., n-1\}$ qui est le reste dans la division de a par n. Il y a donc exactement n classes d'équivalences, et on note souvent l'ensemble des classes d'équivalence par :

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

$$\mathbb{Z}_0 = \mathbb{Z}/0\mathbb{Z} = \{\{a\} |\ a \in \mathbb{Z}\} = \mathbb{Z}, \text{ par identification.}$$

$$\mathbb{Z}_1 = \mathbb{Z}/1\mathbb{Z} = \{\mathbb{Z}\} = \{\overline{0}\}.$$

On déduit donc le théorème suivant.

Théorème 2. *Pour tout entier naturel non nul n, l'ensemble des classes d'équivalence modulo n est*

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

Cet ensemble est de cardinal égal à n et il est en bijection avec l'ensemble de tous les restes dans la division euclidienne par n.

Remarque 1. Dire que a et b sont congrus modulo n revient à dire qu'ils ont le même reste dans la division euclidienne par n.

Proposition 3. *Soit n un entier strictement positif.*

1. *Pour tous entiers relatifs a, b, c, d on a les implications*
$$\begin{cases} a \equiv b\ [n] \\ c \equiv d\ [n] \end{cases} \Longrightarrow a + c \equiv b + d\ [n]\ \text{et}\ ac \equiv bd\ [n]$$
On dit que la congruence est compatible avec l'addition et la multiplication.
2. *Pour tout entier naturel k, on a l'implication : $a \equiv b\ [kn] \Rightarrow a \equiv b\ [n]$.*
3. *Pour tout entier naturel k, on a l'implication : $a \equiv b\ [n] \Rightarrow a^k \equiv b^k\ [n]$.*
4. *Si q est un entier relatif différent de 0, alors on a l'équivalence :*
$a \equiv b\ [n] \Leftrightarrow qa \equiv qb\ [qn]$.
5. *Si les entiers q et n sont premiers entre eux, alors : $qa \equiv qb\ [n] \Longleftrightarrow a \equiv b[n]$.*

Preuve. Simple à vérifier. □

Remarque 2. Par le théorème précédent, on peut donc additionner, soustraire, multiplier les congruences relatives au même module n. En revanche, on ne peut pas toujours simplifier les congruences sauf si a et n sont premiers entre eux. Cela montre que la situation est bonne lorsque n est premier.

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

Dans tout ce qui suit $\mathbb{Z}_n$ désigne $\mathbb{Z}/n\mathbb{Z}$. La compatibilité de la relation de congruence modulo n avec l'addition et la multiplication sur $\mathbb{Z}$, va nous permettre de transporter la structure d'anneau de $\mathbb{Z}$ à $\mathbb{Z}_n$.

2.3.1. L'anneaux $\mathbb{Z}_n$.

On définit sur $\mathbb{Z}_n$ deux opérations (deux lois de composition internes) :

1. l'addition par : $\overline{x} + \overline{y} = \overline{x + y}$,
2. la multiplication par : $\overline{x} \times \overline{y} = \overline{x \times y}$.

Lemme 1. *Les opérations qu'on vient de définir ne dépendent pas des représentants choisis.*

Preuve. En effet, soient x et y dans $\mathbb{Z}_n$, et soient a et a' dans $\mathbb{Z}$ des représentants de x, et b et b' dans $\mathbb{Z}$ des représentants de y, alors
$$\begin{cases} x + y = \overline{a} + \overline{b} = \overline{a + b} \\ xy = \overline{a} \times \overline{b} = \overline{ab} \end{cases}$$

D'autre part, on a $a \equiv a'$ et $b \equiv b'$ modulo n, donc $a+b \equiv a'+b'$ et $ab \equiv a'b'$ modulo n (Proposition 3), donc $\overline{a+b} = \overline{a'+b'}$ et $\overline{ab} = \overline{a'b'}$, d'où $x+y = \overline{a+b} = \overline{a'+b'}$ et $xy = \overline{ab} = \overline{a'b'}$. Ce qui prouve que les définitions de $x+y$ et xy ne dépendent pas des choix des représentants de x et y. □

Théorème 3. *Soit n un entier naturel. Alors $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ muni de l'addition des classes est un groupe, abélien, cyclique engendré par $\overline{1}$ et d'ordre n.*

Preuve. On montre facilement que l'addition des classes :

1. est une loi de composition interne sur $\mathbb{Z}_n$,
2. est associative,
3. admet un élément neutre qui est $\overline{0}$,
4. tout élément $\overline{x}$ de $\mathbb{Z}_n$ admet un symétrique qui est $-\overline{x}$,
5. tout élément x de $\mathbb{Z}_n$ s'écrit :

$$x = \overline{k} = \underbrace{\overline{1} + \overline{1} + \cdots + \overline{1}}_{k \text{ fois}}.$$

avec $\overline{k} = 0$ si, et seulement si, k est multiple de n, on en déduit que $(\mathbb{Z}_n, +)$ est un groupe cyclique d'ordre n engendré par $\overline{1}$. En fait, à isomorphisme près, c'est le seul.

□

Théorème 4. *Soit n un entier naturel. Alors $\mathbb{Z}_n^* = (\mathbb{Z}/n\mathbb{Z})^* = \mathbb{Z}/n\mathbb{Z} - \{\overline{0}\}$ muni de la multiplication des classes est un groupe si, et seulement si, n est un nombre premier.*

Preuve. Pour tout $n \in \mathbb{N}$, il est simple de voir que la multiplication des classes :

1. est une loi de composition interne sur $\mathbb{Z}_n^*$,
2. est associative,
3. admet un élément neutre qui est $\overline{1}$.

Supposons que $((\mathbb{Z}/n\mathbb{Z})^*, \times)$ est un groupe. Donc tout élément de $\mathbb{Z}_n^*$ est inversible, d'où pour tout a tel que $1 \leq a \leq n-1$, $\overline{a}$ admet un inverse $\overline{b}$ dans $(\mathbb{Z}/n\mathbb{Z})^*$, c-à-d $\overline{a}\overline{b} = \overline{1} \iff ab \equiv 1[n]$. Alors il existe $k \in \mathbb{Z}$ tel que $ab + nk = 1$, d'où $a \wedge n = 1$; par suite n est premier.

Inversement, si n est premier, alors n est premier à tout a tel que $1 \leq a \leq n-1$. Donc le théorème de Bézout nous implique l'existence de b, $k \in \mathbb{Z}$ tels que $ab + nk = 1$, d'où $\overline{a}\overline{b} = \overline{1}$. Par suite tout élément de $(\mathbb{Z}/n\mathbb{Z})^*$ est inversible. □

Théorème 5. *Soit n un entier naturel, notons $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$.*

1. $(\mathbb{Z}_n, +, .)$ *est un anneau commutatif unitaire.*
2. *L'application* $\pi_n : \begin{array}{ccc} (\mathbb{Z}, +, \cdot) & \longrightarrow & (\mathbb{Z}_n, +, \cdot) \\ a & \longmapsto & \overline{a} \end{array}$ *est un homomorphisme d'anneaux surjectif. On l'appelle la surjection canonique.*

Preuve. On vérifie facilement que ces deux lois confèrent à $\mathbb{Z}_n$ une structure d'anneau commutatif unitaire et que π_n est bien un homomorphisme d'anneaux. □

Remarque 3. L'anneau $\mathbb{Z}/n\mathbb{Z}$ est **l'anneau quotient** de l'anneau $\mathbb{Z}$ par l'idéal $I = n\mathbb{Z}$. D'où le résultat suivant.

Théorème 6. *Soit p un entier naturel. Alors*

$$p \text{ est premier si et seulement si } (\mathbb{Z}/p\mathbb{Z}, +, \cdot) \text{ est un corps.}$$

Dans ce cas le corps $\mathbb{Z}/p\mathbb{Z}$ est noté $\mathbb{F}_p$.

Preuve. On sait déjà que $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ est un anneau, donc $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ est un corps si et seulement si tout élément non nul de $\mathbb{Z}/n\mathbb{Z}$ est inversible. D'où le théorème 4 implique le résultat. □

2.3.2. **Le groupe multiplicatif $\mathbb{Z}_n^\times$.**
Rappelons que dans un anneau A, un élément a est dit inversible s'il existe un élément b de A tel que $ab = 1$, et nous savons que dans tout anneau, les éléments inversibles (pour le multiplication) forment un groupe multiplicatif. Cela s'applique sur l'anneau $\mathbb{Z}/n\mathbb{Z}$, et on a la définition suivante.

Définition 3. On dit qu'un élément $\overline{a} \in \mathbb{Z}_n$ est inversible s'il existe $\overline{b} \in \mathbb{Z}_n$ tel que $\overline{a}\overline{b} = \overline{1}$. On note par $\mathbb{Z}_n^\times$ l'ensemble des éléments inversibles de $\mathbb{Z}_n$. C'est un groupe pour la multiplication, puisque l'ensemble des unités d'un anneau quelconque A est un groupe multiplicatif.

Le théorème de Bézout, nous permet de déduire le résultat suivant.

Théorème 7. *Soit a un entier relatif. Les propriétés suivantes sont équivalentes :*

1. $\overline{a}$ *est inversible dans* $\mathbb{Z}_n$,
2. a *est premier avec* n,
3. $\overline{a}$ *est un générateur de* $(\mathbb{Z}_n, +)$.

Preuve. Dire que $\overline{a}$ est inversible dans $\mathbb{Z}_n$ équivaut à dire qu'il existe $\overline{b}$ dans $\mathbb{Z}_n$ tel que $\overline{a}\overline{b} = \overline{1}$, encore équivalent à dire qu'il existe b, q dans $\mathbb{Z}$ tels que $ab + qn = 1$, ce qui équivaut à dire que a et n sont premiers entre eux (théorème de Bézout).

En traduisant le fait que $\overline{a}$ est inversible dans $\mathbb{Z}_n$ par l'existence d'un entier relatif b tel que $\overline{a}\overline{b} = \overline{b}\overline{a} = \overline{1}$, cela est équivaut à dire que $\overline{1}$ est dans $\langle\overline{a}\rangle$, le groupe engendré par $\overline{a}$, car

$$\overline{1} = \overline{ba} = b \times \overline{a} = \underbrace{\overline{a} + \overline{a} + \cdots + \overline{a}}_{b \text{ fois}} \in \langle\overline{a}\rangle.$$

Donc ce groupe est $\mathbb{Z}_n$, puisque pour tout $\overline{x} \in \mathbb{Z}_n$ on a :

$$\overline{x} = \overline{x} \times \overline{1} = \underbrace{\overline{1} + \overline{1} + \cdots + \overline{1}}_{x \text{ fois}} \in \langle\overline{a}\rangle.$$

□

Remarque 4. La démonstration précédente montre que si a est inversible modulo n, son inverse peut être calculé à l'aide de l'algorithme d'Euclide.

Nous pouvons déterminé la structure de $\mathbb{Z}_n^\times$ dans le cas général. Mais notons qu'il suffit de le faire seulement dans le cas ou n est une puissance d'un nombre premier. En effet, lorsque on décompose n en produit de facteurs premiers sous la forme $n = \prod_i p_i^{r_i}$, le groupe $\mathbb{Z}_n^\times$ s'identifie via le théorème des restes chinois au produits des groupes $\mathbb{Z}/p_i^{r_i}\mathbb{Z}$, comme il résulte de la section suivante.

2.3.3. **Le théorème des restes chinois.**

Commençons d'abord par définir le système de congruences.

Définition 4. Un système de congruences est un système de la forme

$$(S) \qquad \begin{cases} x \equiv a_1 \pmod{m_1}, \\ x \equiv a_2 \pmod{m_2}, \\ \cdots \\ x \equiv a_r \pmod{m_r}, \end{cases}$$

où les a_i, et les m_i sont des entiers donnés.

Résoudre le système (S) consiste à déterminer tous les entiers $x \in \mathbb{Z}$ vérifiant le système. Lorsque les entiers m_i sont premiers entre eux deux à deux, alors le système (S) admet toujours des solutions. Ce résultat est connu sous le nom de Théorème des restes chinois.

Théorème 8 (Théorème des restes chinois). *Soient $m_1, m_2, \cdots, m_r$ des entiers positifs premiers entre eux deux à deux. Alors le système de congruences suivant :*

$$(S) \qquad \begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \cdots \\ x \equiv a_r \pmod{m_r} \end{cases}$$

admet une solution unique c modulo $M = m_1 \times m_2 \times \ldots \times m_r$ qui est donnée par la formule :

$$c = a_1 M_1 y_1 + a_2 M_2 y_2 + \ldots + a_r M_r y_r$$

avec $M_i = \dfrac{M}{m_i}$ et $M_i y_i \equiv 1 \pmod{m_i}$ pour tout i compris entre 1 et r.

Remarque 5. Le système (S) admet une infinité de solutions dans $\mathbb{Z}$ données par $x = c + kM$, $k \in \mathbb{Z}$. Deux solutions distinctes sont congrues modulo M.

Exemple 1.

1. Cherchons à résoudre le système de congruences suivant :

$$\begin{cases} x \equiv 1 \pmod{3} \\ x \equiv 2 \pmod{5} \\ x \equiv 3 \pmod{7} \end{cases}$$

Posons $M = 3 \times 5 \times 7 = 105$, alors

$$M_1 = \frac{105}{3} = 35 \text{ et } 35 \times y_1 \equiv 1 \pmod{3}, \text{ d'où } y_1 = 2,$$
$$M_2 = \frac{105}{5} = 21 \text{ et } 21 \times y_2 \equiv 1 \pmod{5}, \text{ d'où } y_2 = 1,$$
$$M_3 = \frac{105}{7} = 15 \text{ et } 15 \times y_3 \equiv 1 \pmod{7}, \text{ d'où } y_3 = 1.$$

Donc $x = 1 \times 35 \times 2 + 2 \times 21 \times 1 + 3 \times 15 \times 1 = 157 \equiv 52 \pmod{105}$.

2. Cherchons x tel que

$$\begin{cases} x \equiv 3 \pmod{17} \\ x \equiv 4 \pmod{11} \\ x \equiv 5 \pmod{6} \end{cases}$$

En appliquant le théorème chinois, on trouve que :

$$M = 17 \times 11 \times 6 = 1122,\ M_1 = 66,\ M_2 = 102 \text{ et } M_3 = 187.$$

L'inversion de chaque M_i (on peut utiliser l'algorithme d'Euclide) donne

$$y_1 = 8,\ y_2 = 4 \text{ et } y_3 = 1.$$

Par suite :

$$x = 3 \times 66 \times 8 + 4 \times 102 \times 4 + 5 \times 187 \times 1 = 4151 \equiv 785 \pmod{1122}.$$

Preuve du théorème 11. Il suffit de démontrer le théorème pour un système à deux équations et d'appliquer ensuite la récurrence :

$$(S) \qquad \begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2}. \end{cases}$$

Par l'identité du Bezout, il existe u et v deux entiers tels que $um_1 + vm_2 = 1$. Donc l'entier c défini par l'égalité $c = a_2um_1 + a_1vm_2$ est solution du système puisque
$\begin{cases} c = a_1(1 - um_1) + a_2um_1 = a_1 + um_1(a_2 - a_1) \equiv a_1 \pmod{m_1}, \\ c = a_2(1 - vm_2) + a_1vm_2 = a_2 + um_1(a_1 - a_2) \equiv a_2 \pmod{m_2}. \end{cases}$

Il est aussi facile de vérifier que pour tout entier $k \in \mathbb{Z}$, l'entier $x = c + km_1m_2$ est aussi solution du système (S).

Inversement, soit x une solution de (S), i.e., $\begin{cases} x = a_1 + m_1k_1, \ k_1 \in \mathbb{Z} \\ x = a_2 + m_2k_2, \ k_2 \in \mathbb{Z}. \end{cases}$
Alors après un petit calcule on obtient que $x-c$ est congru à 0 modulo m_1 et modulo m_2, donc m_1 et m_2 divisent $x-c$, par suite m_1m_2 divise $x-c$ puisque $pgcd(m_1, m_2) = 1$. □

Remarque 6. Le théorème des restes chinois nous dit qu'il y a une seule solution x vérifiant $0 \leq x < M$, c-à-d, il y a une solution unique dans $\mathbb{Z}/M\mathbb{Z}$. Chose que nous pouvons énoncer comme suit.

Théorème 9 (**Théorème des restes chinois**). *Soient $m_1, m_2, \cdots, m_r$ des entiers positifs premiers entre eux deux à deux. Posons $M = m_1 \times m_2 \times \ldots \times m_r$, alors les anneaux $\mathbb{Z}/M\mathbb{Z}$ et $\mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \times \ldots \times \mathbb{Z}/m_r\mathbb{Z}$ sont isomorphes. Et l'application*

$$\begin{array}{rccl} \psi : & \mathbb{Z}/M\mathbb{Z} & \longrightarrow & \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \times \ldots \times \mathbb{Z}/m_r\mathbb{Z} \\ & \overline{x} \pmod{M} & \longmapsto & (\overline{x} \pmod{m_1}, \overline{x} \pmod{m_2}, \cdots, \overline{x} \pmod{m_r}) \end{array}$$

réalise un isomorphisme entre ces deux anneaux.

Preuve. On vérifie facilement que ψ est un homomorphisme d'anneaux. Il résulte du théorème précédent 8 que ψ est surjective. En effet, soit $(\overline{a_1}, \overline{a_2}, \cdots, \overline{a_r}) \in \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \times \ldots \times \mathbb{Z}/m_r\mathbb{Z}$, existe-t-il $\overline{x} \in \mathbb{Z}/M\mathbb{Z}$ tel que

$$\psi(\overline{x}) = (\overline{a_1}, \overline{a_2}, \cdots, \overline{a_r}) \Longleftrightarrow \begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \cdots \\ x \equiv a_r \pmod{m_r}. \end{cases}$$

L'existence de $\overline{x}$ est assuré par le théorème 8. Donc ψ bijective puisque les deux anneaux $\mathbb{Z}/M\mathbb{Z}$ et $\mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \times \ldots \times \mathbb{Z}/m_r\mathbb{Z}$ ont même nombre d'éléments M. □

Corollaire 7. *Soient H et K deux groupes cycliques d'ordres respectifs m et n. Le groupe produit $H \times K$ est cyclique si et seulement si m et n sont premiers entre eux.*

Preuve. On sait que les groupes H et K sont respectivement isomorphes aux groupes $\mathbb{Z}/m\mathbb{Z}$ et $\mathbb{Z}/n\mathbb{Z}$ (voir corollaire 16 page 23), donc la condition est suffisante d'après le théorème des restes chinois.

Inversement, elle est nécessaire car si $pgcd(m, n) = d > 1$, alors on pose $m = dm_1$ et $n = dn_1$. Soit $q = ppcm(m, n) = dm_1n_1 = n_1m = m_1n$. Comme $mn = qd$, on a $q < mn$, et tout élément $(x, y) \in H \times K$ vérifie $(x, y)^q = (x^q, y^q) = (x^{n_1m}, y^{m_1n}) = (1, 1)$. Il n'existe donc pas dans $H \times K$ d'élément d'ordre mn, ainsi $H \times K$ n'est pas cyclique, ce qui est absurde. □

Corollaire 8. *Soit m et n deux entiers premiers entre eux, les groupes multiplicatifs $(\mathbb{Z}/mn\mathbb{Z})^\times$ et $(\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$ sont isomorphes.*

Preuve. Les anneaux $\mathbb{Z}/mn\mathbb{Z}$ et $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ sont isomorphes, donc les groupes $(\mathbb{Z}/mn\mathbb{Z})^\times$ et $(\mathbb{Z}/m\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z})^\times$ le sont aussi. Il est facile de voir que $(\mathbb{Z}/m\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z})^\times = (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$, puisque le groupe d'unités de l'anneau $A \times B$ est $U(A \times B) = U(A) \times U(B)$. □

2.3.4. **L'indicateur d'Euler.**

Définition 5. Soit n un entier naturel non nul. On appelle indicateur d'Euler de n le nombre des entiers compris entre 1 et n et qui sont premiers avec n, il est noté $\varphi(n)$.

C'est-à-dire φ est la fonction définie par :

$$\begin{array}{rccl} \varphi & : & \mathbb{N}^* & \longrightarrow & \mathbb{N}^* \\ & & n & \longmapsto & \text{card}(A), \text{ où } A = \{m \in \mathbb{N}^* \mid m \leq n \text{ et } m \text{ premier avec } n\}. \end{array}$$

Exemples 2.

- $\varphi(8) = 4$ car parmi les nombres de 1 à 8, seuls les quatre nombres 1, 3, 5 et 7 sont premiers avec 8.
- $\varphi(6) = 2$ car seuls 1 et 5 sont premier avec 6.
- $\varphi(5) = 4$.

Remarque 7. Si n est premier, alors tout entier compris entre 1 et $n - 1$ est premier avec n. Par suite $\varphi(n) = n - 1$.

Le théorème 7 nous permet d'énoncer le résultat suivant.

Proposition 4. *Pour tout entier naturel $n \geq 1$, $\varphi(n)$ est égal au nombre*

a. de générateurs du groupe cyclique $(\mathbb{Z}_n, +)$.
b. d'éléments du groupe multiplicatif $\mathbb{Z}_n^\times = (\mathbb{Z}/n\mathbb{Z})^\times$.

C'est-à-dire que les générateurs du groupe $(\mathbb{Z}/n\mathbb{Z}, +)$ sont les classes $\overline{a}$ modulo n, où $1 \leq a \leq n$ et $a \wedge n = 1$, et sont aussi les éléments de l'ensemble $\mathbb{Z}_n^\times = (\mathbb{Z}/n\mathbb{Z})^\times$ dont l'ordre est $\varphi(n)$.

Théorème 10 (Euler). *Pour tout entier relatif a premier avec n, on a : $a^{\varphi(n)} \equiv 1\ [n]$.*

Preuve. Si a est premier avec n, alors $\overline{a}$ appartient à $\mathbb{Z}_n^\times$ qui est un groupe d'ordre $\varphi(n)$. Donc l'ordre de $\overline{a}$ divise $\varphi(n)$ (théorème de Lagrange), ce qui entraîne $\overline{a}^{\varphi(n)} = \overline{1}$, ou encore $a^{\varphi(n)} \equiv 1\ [n]$. □

Pour n premier, on a $\varphi(n) = n - 1$ et le théorème d'Euler devient le petit théorème de Fermat.

Théorème 11 (Petit Théorème de Fermat). *Soit p un nombre premier, alors pour tout $a \in \mathbb{Z}$ on a : $a^p \equiv a \pmod{p}$. De plus, si $a \wedge p = 1$, alors $a^{p-1} \equiv 1 \pmod{p}$.*

Preuve. Soit $a \in \mathbb{Z}$. Il est connu qu'on a ou bien a est multiple de p ou bien a est premier avec p. Soit $\overline{a}$ la classe de a modulo p.
- Si a est multiple de p, a^p est aussi multiple de p, on a donc $a^p \equiv a \equiv 0 \pmod{p}$.
- Si $\text{pgcd}(a, p) = 1$, alors $\overline{a} \in (\mathbb{Z}/p\mathbb{Z})^\times$ d'après le théorème 7. Or $(\mathbb{Z}/p\mathbb{Z})^\times$ est d'ordre $p - 1$ donc $\overline{a}^{p-1} = \overline{1}$. Ceci s'écrit $a^{p-1} \equiv 1 \pmod{p}$, il en résulte $a^p \equiv a \pmod{p}$. □

Dans le cas où n est premier, alors tous les éléments de $\mathbb{Z}_n - \{0\}$ sont inversibles et en conséquence $\mathbb{Z}_n$ est un corps. En fait on a le résultat plus précis suivant.

Théorème 12. *Pour $n \geq 2$ il y a équivalence entre :*

1. *n est premier ;*
2. *$\varphi(n) = n - 1$;*
3. *$\mathbb{Z}_n$ est un corps ;*
4. *$\mathbb{Z}_n$ est intègre.*

Preuve. Pour n premier, on a $\varphi(n) = n - 1$, donc $\mathbb{Z}_n$ est un corps et c'est un anneau intègre.

Supposons $\mathbb{Z}_n$ est intègre, montrons que les seuls diviseurs positifs de n sont 1 et n. Soit d un diviseur de n différent de n dans $\mathbb{N}$. Il existe donc un entier q compris entre 2 et n tel que $n = qd$, donc dans $\mathbb{Z}_n$ on a $\overline{q}\overline{d} = \overline{0}$ avec $\overline{d} \neq \overline{0}$, ce qui impose $\overline{q} = \overline{0}$, donc $q = n$ et $d = 1$. L'entier n est donc premier. □

Le théorème des restes chinois nous permet de montrer le résultat suivant.

Théorème 13. *La fonction indicatrice d'Euler φ est multiplicative, c'est-à-dire, si m et n sont premiers entre eux, alors $\varphi(mn) = \varphi(m)\varphi(n)$.*

Preuve. Comme $\varphi(k)$ est le nombre des inversibles dans $\mathbb{Z}/k\mathbb{Z}$, alors le résultat est assuré par le corollaire 8, puisque les groupes $(\mathbb{Z}/mn\mathbb{Z})^\times$ et $(\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$ sont isomorphes. □

Corollaire 9. *Si m et n sont deux entiers premiers distincts, alors $\varphi(mn) = \varphi(m)\varphi(n)$.*

Preuve. Si m et n sont deux entiers premiers, alors m et n sont premiers entre eux ; donc le Théorème 13 implique le résultat. □

Proposition 5.
Si p est premier, alors

$$\forall m \in \mathbb{N}^*,\ \varphi(p) = p - 1 \quad et \quad \varphi(p^m) = p^m - p^{m-1} = p^{m-1}(p-1) = p^m\left(1 - \frac{1}{p}\right).$$

Preuve. Soit p un nombre premier. Par définition $\varphi(p^m)$ est le cardinal de l'ensemble

$$F(p^m) = \{k \in \mathbb{N} \mid 1 \leq k \leq p^m \text{ et } k \wedge p^m = 1\} = \{k \in \mathbb{N} \mid 1 \leq k \leq p^m \text{ et } k \wedge p = 1\}.$$

Le complémentaire de $F(p^m)$ est l'ensemble des entiers k compris entre 1 et p^m et qui ne sont pas premiers avec p^m. Soit k un tel entier. Alors k n'est pas premier avec p^m si, et seulement si, $k \wedge p^m = \delta$ et $\delta \neq 1$, ceci est équivalent à dire que k est divisible par p, ce qui est équivaut aussi à dire que k est un multiple de p, i.e., $k = mp$ avec $1 \leq m \leq p^{m-1}$, il y a donc p^{m-1} possibilités. On en déduit alors que : $\varphi(p^m) = p^m - p^{m-1} = p^{m-1}(p-1)$. □

Théorème 14. *Si $n \geq 2$ a pour décomposition en facteurs premiers $n = \prod_{i=1}^{i=r} p_i^{\alpha_i}$ avec $2 \leq p_1 < p_2 < \cdots < p_r$ des nombres premiers et les α_i sont des entiers naturels non nuls, alors on a :*

$$\varphi(n) = \prod_{i=1}^{i=r} \varphi(p_i^{\alpha_i}) = \prod_{i=1}^{i=r} p_i^{\alpha_i - 1}(p_i - 1) = n \prod_{i=1}^{i=r}\left(1 - \frac{1}{p_i}\right)$$

Preuve. Immédiat par le théorème 13 et la proposition 5. □

Proposition 6. *Pour tout $n \geq 3$, $\varphi(n)$ est un entier pair.*

Preuve. Pour $n = 2^m$ avec $m \geq 2$, on a $\varphi(n) = 2^{m-1}$ qui est pair.
Pour $n = 2^m \prod_{i=1}^{i=r} p_i^{\alpha_i} = p_1^{\alpha_1} M$ avec $m \geq 0$, $r \geq 1$ et tous les p_i sont premiers impairs, on a :

$$\varphi(n) = \varphi(p_1^{\alpha_1})\varphi(M) = p_1^{\alpha_1 - 1}(p_1 - 1)\varphi(M)$$

qui est pair, puisque $p_1 - 1$ l'est. □

Proposition 7. *Soient m et n deux entiers naturels non nuls tels que m divise n, alors $\varphi(m)$ divise $\varphi(n)$.*

Preuve. Posons $n = mq$, alors si un premier p divise n sans diviser m il divisera q. Soient P_m (resp. P_n) l'ensemble des diviseurs premiers de m (resp. de n). D'après le théorème 14, on a les égalités :

$$\frac{\varphi(n)}{\varphi(m)} = \frac{n}{m} \prod_{p \in P_n - P_m} \left(1 - \frac{1}{p}\right) = q \prod_{p \in P_n - P_m} \left(1 - \frac{1}{p}\right) = \frac{q}{\prod_{p \in P_n - P_m} p} \left(\prod_{p \in P_n - P_m} (p-1) \right).$$

D'autre part, pour tout nombre premier $p \in P_n - P_m$, p divise n sans diviser m, donc p divise $\frac{n}{m} = q$. Il en résulte que q est divisible par le nombre $\prod_{p \in P_n - P_m} p$; par suite le deuxième membre de l'égalité précédente est un entier, d'où le résultat. □

On déduit également que $\varphi(n)$ est compris entre 1 et n (ce qui se voit aussi avec la définition).

3. Groupes finis

3.1. **Généralités.** Commençons par rappeler le résultat suivant, qui est une propriété essentielle des groupes finis.

Théorème 15 (Lagrange)**.** *Dans un groupe fini G, l'ordre d'un sous-groupe H divise celui de G.*

Preuve. Pour g fixé dans le groupe G, l'application $h \longmapsto gh$ est une bijection de G sur G et sa restriction à H réalise une bijection de H sur gH. Il en résulte que gH et H ont même cardinal.

L'ensemble des classes à gauche suivant H réalise une partition de G et ces classes sont en nombre fini de même cardinal égal à celui de H, il en résulte que : $\text{card}(G) = [G : H]\text{card}(H)$. □

L'étude d'un groupe comporte l'étude de tous ses sous-groupes, le théorème précédent permet de cerner la recherche des sous-groupes, un groupe d'ordre 8 par exemple ne possédera pas de sous-groupe d'ordre 3, 5 ou 7. De même qu'un groupe d'ordre premier ne possédera que ses deux sous-groupes triviaux.

Définition 6. Soient G un groupe et soit $a \in G$. On appelle ordre de a l'ordre du sous-groupe de G engendré par a, c-à-d, $\text{card}(\langle a\rangle) = \text{card}(\{a^k \mid k \in \mathbb{Z}\})$. Le seul élément de G d'ordre 1 est son élément neutre e.

Remarque 8. Soit a un élément d'un groupe G. On dit que a est d'ordre fini dans G si le groupe $\langle a\rangle$ est fini.

Théorème 16. *Soit G un groupe fini d'élément neutre e, et soit $a \in G$ d'ordre m. Alors*

1. *m divise l'ordre de G.*
2. *m est le plus petit entier positif tel que $a^m = e$.*
3. *Les éléments $e, a, a^2, \cdots, a^{m-1}$ sont tous distincts dans G.*
4. $\langle a\rangle = \{e, a, a^2, \cdots, a^{m-1}\}$.

Preuve.

1. Découle du Théorème de Lagrange.
2. Si $m = 1$, c'est évident. On suppose $m > 1$, la démonstration se fait en deux étapes :

étape 1: on montre qu'il existe au moins un entier $1 \leq \ell \leq m$ tel que $a^\ell = e$. Soit l'ensemble

$$H = \{e, a, a^2, \cdots, a^m, a^{m+1}\} \subset \langle a \rangle.$$

Comme a est d'ordre m, alors il existe au moins deux éléments égaux dans H.

Donc $\exists k$, $\exists \ell$, $1 \leq \ell \leq m$ et $1 \leq \ell + k \leq m + 1$ vérifiant $a^{k+\ell} = a^k$.

D'où $1 \leq \ell \leq m$ et $a^\ell = e$.

étape 2: soit n le plus petit entier strictement positif tel que $a^n = e$, alors il résulte de l'étape 1, que $n \leq \ell \leq m$.

Montrons que $\langle a \rangle \subset \{e, a, a^2, \cdots, a^{n-1}\}$. Soit $k \in \mathbb{Z}$, la division euclidienne de k par n s'écrit $k = nq + r$, avec $0 \leq r \leq n - 1$, ce qui donne

$$a^k = (a^n)^q a^r = a^r \in \{e, a, a^2, \cdots, a^{n-1}\}, \text{ c-à-d,}$$
$$\langle a \rangle \subset \{e, a, a^2, \cdots, a^{n-1}\},$$

il en résulte $m = \text{card}(\langle a \rangle) \leq \text{card}(\{e, a, a^2, \cdots, a^{n-1}\}) \leq n$, c'est-à-dire , en tenant compte de l'étape 1, que $m = \text{card}(\langle a \rangle) = \text{card}(\{e, a, a^2, \cdots, a^{n-1}\}) = n$. Cela démontre 2. et 4.

3. Ce point résulte du fait que $m = \text{card}(\{e, a, a^2, \cdots, a^{m-1}\})$. □

Il résulte de ce théorème une série de corollaires.

Corollaire 10. *Soit G un groupe fini d'ordre n d'élément neutre e, alors pour tout $a \in G$, $a^n = e$.*

Preuve. Soit $a \in G$ d'ordre m, donc m divise l'ordre n de G ; soit alors $k \geq 1$ l'entier tel que $n = mk$, d'où $a^n = (a^m)^k = e^k = e$. □

Corollaire 11. *Tout groupe fini G d'ordre premier p est cyclique et engendré par l'un quelconque de ses éléments distincts de e.*

Preuve. Soit $g \in G$, $g \neq e$. Comme $g \in \langle g \rangle$ et $e \in \langle g \rangle$, alors l'ordre m de g est ≥ 2 et divise p, d'où $m = p$, c'est-à-dire $\langle g \rangle = G$. □

Corollaire 12. *Soit G un groupe fini d'ordre n. Pour chaque entier positif k, désignons par $\alpha(k)$ le nombre des éléments d'ordre k de G, alors on a :*

$$n = \sum_{k|n} \alpha(k).$$

Preuve. Notons d'abord que l'ensemble des diviseurs de n est fini.
On sait que si k ne divise pas n, alors $\alpha(k) = 0$.
Si k divise n, désignons par G_k l'ensemble des éléments d'ordre k de G, alors

$$\alpha(k) = \text{card}(G_k).$$

Par suite, tout élément de G appartient à un et un seul ensemble G_k, c'est-à-dire les diviseurs de n forment une partition de G. D'où le résultat. □

Le théorème suivant est souvent utiliser pour déterminer l'ordre d'un élément d'un groupe fini G.

Théorème 17. *Soient G un groupe fini et a, b dans G d'ordres $\theta(a)$ et $\theta(b)$ respectivement. Alors pour tout $k \in \mathbb{N}^*$, on a :*

1. $a^k = e \iff \theta(a)|k$.
2. *On a* $\theta(a^k) = \dfrac{\theta(a)}{\theta(a) \wedge k}$ *(en particulier* $\theta(a^{-1}) = \theta(a)$*).*
3. *Si k divise $\theta(a)$, alors on a* $\theta(a^k) = \dfrac{\theta(a)}{|k|}$.
4. *Si k est premier avec $\theta(a)$, on a alors* $\theta(a) = \theta(a^k)$
5. *Si $ab = ba$, alors ab est d'ordre fini divisant $\theta(a) \vee \theta(b)$.*
   Dans le cas où $\langle a\rangle \cap \langle b\rangle = \langle e\rangle$, on a $\theta(ab) = \theta(a) \vee \theta(b)$.
   De plus, si $\theta(a)$ et $\theta(b)$ sont premiers entre eux, alors $\langle a\rangle \cap \langle b\rangle = \langle e\rangle$, et $\theta(ab) = \theta(a) \vee \theta(b) = \theta(a)\theta(b)$.

Preuve. 1. Notons m l'ordre de a. Si m divise k, posons $k = mk'$, alors $a^k = a^{mk'} = (a^m)^{k'} = e^{k'} = e$.

Réciproquement, si $a^k = e$, alors la division euclidienne de k par m donne $k = mk' + r$ avec $0 \leq r \leq m-1$. Alors $e = a^k = a^{mk'+r} = a^r$. On déduit du point 2. du théorème 16 que $r = 0$. D'où le résultat.
2. Soit $\delta = m \wedge k$, alors il existe deux entiers n', k' premiers entre eux tels que $m = \delta n'$, $k = \delta k'$. Désignons par j l'ordre de a^k. On a d'une part,

$$(a^k)^{n'} = a^{kn'} = a^{\delta k' n'} = a^{mk'} = e^{k'} = e.$$

Donc j divise n'. D'autre part,

$$\begin{aligned}(a^k)^j = a^{kj} = e &\implies \exists q \in \mathbb{Z},\ kj = qm,\ \text{car } m|kj \\ &\implies \exists q \in \mathbb{Z},\ \delta k' j = q\delta n' \\ &\implies \exists q \in \mathbb{Z},\ k'j = qn' \\ &\implies n' \text{ divise } j \ \ \text{(par le théorème de Gauss).}\end{aligned}$$

Par suite $j = n'$, d'où l'ordre de a^k est $j = n' = \dfrac{m}{m \wedge k}$.
Pour les autres points voir le cours d'Algèbre 6 de S4. □

Le corollaire suivant résulte immédiatement du point 2. du Théorème 17.

Corollaire 13. *Soit G un groupe fini. Soient $a \in G$ d'ordre m et k un entier positif. L'ordre de a^k est égal à m si, et seulement si, k est premier avec m.*

Corollaire 14. *Dans un groupe abélien G, l'ensemble des ordres de ses éléments est stable par* ppcm*, c'est-à-dire que le* ppcm *des ordres de deux éléments de G est ordre d'un élément de G.*

Preuve. Soient a et b deux éléments de G d'ordres respectivement m et n. Il faut donc construire un élément de G dont l'ordre est le ppcm de m et n.

Posons $r = \text{ppcm}(m, n)$ et $\delta = \text{pgcd}(m, n)$, comme $r.\delta = mn$, alors il existe m' et n' premiers entre eux tels que $r = m'n'$ (on peut aussi utiliser la décomposition en facteurs premiers pour justifier l'existence de m' et n'). Donc $x = a^{\frac{m}{m'}}$ (resp. $y = b^{\frac{n}{n'}}$) est d'ordre m' (resp. n'), on obtient le résultat par application du point 5 du Théorème 17 au produit xy. □

3.2. **Groupes cycliques.** Rappelons d'abord que tout groupe cyclique est commutatif. Le théorème suivant est une conséquence directe du Théorème 16.

Théorème 18. *Soit G un groupe cyclique fini d'ordre n et d'élément neutre e, et soit $a \in G$ un générateur de G. Alors*

1. *a est d'ordre n.*
2. *Tous les éléments $e, a, a^2, \cdots, a^{n-1}$ sont distincts dans G.*
3. *$G = \langle a \rangle = \{a^k \mid k \in \mathbb{N}\} = \{e, a, a^2, \cdots, a^{n-1}\}$, en notation additive*
   $G = \langle a \rangle = \{ka \mid k \in \mathbb{N}\} = \{e, a, 2a, \cdots, (n-1)a\}$.

Remarque 9. Un groupe G est cyclique d'ordre n si et seulement s'il existe $a \in G$ d'ordre n.

Corollaire 15. *Deux groupes cycliques de même ordre sont isomorphes.*

Preuve. Soient $G = \langle a \rangle$ et $H = \langle b \rangle$ deux groupes cycliques de même ordre n, de générateurs a et b respectivement. Soit l'application $f : G \longrightarrow H$ définie par :

$$\forall k \in \mathbb{N}, \begin{cases} f(a^k) = b^k \text{ si } G \text{ et } H \text{ sont multiplicatifs,} \\ f(ka) = kb \text{ si } G \text{ et } H \text{ sont additifs,} \\ f(a^k) = kb \text{ si } G \text{ est multiplicatif et } H \text{ est additif,} \\ f(ka) = b^k \text{ si } G \text{ est additif et } H \text{ est multiplicatif.} \end{cases}$$

Il est simple de voir que l'application f est un morphisme, et comme elle est surjective par construction, alors f est un isomorphisme de groupes. □

Corollaire 16. *Tout groupe cyclique d'ordre n est isomorphe à $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$.*

Preuve. Soit G un groupe cyclique d'ordre n, comme $\mathbb{Z}_n$ est cyclique d'ordre n (Théorème 3), alors G est isomorphe à $\mathbb{Z}_n$ par le Corollaire 15. □

Remarque 10. Tout groupe fini d'ordre un nombre premier p est isomorphe au groupe additif $(\mathbb{Z}/p\mathbb{Z}, +)$.

Une question importante concerne la description des générateurs d'un groupe cyclique : en particulier, combien y a-t-il de générateurs dans un groupe cyclique d'ordre n ? Pour répondre à cette question, on va utiliser la fonction indicatrice d'Euler.

Théorème 19. *Un groupe cyclique G d'ordre n possède $\varphi(n)$ générateurs distincts. De plus, si g est un générateur de G, les $\varphi(n)$ générateurs de G sont les éléments g^k, où $1 \leq k \leq n-1$ et* $\text{pgcd}(n, k) = 1$.

Preuve. D'après le Théorème 18, tous les éléments g^k sont distincts pour $1 \leq k \leq n-1$. Le Corollaire 13 implique que si $k > 0$, alors g^k est générateur de G si, et seulement si, il est d'ordre n, mais ceci est équivaut à dire que $\text{pgcd}(k, n) = 1$. □

Le résultat qui suit nous assure que les sous-groupes d'un groupe cyclique sont cycliques.

Théorème 20. *Soit $G = \langle g \rangle$ un groupe cyclique d'ordre n. Alors tous les sous-groupes de G sont cycliques d'ordre un diviseur de n. Réciproquement, pour tout diviseur d de n, il existe un unique sous-groupe H de G d'ordre d, c'est le groupe cyclique engendré par $g^{\frac{n}{d}}$: $H = \langle g^{\frac{n}{d}} \rangle$*

Preuve. Soit H un sous-groupe de G d'ordre d, alors $d|n$ (Théorème de Lagrange).
- Si $d = 1$, on a alors $H = \{e\} = \langle g^n \rangle$.
- Si $d \geq 2$, H n'est pas réduit à $\{e\}$, donc il existe un entier k compris entre 1 et $n-1$ tel que $g^k \in H$. Posons

$$p = \min(\{k \in \{1, \cdots, n-1\} |\ g^k \in H\}).$$

Donc $\forall q \in \mathbb{N}$, $g^{pq} = (g^p)^q \in H$. En écrivant, pour tout $h = g^k \in H$, $k = pq + r$ avec $0 \leq r \leq p-1$ (division euclidienne par p), on a $g^r = g^k (g^{pq})^{-1} \in H$ et nécessairement $r = 0$, puisque p est le plus petit entier qui a cette propriété. On a donc $H \subset \langle g^p \rangle \subset H$, soit $H = \langle g^p \rangle$.

Comme $g^n = e \in H$, alors on déduit que n est un multiple de p et que l'ordre de H est $d = \dfrac{n}{n \wedge p} = \frac{n}{p}$, c'est-à-dire que $H = \langle g^{\frac{n}{d}} \rangle$. Un tel sous-groupe d'ordre d est donc unique.

Réciproquement, Pour tout diviseur d de n, $H = \langle g^{\frac{n}{d}} \rangle$ est un sous-groupe cyclique de G et l'ordre de $g^{\frac{n}{d}}$ est $\dfrac{n}{n \wedge \frac{n}{d}} = d$. □

Corollaire 17. *Tous les sous-groupes de $\mathbb{Z}_n$ sont cycliques d'ordre un diviseur de n. Réciproquement pour tout diviseur d de n, il existe un unique sous-groupe de $\mathbb{Z}_n$ d'ordre d, c'est le groupe cyclique engendré par $\overline{q} = \dfrac{\overline{n}}{\overline{d}}$: $H = \langle \overline{q} \rangle = \{\overline{0}, \overline{q}, \cdots, (d-1)\overline{q}\}$.*

Corollaire 18. *Soit $G = \langle g \rangle$ un groupe cyclique d'ordre n. Pour chaque diviseur d de n, l'ensemble*

$$U_d = \{x \in G \mid x^d = e\}$$

est un sous-groupe d'ordre d de G égal à $\langle g^{\frac{n}{d}} \rangle$. Il en résulte que G possède exactement $\varphi(d)$ éléments d'ordre d.

Preuve. Il suffit de montrer que U_d est un sous-groupe de G d'ordre d. Comme G est abélien, alors U_d est un sous-groupe de G. Par suite le Corollaire 10 nous implique que $H = \langle g^{\frac{n}{d}} \rangle \subset U_d$.

Montrons que U_d est d'ordre d. Posons $n = dm$ on a l'équivalence, pour tous entier $k \in \mathbb{N}^*$ et $x = g^k \in U_d$, on a :

$$(g^k)^d = g^{kd} = e \Longleftrightarrow kd \text{ est un multiple de } n = dm \Longleftrightarrow k \text{ est un multiple de } m.$$

Les éléments de U_d sont donc g^m, g^{2m}, $\cdots$, $g^{dm} = g^n = e$. Ces éléments sont tous distincts car $\ell m \leq n$ pour tout $\ell = 1, 2, \cdots, d$. Le sous-groupe U_d est donc cyclique

d'ordre d, engendré par g^m. Par suite il possède $\varphi(d)$ générateurs qui sont les seuls éléments d'ordre d de U_d donc de G. □

Corollaire 19. *Tout entier naturel n est la somme des indicateurs de ses diviseurs :*

$$n = \sum_{d|n} \varphi(d),$$

c'est-à-dire, si d_1, d_1, $\cdots$, d_r sont les diviseurs de n, alors

$$\varphi(d_1) + \varphi(d_2) + \cdots + \varphi(d_r) = n.$$

Preuve. C'est une conséquence des corollaires 18 et 12. □

Théorème 21. *Soit G un groupe d'ordre n. Pour chaque diviseur d de n, posons*

$$U_d = \{x \in G \mid x^d = e\} \text{ et } \alpha(d) = \text{le nombre d'éléments d'ordre } d \text{ de } G.$$

Les conditions suivantes sont équivalentes.

1. *Pour chaque diviseur d de n,* $\text{card}(U_d) \leq d$.
2. *Pour chaque diviseur d de n,* $\alpha(d) \leq \varphi(d)$.
3. *Pour chaque diviseur d de n,* $\alpha(d) = \varphi(d)$.
4. *G est cyclique.*
5. *Pour chaque diviseur d de n,* $\text{card}(U_d) = d$.

Preuve. Notons que si G n'est pas commutatif, U_d n'est pas nécessairement un sous-groupe de G.

1. $\Longrightarrow$ 2. Si $\alpha(d) \geq 1$, alors il existe un élément $x \in G$ d'ordre d, donc $x \in U_d$, par suite par le Corollaire 10, $\langle x \rangle \subset U_d$. D'où $\text{card}(\langle x \rangle) = d \leq \text{card}(U_d)$. Sous l'hypothèse 1., on en déduit que $d = \text{card}(U_d)$, donc $\langle x \rangle = U_d$.

Le sous-groupe $\langle x \rangle$ possède $\varphi(d)$ générateurs, et l'égalité $\langle x \rangle = U_d$ implique que ce sont les seuls éléments d'ordre d de G. On en déduit $\alpha(d) = \varphi(d)$. Autrement dit, ou bien $\alpha(d) = 0$ ou bien $\alpha(d) = \varphi(d)$, d'où $\alpha(d) \leq \varphi(d)$.

2. $\Longrightarrow$ 3. On sait que $n = \sum_{d|n} \varphi(d) = \sum_{d|n} \alpha(d)$, donc si la condition 2 ; est vérifiée on déduit que $\alpha(d) = \varphi(d)$ pour tout diviseur d de n.

3. $\Longrightarrow$ 4. Pour $d = n$, on déduit de la condition 3. que $\alpha(n) = \varphi(n) \geq 1$, le groupe G possède donc un élément d'ordre n, il est par suite cyclique.

4. $\Longrightarrow$ 5. Cette implication est assurée par le Corollaire 18.

5. $\Longrightarrow$ 1. Simple. □

3.3. **Structure de $(\mathbb{Z}/p^n\mathbb{Z})^\times$ avec p un premier impair.**
Pour déterminer la structure de $(\mathbb{Z}/p^n\mathbb{Z})^\times$, nous avons besoin des lemmes suivants.

Lemme 2. *Soient n un entier naturel, p un nombre premier impair et a un entier, alors*

1. $(1+p^na)^p \equiv 1+p^{n+1}a \pmod{p^{n+2}}$,
2. $(1+pa)^{p^n} \equiv 1+p^{n+1}a \pmod{p^{n+2}}$.

Preuve. Par la formule du binôme de Newton on obtient

$$(1+p^na)^p = 1+pp^na+\complement_p^2 p^{2n}a^2+p^{3n}(\cdots),$$

or p divise $\complement_p^2$, $2n+1 \geq n+2$ et $3n \geq n+2$, ceci donne le premier point.

Le deuxième point se démontre par récurrence sur n. Supposons qu'on a :

$$(1+pa)^{p^{n-1}} = 1+p^na+p^{n+1}b,$$

on en déduit par application du premier point que

$$(1+pa)^{p^n} = (1+p^n(a+pb))^p \equiv 1+p^{n+1}(a+pb) \pmod{p^{n+2}}.$$

Ce qui montre le résultat. □

Lemme 3. *Soient $n \geq 2$ un entier naturel et u un entier congru à $1 \pmod p$. Alors $u^{p^{n-1}} \equiv 1 \pmod{p^n}$, de plus $u \pmod{p^n}$ est un élément d'ordre p^{n-1} du groupe $(\mathbb{Z}/p^n\mathbb{Z})^\times$ si et seulement si $u \not\equiv 1 \pmod{p^2}$.*

Preuve. Posons $u = 1+pa$, alors par le Lemme 2 et pour la valeur $n-1$, on a $u^{p^{n-1}} \equiv 1 \pmod{p^n}$ et l'ordre de $u \pmod{p^n}$ divise p^{n-1}. Dire qu'il lui est égal revient à dire que $u^{p^{n-2}} \not\equiv 1 \pmod{p^n}$. Or le même Lemme et pour $n-2$ affirme que cette condition est équivalente à $a \not\equiv 0 \pmod p$, c'est-à-dire que $u \not\equiv 1 \pmod{p^2}$. □

Théorème 22. *Soit p un entier premier. Alors pour chaque diviseur d de $p-1$, il existe d éléments de $(\mathbb{Z}/p\mathbb{Z})^\times$ d'ordre $\varphi(d)$. En particulier $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique d'ordre $p-1$.*

Preuve. La première partie du théorème est assirée par le Corollaire 18. Notons $\alpha(d)$ le nombre d'éléments d'ordre d de $(\mathbb{Z}/p\mathbb{Z})^\times$, alors nous avons déjà vu dans la preuve du Théorème 21 que $\alpha(d) = \varphi(d)$. Donc pour $d = p-1$, on déduit qu'il existe des éléments d'ordre $p-1$ qui est bien l'ordre de $(\mathbb{Z}/p\mathbb{Z})^\times$. D'où le résultat. □

Théorème 23. *Soient p un entier premier impair et $n \geq 2$ un entier naturel. Alors le groupe $(\mathbb{Z}/p^n\mathbb{Z})^\times$ est cyclique d'ordre $\varphi(p^n) = p^n - p^{n-1} = p^{n-1}(p-1)$.*

Preuve. Nous avons déjà vu (Proposition 4) que le groupe $(\mathbb{Z}/p^n\mathbb{Z})^\times$ est d'ordre $\varphi(p^n) = p^n - p^{n-1}$. Comme p^{n-1} et $p-1$ sont premiers entre eux, alors, compte tenu du Corollaire 14, il suffit de montrer qu'il possède un élément d'ordre p^{n-1} et un élément d'ordre un multiple de $p-1$. La première assertion est garantie par le Lemme 3 en prenant $a = u = 1+p$ qui est d'ordre p^{n-1}. D'autre part, par la Proposition 4, il existe un entier $b \bmod p$ d'ordre $\varphi(p) = p-1$, donc b est d'ordre un multiple de $p-1 \bmod p^n$. D'où le résultat. □

3.4. **Structure de $(\mathbb{Z}/2^n\mathbb{Z})^\times$.**

Remarquons que si $n = 1$ ou 2, alors la structure de $(\mathbb{Z}/2^n\mathbb{Z})^\times$ est facile à déterminer : pour $n = 1$, on a $(\mathbb{Z}/2\mathbb{Z})^\times = \{\overline{1}\}$ est réduit à l'élément neutre et pour $n = 2$, on trouve que $(\mathbb{Z}/4\mathbb{Z})^\times = \{\overline{1}, \overline{3}\} = \langle\overline{3}\rangle$ est cyclique d'ordre 2. Mais pour $n \geq 3$ les choses sont décidément plus subtiles. En effet, le résultat suivant montre que, pour $n \geq 3$, $(\mathbb{Z}/2^n\mathbb{Z})^\times$ n'est jamais cyclique.

Lemme 4. *Soit a un entier impair de $\mathbb{Z}$, alors pour tout $n \geq 3$, $a^{2^{n-2}} \equiv 1 \pmod{2^n}$.*

Preuve. Par récurrence sur $n \geq 3$.
Pour $n = 3$, tout nombre impair a est congru à 1, 3, 5 ou 7 $\pmod 8$. Élévons au carré on obtient que $a^2 \equiv 1 \pmod 8$ pour chaque cas, comme prévu.
Supposons maintenant le résultat vrai pour un $n \geq 3$. Si a est un entier impair, alors

$$a^{2^{n-2}} = 1+2^n k \Longrightarrow a^{2^{n-1}} = (a^{2^{n-2}})^2 = (1+2^n k)^2 = 1+2^{n+1}k+2^{2n}k^2 \equiv 1 \pmod{2^{n+1}}.$$

La preuve est terminée par récurrence. □

Le Lemme précédent, montre que pour $n \geq 3$, chaque élément de $(\mathbb{Z}/2^n\mathbb{Z})^\times$ admet un ordre au plus égal à 2^{n-2}, tandis que l'ordre de $(\mathbb{Z}/2^n\mathbb{Z})^\times$ est $\varphi(2^n) = 2^{n-1}$ ce qui justifie ce que nous avons dit juste avant le lemme. Il s'avère que la borne 2^{n-2} de l'ordre des éléments de $(\mathbb{Z}/2^n\mathbb{Z})^\times$ est atteinte : il y a, en effet, des éléments dont les ordres atteignent 2^{n-2}.

Proposition 8. *Soit $n \geq 3$, alors l'ordre de la classe $5 + 2n^{\mathbb{Z}}$ est 2^{n-2} dans $(\mathbb{Z}/2^n\mathbb{Z})^\times$.*

Preuve. Résultat admis. □

Plus généralement on a le résultat suivant.

Théorème 24. *Soit $n \geq 3$, l'ordre maximal d'un élément de $(\mathbb{Z}/2^n\mathbb{Z})^\times$ est 2^{n-2}. Soient u un entier impair et $n > 3$, pour que la classe de u modulo 2^n soit d'ordre 2^{n-2} il faut et il suffit que u soit congru à 3 ou à 5 modulo 8.*

Preuve. Résultat admis. □

On admet aussi le résultat suivant.

Théorème 25. *Soit $n \geq 3$, alors $(\mathbb{Z}/2^n\mathbb{Z})^\times$ est isomorphe à au produit $\langle -1 + 2^n\mathbb{Z}\rangle \times \langle 5 + 2^n\mathbb{Z}\rangle$. Le premier facteur est d'ordre 2 et le second est d'ordre 2^{n-2}.*

Remarque 11. Nous avons les résultats suivants :
$(\mathbb{Z}/2\mathbb{Z})^\times = \{\overline{1}\}$,
$(\mathbb{Z}/4\mathbb{Z})^\times = \{\overline{1}, \overline{3}\} = \langle\overline{3}\rangle$,
$(\mathbb{Z}/8\mathbb{Z})^\times = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}$, les classes $\overline{3}$, $\overline{5}$, $\overline{7}$ sont d'ordre 2.

4. Arithmétique des polynômes

Les polynômes ont accompagné les mathématiciens au cours des siècles en les surprenant toujours par la richesse des résultats qui en découlent. Nous allons ici traiter des polynômes de degré quelconque et apprendre à faire quelques manipulations.

Soit K un corps commutatif, considérons $K[X]$ l'anneau des polynômes à coefficients dans K. Il existe de grandes similarités entre l'arithmétique dans $\mathbb{Z}$ et l'arithmétique dans $K[X]$, ce qui s'explique par le fait que ce sont des anneaux intègres, dont tous les idéaux sont principaux de tels anneaux sont dits principaux. Cette similarité nous permet d'aller assez vite et d'omettre certaines preuves.

4.1. **Division euclidienne.**

Définition 7. Soient A, $B \neq 0$ dans $K[X]$, on dit que B divise A s'il existe $Q \in K[X]$ tel que $A = BQ$. On note alors $B|A$. On dit aussi que A est multiple de B ou que A est divisible par B.

Proposition 9. *Soient A, B, $C \in K[X]$.*

1. *$A|B$ et $B|A$ si et seulement s'il existe $\alpha \in K^*$ tel que $A = \alpha B$ (on dit que A et B sont associés).*
2. *Si $A|B$ et $B|C$, alors $A|C$.*
3. *Si $C|A$ et $C|B$, alors $C|(AU + BV)$, pour tout U, $V \in K[X]$.*

Preuve. 1. Soient Q et Q' tels que $A = BQ$ et $B = AQ'$, donc $A = QQ'A$; comme l'anneau $K[X]$ est intègre, alors $QQ' = 1$. Donc $\deg(Q) = 0$, c'est-à-dire que $Q = \alpha \in K^*$ est une constante, d'où le résultat.
2. et 3. sont simples. □

Théorème 26 (Division euclidienne)**.** *Soient $A, B \in K[X]$, avec $B \neq 0$, Il existe un couple (Q, R) unique de polynômes vérifiant la double condition :*

$$A = BQ + R \qquad et \qquad \deg(R) \ < \ \deg(B).$$

Q est appelé le quotient et R le reste et cette écriture est dite : la division euclidienne de A par B.

Remarque 12. Notez que la condition $\deg(R) < \deg(B)$ signifie $R = 0$ ou bien $0 \leq \deg(R) < \deg(B)$. Enfin $R = 0$ si et seulement si $B|A$.

Pour prouver le théorème, nous avons besoin du lemme suivant.

Lemme 5. *Soient A et B deux polynômes non nuls de $K[X]$ tels que* $\deg(B) \leq \deg(A)$. *Alors il existe un polynôme $Q \in K[X]$ tel que* $\deg(A - BQ) < \deg(A)$.

Preuve. Soit a_k le coefficient dominant de A et b_h celui de B. Par hypothèse, on a $k \geq h$. Posons $\alpha = a_k(b_h)^{-1}$ et $Q = \alpha X^{k-h}$, donc le coefficient dominant de BQ est a_k. Par suite $\deg(A - BQ) < k = \deg(A)$. □

Preuve du théorème. **Existence de (Q, R).**
Si B divise A, prenons $R = 0$ et Q tel que $A = BQ$. Sinon, considérons l'ensemble

$\mathcal{R} = \{A - QB \mid Q \in K[X]\}$, qui est donc un ensemble non vide de polynômes non nuls ; puis considérons l'ensemble $E = \{\deg R \mid R \in \mathcal{R}\}$, qui est un ensemble d'entiers positifs non vide. Cet ensemble E possède donc un plus petit élément r ; il existe donc un polynôme

$$R \in \mathcal{R} \text{ tel que } \deg(R) = r \text{ et } A - QB = R.$$

Supposons $r \geq \deg(B) > 0$. D'après le lemme 5, il existe $Q' \in K[X]$ tel que le polynôme

$$L = (A - BQ) - BQ' = A - B(Q + Q')$$

est de degré $r' < r$, ce qui est impossible puisque $A - B(Q + Q') \in \mathcal{R}$. Donc $-\infty \leq r < \deg(B)$.

Unicité de (Q, R)

Soient (Q_1, R_1) et (Q_2, R_2) deux couples vérifiant les deux conditions exigées dans l'énoncé du théorème. On déduit de $A = Q_1B + R_1 = Q_2B + R_2$ que $(Q_2 - Q_1)B = R_1 - R_2$. Ainsi, $R_1 - R_2$ est un multiple de B. Des conditions $\deg R_1 < \deg B$ et $\deg R_2 < \deg B$, on déduit que $\deg(R_1 - R_2) < \deg(B)$, de plus $(Q_2 - Q_1)B = R_1 - R_2$. Ainsi $R_1 - R_2$ est un multiple de B de degré strictement plus petit. La seule possibilité est que $Q_2 - Q_1$ soit nul. On en déduit $Q_1 = Q_2$, puis, en allant reprendre l'égalité $(Q_2 - Q_1)B = R_1 - R_2$, que $R_1 = R_2$. □

Remarques 3. Soient A et B deux polynômes de $K[X]$, avec $B \neq 0$.

1. B est un diviseur de A si le reste de la division euclidienne de A par B est nul.
2. On dit que B est un diviseur propre de A si B divise A et si $1 \leq \deg(B) < \deg(A)$.

Définition 8. Soit $P(X) = c_0 + c_1X + \cdots + c_nX^n$ un polynôme de $K[X]$. Pour chaque $a \in K$, la valeur de P en a est définie par :

$$P(a) = c_0 + c_1a + \cdots + c_na^n \in K.$$

On dit qu'un un élément $a \in K$ est une racine de P si $P(a) = 0 \in K$.

Le résultat suivant est une conséquence de la division euclidienne dans $K[X]$.

Proposition 10. *Un élément $a \in K$ est racine d'un polynôme $P \in K[X]$ si et seulement si $(X - a)$ divise P.*

Preuve. Par la division euclidienne dans K[X] de P par $B(X) = X - a$, il existe un couple unique de polynômes $(Q, R) \in K[X]^2$ tel que $P = BQ + R$, et $\deg(R) < deg(X - a) = 1$. Le polynôme R est donc constant. Comme $B(a) = 0$, alors $P(a) = 0$ si et seulement si $R = 0$. □

Nous citons le théorème suivant, qui va jouer un rôle essentiel dans le chapitre des corps finis.

Théorème 27. *Soient $P \in K[X]$ et $a_1, a_2, \cdots, a_k$ des racines distinctes de P dans K, alors P est divisible par le polynôme $(X - a_1)(X - a_2) \cdots (X - a_k)$ de degré k. Il en résulte qu'un polynôme de degré n de $K[X]$ possède au plus n racines distinctes dans K.*

Preuve. On va raisonner par récurrence. La propriété est vraie pour $k = 1$ d'après la proposition 10. Supposons-la vérifiée pour $k - 1$, alors

$$P(X) = (X - a_1) \cdots (X - a_{k-1})Q(X).$$

Comme $P(a_k) = (a_k - a_1) \cdots (a_k - a_{k-1})Q(a_k) = 0$, alors l'intégrité de K implique $Q(a_k) = 0$, donc $Q(X) = (X - a_k)Q_1(X)$, d'où le résultat. □

Remarque 13. Le théorème 27 reste vrai si on replace le corps K par un anneau intègre A, mais il ne l'est pas si A n'est pas intègre.
Contre-exemple. Dans l'anneau $(\mathbb{Z}/10\mathbb{Z})[X]$ qui n'est pas intègre, on a l'égalité

$$(X - \overline{2})(X - \overline{5}) = X^2 - \overline{5}X - \overline{2}X + \overline{10} = X(X - \overline{7}).$$

Donc le polynôme $P(X) = (X - \overline{2})(X - \overline{5})$ possède 4 racines distinctes dans l'anneau non intègre $\mathbb{Z}/10\mathbb{Z}$ qui sont : $\overline{0}$, $\overline{2}$, $\overline{5}$ et $\overline{7}$. Pour chaque racine $a_i = \overline{0}$, $\overline{2}$, $\overline{5}$ ou $\overline{7}$, P est divisible par $(X - a_i)$. Mais P n'est pas divisible par le produit des $(X - a_i)$, qui est de degré 4.

4.2. **L'anneau K[X].**

Soit $P \in K[X]$, rappelons que l'ensemble $I = \langle P \rangle = \{AQ \mid Q \in K[X]\}$ des multiples de P est un idéal de $K[X]$. C'est l'idéal de $K[X]$ engendré par P.

Réciproquement, nous allons voir, comme dans le cas de $\mathbb{Z}$, que la division euclidienne dans $K[X]$ implique que tout idéal de $K[X]$ est de cette forme, c'est-à-dire principal. Rappelons qu'un polynôme $A \in K[X]$ est dit unitaire (ou normalisé) si son coefficient dominant est égal à 1.

Théorème 28. *Soit I un idéal de $K[X]$ non réduit à $\{0\}$, et soit $r \geq 0$ le* **plus petit des degrés** *des polynômes non nuls appartenant à I.*

1. *Pour tout polynôme $A \in I$ de degré r, on a $I = \langle A \rangle$.*
2. *Il existe un polynôme unitaire unique $U \in I$ tel que $I = \langle U \rangle$.*
3. *I est un idéal propre de $K[X]$ si et seulement si $r \geq 1$.*

Preuve. L'existence de l'entier r est assuré par la propriété fondamentale de $\mathbb{N}$.
1. Soit $A \in I$ de degré $r \geq 0$, et soit $P \in I$. Alors la division euclidienne de P par A s'écrit $P = AQ + R$, avec $\deg(R) < \deg(A) = r$.
Comme $R = P - AQ \in I$, et comme $\deg(R) < r$ et r est le plus petit de sa famille, alors $R = 0$, et par suite $P = AQ$. Cela montre que $I \subset \langle A \rangle$. Réciproquement, il est clair que $\langle A \rangle \subset I$. D'où $\langle A \rangle = I$.
2. Divisant A par son coefficient dominant, on obtient alors un polynôme unitaire $U \in I$ tel que $I = \langle U \rangle$. Ce polynôme est unique car si $U' \in I$ est un polynôme unitaire tel que $I = \langle U \rangle = \langle U' \rangle$, alors chacun des deux polynômes U et U' divise l'autre, il existe donc $\alpha \in K^*$ tel que $U = \alpha U'$ (proposition 9). Or les polynômes U et U' sont unitaires, donc on a nécessairement $\alpha = 1$, d'où $U = U'$.
3. Comme U est unitaire on a : $\deg(U) = 0 \Longleftrightarrow U = 1 \in I \Longleftrightarrow I = K[X]$. □

Remarquons que si $I = \{0\}$, on peut écrire $I = \langle 0 \rangle$, ce qui montre que tout idéal I de $K[X]$ est principal. Le théorème 28 nous permet donc d'énoncer le résultat suivant :

Théorème 29. *Soit K un corps, alors l'anneau $K[X]$ est principal.*

Remarque 14. Le groupe des unités de $K[X]$ est formé par les polynômes constants non nuls.

4.3. **Polynômes irréductibles.**

Définition 9. Un polynôme P est dit *irréductible* s'il est non constant et n'admet pas de diviseur propre, i.e., P est irréductible si ses seuls diviseurs sont les inversibles de K et ses polynômes associés. Un polynôme non irréductible est aussi dit *réductible*.

Exemples 3.
1. Tous les polynômes de degré 1 sont irréductibles.
2. Pour $K = \mathbb{C}$, les seuls polynômes irréductibles sont ceux de degré 1.
3. Pour $K = \mathbb{R}$, les polynômes irréductibles sont ceux de degré 1, et les polynômes de degré 2 de discriminant négatif.

Théorème 30. *Soit P un polynôme de degré $n \geq 1$, et soit $D \subset \mathbb{N}$ l'ensemble des degrés des diviseurs non constants de P. Alors $D \neq \emptyset$ car $n \in D$.*
Soit r le plus petit élément de D et soit A un diviseur de P de degré r, alors A est irréductible. Cela signifie que tout polynôme de degré positif admet un facteur irréductible.

Preuve. Simple à vérifier. □

Remarque 15. Il est faux de penser qu'un polynôme est irréductible si et seulement s'il n'a pas de racine. Voilà des contre-exemples
1. Tout polynôme de degré 1 admet une racine, mais il est irréductible.
2. Le polynôme $(X^2+1)^3$, de degré 6, n'a pas de racine dans $\mathbb{R}$ mais il est réductible dans $\mathbb{R}[X]$.
3. Le polynôme $(X^2+X+1)^2$, de degré 4, n'a pas de racine dans $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$ mais il est réductible dans $\mathbb{F}_2[X]$.

Cependant on a l'équivalence suivante.

Proposition 11. *Un polynôme de degré 2 ou 3 est irréductible dans $K[X]$ si et seulement s'il n'admet pas de racine dans K.*

Preuve. Un polynôme P est réductible si et seulement s'il possède un diviseur propre, c'est-à-dire P admet un diviseur A vérifiant $1 \leq \deg(A) < \deg(P)$, donc $\deg(P) \geq 2$. Posons $P = AB$, et supposons que $\deg(P) \leq 3$, alors

$$\begin{gathered} 1 \leq \deg(B) \leq \deg(P) - 1 \leq 2, \\ 1 \leq \deg(A) \leq \deg(P) - 1 \leq 2 \text{ et} \\ \deg(A) + \deg(B) = \deg(P). \end{gathered}$$

Alors on en déduit que $\deg(A) = 1$ ou $\deg(B) = 1$, donc P admet une racine puisque tout polynôme de degré 1 a une racine. □

Exemple 2. Dans $\mathbb{F}_2[X]$, montrer que le seul polynôme irréductible de degré 2 est X^2+X+1, et que les seuls polynômes irréductibles de degré 3 sont X^3+X^2+1 et X^3+X+1.

4.4. **Plus grand commun diviseur de deux polynômes.**
Soient A et B deux polynômes non tous deux nuls de $K[X]$, il est facile de vérifier que l'ensemble

$$I(A,B)=\{AU+BV \mid (U,V)\in K[X]^2\}$$

est un idéal de $K[X]$. Comme A et B sont éléments de $I(A,B)$, cet idéal n'est pas réduit à $\{0\}$. Il existe, d'après le théorème 28, un unique polynôme unitaire $D\in K[X]$ tel que $I(A,B)=\langle D\rangle$.

Définition 10. Soient $A,B\in K[X]$, avec $A\neq 0$ ou $B\neq 0$. L'unique polynôme unitaire $D\in K[X]$ tel que $I(A,B)=\langle D\rangle$ est appelé le pgcd (plus grand commun diviseur) de A et B, et est noté $\mathrm{pgcd}(A,B)$.

La démonstration des énoncés qui suivent est presque identique à celle des énoncés qui leur correspondent dans le cas de l'anneau $\mathbb{Z}$.

Théorème 31 (Propriété caractéristique du pgcd). *Soient A et B deux polynômes de $K[X]$ non tous deux nuls. Le pgcd de A et B est l'unique polynôme unitaire $D\in K[X]$ tel que*

1. *D est un diviseur commun de A et B.*
2. *Tout diviseur commun de A et B divise D.*

Preuve. Comme A et B appartiennent à $I(A,B)$, alors $\langle A\rangle\subset I(A,B)=\langle D\rangle$ et $\langle B\rangle\subset I(A,B)=\langle D\rangle$, d'où D divise A et B. De plus, si un polynôme de $K[X]$ divise A et B, alors il divise toute combinaison linéaire de A et B, d'où il divise D. Par suite, D vérifie les conditions 1 et 2.

Inversement, soit $F\in K[X]$ réalisant les conditions 1 et 2. Alors F divise toute combinaison linéaire de A et B, d'où $I(A,B)\subset\langle F\rangle$, ce qui implique que F divise leur pgcd D. D'après la condition 2, D divise F. Puisque D et F sont unitaires, on a donc $F=D$. □

Remarques 4.

- $\mathrm{pgcd}(A,B)$ est un polynôme unitaire.
- Si $A|B$ et $A\neq 0$, alors $\mathrm{pgcd}(A,B)=\frac{1}{\alpha}A$, où α est le coefficient dominant de A.

- Pour tout $\alpha \in K$, $\text{pgcd}(\alpha A, B) = \text{pgcd}(A, B)$.

Définition 11. Soient $A, B \in K[X]$. On dit que A et B sont premiers entre eux si $\text{pgcd}(A, B) = 1$.

Remarque 16. Deux polynômes irréductibles de $K[X]$ sont premiers entre eux ou sont associés.

Théorème 32 (Théorème de Bézout). *Soient $A, B \in K[X]$ des polynômes avec $A \neq 0$ ou $B \neq 0$. Soit D un diviseur commun unitaire de A et B. Alors $D = pgcd(A, B)$ si et seulement s'il existe deux polynômes $U,\ V \in K[X]$ tels que $AU + BV = D$.*

Remarque 17. Si $D = \text{pgcd}(A, B)$, alors les polynômes U et V ne sont pas uniques puisqu'un simple calcul prouve que si U et V vérifient l'égalité : $AU + BV = D$, alors les polynômes $U' = U + BQ$ et $V' = V - AQ$, où Q est un polynôme quelconque, vérifient aussi l'égalité $AU + BV = D$.

De plus, il faut remarquer que, dans le cas général, cette relation ne caractérise pas le PGCD car il en existe une de même type pour tout multiple de D.

Corollaire 20 (Caractérisation des polynômes premiers entre eux à l'aide d'une identité de Bézout).
Soient $A,\ B \in K[X]$ deux polynômes. A et B sont premiers entre eux si et seulement s'il existe deux polynômes $U,\ V \in K[X]$ tels que $AU + BV = 1$.

Corollaire 21 (Théorème de Gauss). *Soient $A,\ B,\ C \in K[X]$ trois polynômes. Si A divise BC et $pgcd(A, B) = 1$, alors avec $A|C$.*

Preuve. Il existe $U, V \in K[X]$ tels que $AU + BV = 1$, d'où l'égalité $A(UC) + V(BC) = C$, donc A divise C. □

Corollaire 22. *Soient $A,\ B,\ C \in K[X]$ trois polynômes. Si $pgcd(A, B) = 1$ et si $A|C$ et $B|C$, alors $AB|C$.*

Corollaire 23. *Soient $A,\ B,\ C \in K[X]$ trois polynômes. Si $\text{pgcd}(A, B) = 1$ et $\text{pgcd}(A, C) = 1$, alors $\text{pgcd}(A, BC) = 1$.*

Proposition 12. *Soient A et B deux polynômes. On suppose que l'un au moins n'est pas nul. Soit D leur pgcd et soient A_1 et B_1 les quotients respectifs de A et B par D. Alors les polynômes A_1 et B_1 sont premiers entre eux.*

Preuve. On a $A = DA_1$ et $B = DB_1$, alors $D = AU + BV = DA_1U + VDB_1$, donc $A_1U + VB_1 = 1$. D'où le résultat. □

Proposition 13. *Soient A et B deux polynômes de $K[X]$, avec $B \neq 0$, et soit R le reste de la division euclidienne de A par B, alors* $\text{pgcd}(A, B) = \text{pgcd}(B, R)$.

Ce résultat justifie l'algorithme d'Euclide étendu pour les polynômes.

Le résultat suivant se déduit du théorème 30 qui assure l'existence d'un facteur irréductible, il est l'analogue du Théorème fondamental de l'arithmétique.

Théorème 33. *Tout polynôme non nul $Q \in K[X]$ s'écrit d'une façon unique, à une permutation près, sous la forme :*

$$Q = \beta P_1^{\alpha_1} P_2^{\alpha_2} \cdots P_r^{\alpha_r} = \beta \prod_{i=1}^{r} P_i^{\alpha_i},$$

où $\beta \in K^*$, les polynômes P_i sont irréductibles, unitaires et tous distincts, les entiers α_i sont dans $\mathbb{N}^*$.

Exemple 3. Dans $\mathbb{F}_2[X]$ on a :

$$\begin{aligned} Q(X) &= X^5 + X^4 + X^3 + X^2 + X + 1 \\ &= X^3(X^2 + X + 1) + X^2 + X + 1 \\ &= (X^2 + X + 1)(X^3 + 1) \\ &= (X^2 + X + 1)(X^3 - 1), \text{ dans } \mathbb{F}_2, \text{ -1=1} \\ &= (X^2 + X + 1)(X - 1)(X^2 + X + 1) \\ &= (X - 1)(X^2 + X + 1)^2. \end{aligned}$$

Nous terminons cette section par la proposition suivante.

Proposition 14. *Soit A un polynôme irréductible divisant un produit de polynômes $A_1 \cdots A_r$ dans $K[X]$. Alors A divise l'un des A_i. Bien sur, si les A_i sont aussi irréductible, alors A est égale à l'un d'eux.*

4.5. **Plus petit commun multiple de deux polynômes.** Considérons deux polynômes non nuls A et B de $K[X]$. L'ensemble $\langle A\rangle \cap \langle B\rangle$ est un idéal non nul de $K[X]$. Il existe donc un unique polynôme unitaire $M \in K[X]$ tel que l'on ait

$$\langle A\rangle \cap \langle B\rangle = \langle M\rangle.$$

D'où la proposition suivante.

Proposition 15. *Soient $A, B \in K[X]$ deux polynômes non nuls, alors il existe un unique polynôme unitaire M de plus petit degré tel que $A|M$ et $B|M$.*

Définition 12. L'unique polynôme M est appelé le ppcm (plus petit commun multiple) de A et B, et est noté $\text{ppcm}(A, B)$.

Théorème 34. *Soit M un polynôme unitaire de $K[X]$. Alors, M est le* ppcm *de A et B si et seulement si les deux conditions suivantes sont vérifiées :*

1. *le polynôme M est un multiple de A et B.*
2. *tout multiple de A et B dans $K[X]$ est un multiple de M.*

Preuve. Puisque M appartient à $\langle A\rangle$ et $\langle B\rangle$, le polynôme M est un multiple de A et B. Par ailleurs, si un polynôme F de $K[X]$ est multiple de A et B, donc il est dans $\langle M\rangle$, c'est donc un multiple de M.

Inversement, soit $F \in K[X]$ réalisant les conditions 1 et 2. On déduit de la condition 1 que F est dans $\langle M\rangle$. D'après la condition 2, M est dans $\langle F\rangle$. Par suite, on a $\langle F\rangle = \langle M\rangle$, puis $F = M$ vu que F et M sont unitaires. □

Corollaire 24. *Soient $A, B \in K[X]$ deux polynômes non nuls et M =ppcm(A, B). Si C est un polynôme de $K[X]$ tel que $A|C$ et $B|C$, alors $M|C$.*

Corollaire 25. *Soient $A, B \in K[X]$ deux polynômes non nuls. Si* $\text{pgcd}(A, B) = 1$, *alors* $\text{ppcm}(A, B) = AB$.

Proposition 16. *Soient A et B deux polynômes non nuls de $K[X]$. Posons $D =$* $\text{pgcd}(A, B)$ *et $M =$* $\text{ppcm}(A, B)$, *alors on a $\langle AB\rangle = \langle DM\rangle$.*

Preuve. Il suffit de montrer l'égalité d'idéaux

$$\left\langle \frac{AB}{D^2} \right\rangle = \left\langle \frac{M}{D} \right\rangle.$$

Le polynôme M/D est le ppcm de A/D et B/D (Théorème 34). Par ailleurs, les polynômes A/D et B/D sont premiers entre eux. On se ramène ainsi à prouver l'assertion dans le cas où $D = 1$. Supposons donc A et B premiers entre eux et vérifions que l'on a $\langle AB\rangle = \langle M\rangle$. Le polynôme AB est un multiple de A et B. Par ailleurs, soit C un multiple de A et B. Compte tenu du théorème 34, tout revient à vérifier que C est un multiple de AB. Il existe R et S dans $K[X]$ tels que $C = RA$ et $C = SB$. On a $RA = SB$, donc A divise SB. Puisque A est par hypothèse premier avec B, on déduit du théorème de Gauss que A divise S, ce qui entraîne le résultat. □

Théorème 35. *Soient A et B deux polynômes non nuls de $K[X]$. Soient*

$$A = \lambda \prod_{i=1}^{r} P_i^{\alpha_i} \quad et \quad B = \mu \prod_{i=1}^{r} P_i^{\beta_i}$$

les décompositions de A et B en produit d'éléments irréductibles. Soient D et M respectivement le pgcd et le ppcm de A et B. On a alors

$$D = \prod_{i=1}^{r} P_i^{\min(\alpha_i,\beta_i)} \qquad et \qquad M = \prod_{i=1}^{r} P_i^{\max(\alpha_i,\beta_i)}.$$

Pour tout $i \in \{1, 2, \cdots, r\}$, l'égalité $\min(\alpha_i, \beta_i) + \max(\alpha_i, \beta_i) = \alpha_i + \beta_i$ implique l'égalité des idéaux $\langle DM \rangle = \langle AB \rangle$.

4.6. L'ensemble quotient $K[X]/\langle P \rangle$.

C'est l'analogue de l'ensemble quotient $\mathbb{Z}/n\mathbb{Z}$ pour $n \in \mathbb{N}$.

4.6.1. Définition de l'ensemble quotient $K[X]/\langle P \rangle$.

Soit $P \in K[X]$ un polynôme non constant ($\deg(P) \geq 1$). Comme dans $\mathbb{Z}$, considérons la relation modulo P définie par :

$$\begin{aligned} \forall (A, A') \in K[X]^2,\ A \equiv A' \pmod{P} \quad &\Longleftrightarrow A' - A \in \langle P \rangle \\ &\Longleftrightarrow A' - A = PQ,\ Q \in K[X]. \end{aligned} \tag{1}$$

Cette relation est une relation d'équivalence (simple à vérifier). Pour chaque polynôme $A \in K[X]$, on désigne par $\overline{A}$ sa classe d'équivalence modulo P :

$$\overline{A} = \{A' \in K[X] \mid A \equiv A' \pmod{P}\} = \{A + PQ \mid Q \in K[X]\}.$$

Notons par $K[X]/\langle P \rangle$ l'ensemble quotient de $K[X]$ par la relation d'équivalence définie dans (1), c'est- à-dire l'ensemble des classes modulo P.

Sur l'ensemble quotient $K[X]/\langle P \rangle$, on définit trois lois : deux lois internes " $+$ " (l'addition), " $\times$ " (la multiplication) et une loi externe " $\cdot$ " (la multiplication par un scalaire) par :

$$\forall (A, B) \in K[X]^2, \begin{cases} \overline{A} + \overline{B} = \overline{A + B}, \\ \overline{A} \times \overline{B} = \overline{AB}, \\ \forall a \in K, a \cdot \overline{A} = \overline{aA}. \end{cases}$$

On vérifie facilement que ces définitions ne dépendent pas des représentants choisis, c-à-d, la congruence modulo P est compatible avec ces lois.

Proposition 17. *$(K[X]/\langle P \rangle, +, \cdot)$ est un K-espace vectoriel, de plus pour tous $\overline{A}$, $\overline{B}$ et $\overline{C}$ dans $K[X]/\langle P \rangle$ et pour tout a dans K on a :*

1. $(\overline{A}+\overline{B})\times\overline{C}=\overline{A}\times\overline{C}+\overline{B}\times\overline{C}$.
2. $\overline{A}\times(\overline{B}+\overline{C})=\overline{A}\times\overline{C}+\overline{B}\times\overline{C}$.
3. $a\cdot(\overline{A}\times\overline{B})=(a\cdot\overline{A})\times\overline{B}=\overline{A}\times(a\cdot\overline{B})$. *Cette axiome entraîne que, pour tous a et b de K et tous $\overline{A}$, $\overline{B}$ dans $K[X]/\langle P\rangle$:* $(a\cdot\overline{A})\times(b\cdot\overline{B})=ab(\overline{A}\times\overline{B})$.

On dit que $(K[X]/\langle P\rangle,+,\cdot,\times)$ **est une algèbre sur** K **ou une** K**-algèbre**. *L'élément neutre pour l'addition est* $\overline{0}$ *et celui de la multiplication est* $\overline{1}$.

Preuve. Simple à vérifier. □

Lemme 6. *Si un polynôme P est irréductible dans $K[X]$, alors l'idéal $\langle P\rangle$ est maximal et donc $K[X]/\langle P\rangle$ est un corps.*

Preuve. Si $\langle P\rangle\subset\langle Q\rangle$, alors Q divise P. Comme P est irréductible, alors $Q\in K^*$ ou $Q=\alpha P$ avec $\alpha\in K^*$. Par suite $\langle P\rangle=\langle Q\rangle$. Il est connu que pour tout anneau A et tout idéal I, le quotient A/I est un corps ssi I est maximal. □

Théorème 36. *Soit $P\in K[X]$ un polynôme non constant. La classe $\overline{A}\in K[X]/\langle P\rangle$ d'un polynôme $A\in K[X]$ est inversible dans $K[X]/\langle P\rangle$ si et seulement si A est premier avec P. Donc le groupe des éléments inversibles de l'anneau $K[X]/\langle P\rangle$ est formé des classes des polynômes $A\in K[X]$ telles que A soit premier avec P.*

Preuve. $\overline{A}\in K[X]/\langle P\rangle$ est inversible dans $K[X]/\langle P\rangle$ si et seulement si il existe $\overline{B}\in K[X]/\langle P\rangle$ tel que $\overline{A}\times\overline{B}=\overline{1}$ ce qui est équivaut à l'existence d'un polynôme $U\in K[X]$ tel que $AB+PU=1$, et par Bézout A est premier avec P. □

Corollaire 26. *Soit $P\in K[X]$ un polynôme non constant. Les conditions suivantes sont équivalentes :*

1. *l'anneau $K[X]/\langle P\rangle$ est intègre.*
2. *le polynôme P est irréductible dans $K[X]$.*
3. *l'anneau $K[X]/\langle P\rangle$ est un corps.*

Preuve. $1\implies 2$. Supposons que $K[X]/\langle P\rangle$ soit intègre. Tout d'abord, P n'est pas inversible, sinon on aura $\langle P\rangle=K[X]$ et $K[X]/\langle P\rangle$ sera un anneau nul, ce qui est exclu par définition.

Soit F un diviseur de P. Il s'agit de montrer que F est inversible ou bien que F et P sont associés. Il existe $Q\in K[X]$ tel que $P=FQ$, d'où $\overline{FQ}=0$. Par l'hypothèse d'intégrité, cela entraîne que $\overline{F}=0$ ou bien que $\overline{Q}=0$. Si $\overline{F}=0$, alors F est dans $\langle P\rangle$, i.e., P divise F, donc P et F sont associés. Si $\overline{Q}=0$, alors Q et P sont associés, par

suite on a $\deg(F) = 0$, i.e., F est inversible (rappelons que les inversibles de $K[X]$ sont les inversibles de K). Cela prouve que P est irréductible dans $K[X]$.

$2 \Longrightarrow 3$. Cette implication est assuré par le lemme 6. On peut montrer ça autrement ; supposons P irréductible dans $K[X]$ et prouvons que tout élément non nul $\overline{F}$ de $K[X]/\langle P\rangle$ est inversible. Puisque P est irréductible et que P ne divise pas F (car $\overline{F} \neq 0$), les polynômes F et P sont premiers entre eux. D'après le théorème 36, $\overline{F}$ est donc inversible, donc $K[X]/\langle P\rangle$ est un corps.

$3 \Longrightarrow 1$. Cette implication est immédiate. □

De ce qui précède, on déduit le résultat fondamental suivant.

Théorème 37. *Soit P un polynôme irréductible de $K[X]$. Alors $L = K[X]/\langle P\rangle$ est un corps commutatif contenant K comme sous-corps et possédant les deux propriétés suivantes :*

1. *le polynôme P a une racine dans L.*
2. *le K-espace vectoriel L est de dimension finie sur K, égale au degré de P.*

Preuve. 1. Ce point est immédiat du corollaire précédant. Posons $\alpha = \overline{X}$ et $P(X) = \sum_{k=0}^{n} a_k X^k$, alors la classe de P est nulle, c'est-à-dire,

$$0 = \overline{P(X)} = \sum_{k=0}^{n} \overline{a_k X^k} = \sum_{k=0}^{n} a_k \overline{X^k} = P(\alpha).$$

2. Pour la preuve de 2 voir théorème 38. □

4.6.2. **Représentation de $K[X]/\langle P\rangle$.**

Soit $q \in \mathbb{Z}$ et soit n un entier positif. On sait que la façon la plus simple de décrire la classe $\overline{q}$ dans $\mathbb{Z}/n\mathbb{Z}$ consiste à écrire $\overline{q} = \overline{r}$, où r est le reste de la division euclidienne de q par n. On peut dire dans ce sens que l'entier $r \in \{0, 1, \cdots, n-1\}$ représente la classe q modulo n. On procède de la même façon dans l'anneau $K[X]/\langle P\rangle$, grâce à la proposition suivante.

Proposition 18. *Soient A et P deux éléments de $K[X]$, on suppose $\deg(P) \geq 1$. Le reste R de la division euclidienne de A par P est le seul polynôme de $K[X]$ tel que*

$$R \equiv A \pmod{P} \quad \text{et} \quad \deg(R) < \deg(P).$$

Preuve. Il est simple de voir que $R \equiv A \pmod{P}$.
L'unicité vient de fait que si $R' \equiv R \pmod{P}$ avec $\deg(R') < \deg(P)$, alors le polynôme $R' - R$ est divisible par P et $\deg(R' - R) < \deg(P)$, ce qui implique $R' - R = 0$. □

Notation : Pour chaque entier positif n, désignons par $K_n[X]$ le sous-espace vectoriel de $K[X]$ constitué des polynômes $Q \in K[X]$ tels que $\deg(Q) < n$.

Dans ce qui suit, posons $n = \deg(P) \geq 1$. La proposition 18 assure alors que pour tout $A \in K[X]$, la classe $\overline{A} \in K[X]/\langle P\rangle$ contient un seul polynôme appartenant à $K_n[X]$, ce polynôme est le reste de la division euclidienne de A par P.

Dans la suite de ce chapitre, on désigne par α la classe du polynôme X dans la K-algèbre quotient $K[X]/\langle P\rangle$, c'est-à-dire $\alpha = X + \langle P\rangle$.
Pour chaque polynôme $A = a_0 + a_1X + \cdots + a_kX^k \in K[X]$, posons

$$A(\alpha) = a_0 + a_1\alpha + \cdots + a_k\alpha^k \in K[X]/\langle P\rangle,$$

de sorte que $A(\alpha) = \overline{A} \pmod P$, et qu'en particulier on a $P(\alpha) = \overline{P(X)} = 0$, c-à-d α est une racine de P dans $K[X]/\langle P\rangle$. Cela permet d'écrire

$$K[X]/\langle P\rangle = \{\overline{A} \mid A \in K[X]\} = \{A(\alpha) \mid A \in K[X]\}.$$

Soit $A = PQ + R$ la division euclidienne de A par P, de la relation $P(\alpha) = 0$ il résulte que $A(\alpha) = R(\alpha)$. On en déduit donc que

$$\begin{aligned} K[X]/\langle P\rangle &= \{R(\alpha) \mid R \in K_n[X]\} \\ &= \{a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} \mid a_i \in K\}. \end{aligned}$$

De plus, il résulte de la proposition 18 que si R_1 et $R_2 \in K_n[X]$, on a l'équivalence

$$R_1(\alpha) = R_2(\alpha) \Longleftrightarrow R_1 = R_2.$$

En fait, la famille $\{1, \alpha, \alpha^2, \cdots, \alpha^{n-1}\}$ est une base du K-espace vectoriel $K[X]/\langle P\rangle$. On a l'important théorème suivant.

Théorème 38. *Soit $P \in K[X]$ un polynôme de degré $n \geq 1$. Désignons par $\alpha = X + \langle P\rangle$ la classe du polynôme X modulo P.*

1. *Tout élément $\overline{A} \in K[X]/\langle P\rangle$ s'écrit d'une façon et d'une seule sous la forme*
$$\overline{A} = R(\alpha), \text{ où } R \in K_n[X].$$
2. *En tant que K-algèbre, $L = K[X]/\langle P\rangle$ est un K-espace vectoriel de dimension $n = \dim_K(L) = \deg(P)$ et la famille $\{1, \alpha, \alpha^2, \cdots, \alpha^{n-1}\}$ en constitue une base, qu'on appelle la base canonique de $K[X]/\langle P\rangle$.*

Preuve. 1. Déjà prouvé.
2. Montrons que la famille $F = \{1, \alpha, \alpha^2, \cdots, \alpha^{n-1}\}$ est une base de L. Soient λ_i des éléments de K tels que $\sum_{i=0}^{n-1} \lambda_i\alpha^i = \overline{0}$, cela signifie que $\sum_{i=0}^{n-1} \lambda_i\alpha^i \in \langle P\rangle$, or $\deg(P) =$

n, donc forcement tous les λ_i sont nuls. D'où la famille F est libre, de plus elle est génératrice, et le résultat en découle. □

4.6.3. **Règles de calcul dans $K[X]/\langle P\rangle$.**
Sous les hypothèses du théorème 38 ci-dessus, chaque élément $x \in K[X]/\langle P\rangle$ s'écrit de façon unique $x = R(\alpha)$, avec $R \in K_n[X]$.

L'addition ne pose pas de problème puisque la somme de deux polynômes de $K_n[X]$ appartient à $K_n[X]$.

Pour la multiplication, on procède comme suit.

Règle de calcul pour la multiplication. Pour multiplier deux éléments $R_1(\alpha)$ et $R_2(\alpha)$ dans $K[X]/\langle P\rangle$, on calcule le reste R de la division euclidienne dans $K[X]$ du polynôme produit R_1R_2 par P et on écrit :

$$R_1(\alpha)R_2(\alpha) = R(\alpha).$$

Exemple.
Supposons par exemple $K = \mathbb{Q}$ et $P = X^3 - X + 1$, donc $\deg(P) = 3$.

$$Q[X]/\langle P\rangle = \{a\alpha^2 + b\alpha + c \mid a, b, c \in \mathbb{Q}\}.$$

On veut effectuer le produit $(\alpha^2 + \alpha)(\alpha^2 + 1)$, on écrit :

$$(\alpha^2 + \alpha)(\alpha^2 + 1) = \alpha^4 + \alpha^3 + \alpha^2 + \alpha,$$

puis le reste de la division euclidienne est $R = 2X^2 + X - 1$, puisque

$$X^4 + X^3 + X^2 + X = (X^3 - X + 1)(X + 1) + 2X^2 + X - 1.$$

Donc $(\alpha^2 + \alpha)(\alpha^2 + 1) = R(\alpha) = 2\alpha^2 + \alpha - 1$.
On peut aussi arriver à ce résultat en utilisant la relation

$$P(\alpha) = \alpha^3 - \alpha + 1 = 0 \Longleftrightarrow \alpha^3 = \alpha - 1.$$

Donc, en remplaçant autant de fois qu'il le faut α^3 par $\alpha - 1$, on obtient

$$(\alpha^2 + \alpha)(\alpha^2 + 1) = \alpha^4 + \alpha^3 + \alpha^2 + \alpha = \alpha(\alpha - 1) + \alpha - 1 + \alpha^2 + \alpha = 2\alpha^2 + \alpha - 1.$$

4.7. **Exercices.** Montrer que le corps $\mathbb{C}$ des nombres complexes n'est autre que le corps quotient $\mathbb{R}[X]/\langle X^2+1\rangle$. A quoi correspond dans $\mathbb{C}$ la classe α de X dans $\mathbb{R}[X]/\langle X^2+1\rangle$? La base $\{1, \alpha\}$?

5. Corps finis

L'objectif de ce chapitre est de construire les corps finis et de donner quelques applications.

5.1. **Rappels et Généralités.**

Définition 13. Un corps K est un ensemble non vide muni de deux lois de composition internes (deux opérations), notées $+$ et $\times$ vérifiant les conditions suivantes :

1. $(K, +)$ est un groupe abélien.
2. $(K^*, \times)$ est un groupe où $K^* = K - \{0\}$.
3. La loi $\times$ est distributive par rapport à $+$.

Remarque 18.

1. Autrement dit, un corps est un anneau unitaire non réduit à 0 dans lequel tout élément $x \neq 0$ possède un inverse. Le groupe des unités du corps K, c'est-à-dire, le groupe des éléments inversibles pour la multiplication $\times$ est égal à $K^* = K - \{0\}$.
2. Un corps dont la multiplication est commutative est dit commutatif.

Proposition 19. *Soit A un anneau unitaire non réduit à $\{0\}$. Alors A est un corps si et seulement si les seuls idéaux de A sont A et $\{0\}$.*

Preuve. Supposons que les seuls idéaux de A soient A et $\{0\}$. Comme A est non nul, alors il existe $a \in A$ tel que $a \neq 0$. Soit $aA = \langle a \rangle$ l'idéal principal engendré par a. Comme il est non nul, i.e. $aA \neq \{0\}$, alors $aA = A$. Il existe donc $x \in A$ tel que $ax = 1$, 1 étant l'élément neutre de A. Ainsi a est inversible, et par suite A est un corps.

Inversement, si A est un corps et I un idéal non nul de A, alors pour tout $a \in I$ on a : $aa^{-1} = 1 \in I$; or tout idéal contenant 1 coïncide avec A. D'où la proposition. □

Exemple 4. Pour chaque nombre premier p, l'anneau $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ est un corps à p éléments.

Définition 14. On appelle sous-corps d'un corps K tout sous-ensemble k de K qui est lui même un corps par rapport à l'addition et à la multiplication de K.

Ainsi un sous-ensemble k de K est un sous-corps si k est un sous-groupe additif de K (pour l'addition de K) et si $k^* = k - \{0\}$ est un sous-groupe multiplicatif de K^*. Si k est un sous-corps de K, on dit que K est un sur-corps de k ou K est une extension de k.

Définition 15. On dit que deux corps K et L sont isomorphes s'il existe un isomorphisme de corps u de K sur L, c'est-à-dire une application bijective u de K sur L vérifiant $\forall (x,y) \in K^2,\ u(x+y) = u(x) + u(y)$, $u(xy) = u(x)u(y)$ et $u(1_K) = 1_L$.

Un automorphisme d'un corps K est un isomorphisme de K sur lui-même.

Lemme 7. *Soit K un corps et soit k un sous-corps de K. Alors K est un k-espace vectoriel. On note $[K : k]$ sa dimension, c'est-à-dire* $\dim_k(K) = [K : k]$.

Preuve. Comme K est un corps, alors $(K, +)$ est un groupe commutatif. De plus pour tous $(a, b) \in K \times K$ et $(x, y) \in k \times k$, on a :
$1.x = x$, $a(x + y) = ax + ay$, $(a + b)x = ax + ay$, $(ab)x = a(bx)$. D'où le résultat. □

Lemme 8. *Toute intersection de sous-corps d'un corps K est un sous-corps de K.*

Preuve. Comme cette propriété est vraie pour les anneaux unitaires, alors l'intersection des sous-corps de K est un sous-anneau unitaire de K. Soit a un élément non nul de cette intersection. Dans chacun des sous-corps, cet élément a est inversible dont l'inverse correspond est a^{-1}, l'inverse de a dans K. Donc a^{-1} est dans chacun des sous-corps et a est inversible dans l'intersection qui est donc un sous-corps de K. □

Définition 16. L'intersection, $\Pi(K)$, de tous les sous-corps d'un corps K est appelé sous-corps premier du corps K.

On dit qu'un corps k est un corps premier, s'il est le sous-corps premier d'un corps donné.

Remarques 5.

1. Un corps est donc premier s'il ne contient aucun sous-corps strict. C'est le plus petit corps contenu dans un corps donné.
2. Soit une partie X d'un corps K. On peut définir le plus petit sous-corps $\Pi_X(K)$ de K contenant X. C'est l'intersection de tous les sous-corps de K contenant X. En particulier, si $X = \{1_K\}$, 1_K est l'élément neutre pour la multiplication de K, alors le sous-corps $\Pi_{1_K}(K)$ est contenu dans tous les sous-corps de K. Il coïncide avec le sous-corps premier $\Pi(K)$.

   Dans le paragraphe suivant, nous déterminerons la structure de tous les corps isomorphes à un sous-corps premier d'un corps.

Exemple 5. Les corps $\mathbb{Q}$ et $\mathbb{F}_p$, où p est premier, sont des corps premiers. En effet,

- soit k un sous-corps de $\mathbb{Q}$, alors $0,\ 1 \in k$, d'où $\forall n \in \mathbb{Z}, n = n.1 \in k$. Comme k est un corps, alors $\forall n \in \mathbb{Z}^*, n^{-1} \in k$. Soit $x \in \mathbb{Q}$, alors x s'écrit sous la forme $\frac{m}{n}$ avec $(m,n) \in \mathbb{Z} \times \mathbb{Z}^*$, donc $x = \frac{m}{n} = mn^{-1} \in k$, d'où $\mathbb{Q} \subset k$, par suite $k = \mathbb{Q}$;
- soit k un sous-corps de $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, alors $0,\ 1 \in k$, d'où $\forall n \in \mathbb{Z}, \overline{n} = n.\overline{1} \in k$. D'où $\mathbb{F}_p \subset k$, par suite $k = \mathbb{F}_p$.

Proposition 20. *Soit K un corps, l'homomorphisme $\varphi : \mathbb{Z} \longrightarrow K;\ n \longmapsto n.1_K$ a pour noyau $p\mathbb{Z}$ avec p nul ou un nombre premier.*

Preuve. On sait que $\ker\varphi$, le noyau de φ, est un idéal de $\mathbb{Z}$, il est donc de la forme $p\mathbb{Z}$. Si φ est injective, alors $p = 0$ et $\ker\varphi = \{0\}$. Sinon c-à-d φ n'est pas injective, soit alors une factorisation $p = ab$ de p, alors a et b divisent p, et $\varphi(p) = 0 \Longleftrightarrow (a.1_K).(b.1_K) = 0$, et comme K est intègre, on a $a.1_K = 0$ ou $b.1_K = 0$. Donc $a \in \ker\varphi = p\mathbb{Z}$ ou $b \in \ker\varphi = p\mathbb{Z}$, d'où $p|a$ ou $p|b$. En résumé toute factorisation de $p = ab$ implique que $a = \pm p$ et $b = \mp 1$ ou $a = \pm 1$ et $b = \mp p$ ce qui prouve que p est un nombre premier. □

Définition 17. L'entier p nul ou premier de la proposition précédente est appelé la caractéristique de K.

Par la proposition 20 et la définition 17 on déduit le résultat suivant.

Remarque 19. Si K est un corps de caractéristique p avec $p \neq 0$, alors p est un nombre premier. C'est le plus petit entier positif non nul tel que $p.1_K = 0$.

Proposition 21. *Soient K un corps et p sa caractéristique.*

1. *Si $p \neq 0$, alors le sous-corps premier de K est isomorphe à $\mathbb{Z}/p\mathbb{Z}$.*
2. *Si $p = 0$, alors le sous-corps premier de K est isomorphe au corps des rationnels $\mathbb{Q}$.*

Preuve. Soit l'homomorphisme d'anneaux unitaires de la proposition 20

$$\begin{array}{rccc} \varphi : & \mathbb{Z} & \longrightarrow & K \\ & n & \longmapsto & n.1_K \end{array}$$

On a $\mathrm{Im}(\varphi) = \langle 1_K \rangle$, et son noyau est soit nul, soit égal à $p\mathbb{Z}$ par définition de la caractéristique p.

- Si $p \neq 0$, alors le sous-groupe additif $\langle 1_K \rangle = \{0, 1_K, \cdots, (p-1).1_K\}$ muni de la multiplication induite par celle de K est un sous-anneau commutatif isomorphe à $\mathbb{Z}/p\mathbb{Z}$; or p est premier, donc $\mathbb{Z}/p\mathbb{Z}$ est un corps. Comme ce sous-corps ne contient pas de sous-corps propre, on en déduit que c'est le sous-corps premier de K.

- Si la caractéristique est nulle, alors le groupe monogène $\langle 1_K \rangle$ est infini et isomorphe à $\mathbb{Z}$. C'est donc un sous-anneau commutatif intègre et le corps premier de K est isomorphe au corps des fractions de $\mathbb{Z}$ c'est à dire $\mathbb{Q}$. le corps $\mathbb{Q}$ peut être construit à partir de $\mathbb{Z}$, d'ailleurs $\mathbb{Q}$ est le corps des fractions de $\mathbb{Z}$. □

Remarque 20. Considérons le sous-groupe additif $Im(\varphi) = \langle 1_K \rangle = \{n.1_k \mid n \in \mathbb{Z}\}$ engendré par l'élément neutre 1_K du corps K. C'est un sous-groupe du groupe additif $(K, +)$.

Si $p \neq 0$, alors $Im(\varphi) \simeq \mathbb{Z}/p\mathbb{Z}$ est un sous-groupe fini, $\langle 1_K \rangle$ est un sous-groupe cyclique d'ordre fini p. Donc on a : $p.1_k = 0$, et l'équation $n.1_k = 0$ est vérifiée si et seulement si n est nul ou est un multiple de p.

Si $p = 0$, alors $Im(\varphi)$ est un sous-groupe infini, le groupe monogène $\langle 1_K \rangle$ est infini, l'équation $n.1_k = 0$ avec $n \in \mathbb{Z}$ implique $n = 0$.

Exemple 6. Les corps $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont de caractéristique 0. Pour tout p premier, $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ est de caractéristique p.

Proposition 22. *Soit K un corps commutatif de caractéristique $p \neq 0$. L'application*

$$\begin{array}{rccc} Frob: & K & \longrightarrow & K \\ & x & \longmapsto & x^p \end{array}$$

est un homomorphisme de corps. Il est appelé l'homomorphisme de Frobenius.

Preuve. Soient x et y dans K, la formule du binôme nous donne :

$$\begin{aligned} (x+y)^p &= \sum_{k=0}^{p} \mathsf{C}_p^k \, x^{p-k} y^k \\ &= x^p + \mathsf{C}_p^1 x^{p-1} y + \cdots + \mathsf{C}_p^k x^{p-k} y^k + \cdots + \mathsf{C}_p^{p-1} x y^{p-1} + y^p. \end{aligned}$$

où $\mathsf{C}_p^k = \dfrac{p!}{k!(p-k)!}$. Or pour tout k, $1 \leq k \leq p-1$, p divise C_p^k. Comme p est la caractéristique de K, on en déduit que pour tout k, $1 \leq k \leq p-1$, $\mathsf{C}_p^k = 0$. Donc

$$(x+y)^p = x^p + y^p.$$

Mais $Frob(x+y) = (x+y)^p$, ainsi $Frob(x+y) = Frob(x) + Frob(y)$ pour tous x, y dans K. De même, on a $Frob(xy) = (xy)^p = x^p y^p = Frob(x)Frob(y)$, et par suite $Frob$ est un homomorphisme du corps K. □

5.2. **Les corps finis.**

5.2.1. **Généralités.**

Définition 18. Un corps fini K est un corps contenant un nombre fini d'éléments.

Les premiers exemples de corps finis sont les quotients $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ de l'anneau $\mathbb{Z}$, où p est un nombre premier. D'autres exemples sont donnés par les quotients $\mathbb{F}_p[X]/\langle P\rangle$, où P est un polynôme irréductible de $\mathbb{F}_p[X]$, c'est un corps de cardinal p^n avec $n = \deg(P)$. Nous allons revenir sur ce point.

Soit K un corps fini, son sous-corps premier est donc fini. Il existe par suite (par la proposition 21) un nombre premier p tel que ce sous-corps premier soit isomorphe à $\mathbb{Z}/p\mathbb{Z}$. On en déduit que K est de caractéristique p.

Proposition 23. *Soit K un corps fini. Alors sa caractéristique est non nulle. Autrement dit, tout corps fini a pour caractéristique un nombre premier p. De plus son sous corps premier est (isomorphe à) $\mathbb{Z}/p\mathbb{Z}$.*

Remarque 21. Par la proposition 21 et sa preuve, tout corps fini K de caractéristique p, admet $L = \{0, 1_K, 2.1_K, \cdots, (p-1).1_K\} \simeq \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ comme sous corps. Par identification de L et $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, on déduit que K, ainsi que tous ses sous-corps, admettent $\mathbb{F}_p$ comme sous-corps (cela justifie l'appellation de corps premier pour $\mathbb{F}_p$).

Réciproquement, tout corps fini contenant le corps $\mathbb{F}_p$ est de caractéristique p.

Théorème 39. *Soit K un corps fini et L un sous-corps de K. Alors K est un espace vectoriel sur L de dimension finie, cette dimension $[K : L] = n$. De plus, l'ordre de K est $|L|^n$, où $|L|$ désigne l'ordre de L.*

Preuve. On sait par le Lemme 7 que K est un espace vectoriel sur L. Cet espace vectoriel est nécessairement de dimension finie puisque K est fini. Soit n cette dimension, on sait qu'il existe une base $\{b_1, b_2, \cdots, b_n\}$ de K sur L. Tout élément $x \in K$ s'écrit de façon unique

$$x = \alpha_1 b_1 + \alpha_2 b_2 + \cdots + \alpha_n b_n,\ \alpha_i \in L.$$

Considérons l'application f : $\begin{array}{ccc} K & \longrightarrow & L^n \\ x & \longmapsto & (\alpha_1, \alpha_2, \cdots, \alpha_n) \end{array}$

Il est simple de vérifier que f est bien définie et qu'elle est bijective. D'où le résultat. □

Corollaire 27. *Soit K un corps fini de caractéristique p. Il existe un entier $n \neq 0$ tel que le cardinal de K, $|K|$, soit égale à p^n, de plus $n = \dim_{\mathbb{F}_p}(K)$.*

Preuve. Le sous-corps premier de K est (isomorphe à) $\mathbb{F}_p$. On en déduit que K est un $\mathbb{F}_p$-espace vectoriel. Comme K est fini, cet espace vectoriel est de dimension fini sur $\mathbb{F}_p$. Il est donc isomorphe à $\mathbb{F}_p^n$ où $n = dim_{\mathbb{F}_p}(K)$. Comme $\mathbb{F}_p^n$ contient p^n éléments, on en déduit le corollaire. □

5.2.2. **Théorème de Wedderburn.** Le résultat suivant est publié en 1905 par le mathématicien écossais Joseph Henry Maclagen Wedderburn (1882-1948) mathématicien du xxe siècle. Il était membre de la Royal Society, il avait commencé à 16 ans ses études à l'université d'Édimbourg. Ses travaux portent sur les structures algébriques et tout particulièrement la théorie des corps, dans laquelle il met en évidence des exemples de corps non commutatifs.

Théorème 40 (Wedderburn). *Tout corps fini est commutatif.*

Pour démontrer ce théorème, nous avons besoin des résultats suivants. Soit $n \in \mathbb{N}^*$.

1. Une racine n-ième de l'unité ζ_n est dite **primitive** si $\zeta_n^n = 1$ mais $\zeta_n^d \neq 1$ pour tout $d = 1, \cdots, n-1$, c'est-à-dire ζ_n est une racine de l'unité d'ordre n. Autrement dit, ζ_n est une racine de $X^n - 1$ mais non de $X^k - 1$ pour tout $k < n$).
2. Il faut noter que si ζ_n est une racine primitive n-ième de l'unité, alors les autres n-ième racines de l'unité sont des puissances de ζ_n, et les autres racines primitive n-ième de l'unité sont ζ_n^k, où k est un entier premier avec n.
3. Notons aussi qu'une racine primitive n-ième de l'unité ζ_n est une racine du polynôme Φ_n suivant :
$$\Phi_n(X) = \prod_{0 \leq k < n,\ k \wedge n = 1} \left(X - e^{\frac{2ik\pi}{n}} \right),$$
où $k \wedge n = 1$ signifie que k et n sont premiers entre eux. Le polynôme Φ_n est dit **le n-ième polynôme cyclotomique**.
4. Une relation importante reliant les polyômes cyclotomiques et les racines primitives de l'unité est donnée par
$$\prod_{d|n} \Phi_d(X) = X^n - 1,$$
ce qui montre que x est racine de $X^n - 1$ si et seulement si x est une racine primitive d-ième de l'unité pour un certain d divisant n.
5. Soient m et n deux entiers avec $1 \leq m \leq n$, soit aussi $T \in \mathbb{Z}(X)$ la fraction rationnelle définie par : $T(X) = \dfrac{X^n - 1}{X^m - 1}$. Désignons par Φ_n le n-ième polynôme cyclotomique. Alors on a :

i. $\Phi_n \in \mathbb{Z}[X]$,

ii. si m divise n, alors $T(X) \in \mathbb{Z}[X]$

iii. si m divise n et $m < n$, alors Φ_n divise le polynôme T dans $\mathbb{Z}[X]$.

Preuve du Théorème de Wedderburn. La preuve sera faite par étape :

1. Soit k un corps fini, a priori non nécéssairement commutatif, et Z son centre, i.e.

$$Z = \{a \in k \ \ \forall x \in\in k, ax = xa\}.$$

On vérifie que Z est un sous-corps de k, commutatif, de cardinal $q \geq 2$ (car il contient au moins 0 et 1). De plus, k est un Z-espace vectoriel, donc il existe un entier n tel que $|k| = q^n$ (Théorème 39). Donc pour conclure k est commutatif, il suffit de montrer que $k = Z$, autrement dit $n = 1$ (c'est-à-dire $|k| = |Z| = q$).

2. Nous allons utiliser l'absurde, supposons que k n'est pas commutatif, ceci implique que $Z \neq k$. Pour tout $x \in k$, on note Z_x le centralisateur de x dans k, c'est-à-dire l'ensemble des éléments de k qui commutent avec x, i.e.

$$Z_x = \{a \in k \mid ax = xa\}.$$

Alors on montre que Z est un sous-corps de Z_x et que Z_x est un sous-corps de k. Donc Z_x est un Z-espace vectoriel, d'où d'après le Théorème 39, il existe un entier naturel non nul $d(x)$ tel que

$$|Z_x| = q^{d(x)}.$$

De même, k est un Z_x-espace vectoriel, donc une autre fois le Théorème 39, nous dit qu'il existe un entier naturel non nul m tel que $|k| = |Z_x|^m$.
Mais comme $|k| = q^n$, donc on obtient $q^n = (q^{d(x)})^m$, d'où $n = md(x)$. Retenons de cela que $d(x)$ **divise** n **pour tout** x **de** k.

3. Soit maintenant k^* le groupe multiplicatif de k, on sait qu'on peut faire agir k^* sur lui même par conjugaison, c-à-d, $\forall a \in k^*$, $\forall x \in k^*$; $a.x = axa^{-1}$. En effet, pour tous a, b, x dans k^* on a :
- $1.x = 1x1^{-1} = x$,
- $a.(b.x) = a.(bxb^{-1}) = a(bxb^{-1})a^{-1} = (ab)x(ab)^{-1} = (ab).x$.
Pour tout $x \in k^*$, soit $O_x = \{a.x = axa^{-1} \mid a \in k^*\} = k^*.x$ l'orbite de x, et soit aussi stab(x) $= k_x^*$ le stabilisateur de x sous l'action de k^*, on a :

$$\text{stab(x)} = k_x^* = \{a \in k^* \mid a.x = x\} = \{a \in k^* \mid axa^{-1} = x\} = \{a \in k^* \mid ax = xa\}.$$

Donc $Z_x = \text{stab(x)} \cup \{0\}$, d'où $|Z_x| = card(\text{stab(x)}) + 1$, ainsi

$$card(\text{stab(x)}) = |Z_x| - 1 = q^{d(x)} - 1.$$

Donc par la Proposition **??**, on obtient

$$|O_x| = [k^* : \text{stab(x)}] = \frac{|k^*|}{card(\text{stab(x)})} = \frac{q^n - 1}{q^{d(x)} - 1}.$$

Rappelons aussi que par le Lemme **??**, on a O_x est ponctuel ssi

$$O_x = \{x\} \Longleftrightarrow card(O_x) = 1 \Longleftrightarrow x \in Z^*.$$

Soit (x_i) est une suite de représentants des ℓ orbites non ponctuelles, la formule des classes s'écrit (voir Corollaire **??**) entraîne que :

$$|k^*| = |Z^*| + \sum_{i=1}^{\ell} \frac{|k^*|}{|Z^*_{x_i}|}.$$

soit, $q^n - 1 = q - 1 + \sum_{i=1}^{\ell} \frac{q^n - 1}{q^{d(x_i)} - 1} \Longleftrightarrow q - 1 = (q^n - 1) - \sum_{i=1}^{\ell} \frac{q^n - 1}{q^{d(x_i)} - 1}$.

4. Considérons la fraction rationnelle $F(X) = X^n - 1 - \sum_{i=1}^{\ell} \frac{X^n - 1}{X^{d(x_i)} - 1}$, alors on voit que $F(q) = q - 1$. Or on a vu que pour tout i, $d(x_i)$ divise n, alors la propriété 5ii page 49 nous permet de dire que $F(X) \in \mathbb{Z}[X]$. Mieux que ça, il est clair que $d(x_i) < n$. En effet, si $d(x_i) = n$, ceci implique $|O_{x_i}| = 1$, d'où $O_{x_i} = \{x_i\}$, et donc $x_i \in Z$, ce qui est faux. Alors la propriété 5iii page 49 permet d'affirmer que le polynôme cyclotomique Φ_n divise le polynôme $\frac{X^d - 1}{X^{d(x_i)} - 1}$ dans $\mathbb{Z}[X]$. Or Φ_n divise aussi $(X^n - 1)$ dans $\mathbb{Z}[X]$, on obtient donc que Φ_n divise le polynôme F dans $\mathbb{Z}[X]$. Autrement dit, il existe un polynôme $Q \in \mathbb{Z}[X]$ tel que $F = Q\Phi_n$. Ce qui implique que $F(q) = Q(q)\Phi_n(q)$. Et comme $F(q) = q - 1$, alors $q - 1 = Q(q)\Phi_n(q)$. De plus, $Q \in \mathbb{Z}[X]$, alors $Q(q)$ est un entier non nul, car $q \neq 1$ (Z contient au moins 0 et 1). Ainsi on déduit $\Phi_n(q)$ divise $q - 1$, et $|\Phi_n(q)| \leq q - 1$.
5. Notons par $\zeta_1, \cdots, \zeta_\ell \in \mathbb{C}$ les racines primitives n-ième de l'unité, on a

$$\Phi_n(q) = \prod_{i=1}^{\ell} (q - \zeta_i).$$

Comme $n > 1$, on a que $\zeta_i \neq 1$, pour tout i, donc en applicant l'inégalité triangulaire (qui est stricte ici car $\zeta_i \notin \mathbb{R}^+$), on obtient

$$|\Phi_n(q)| = \prod_{i=1}^{\ell} |q - \zeta_i| > \prod_{i=1}^{\ell} (|q| - |\zeta_i|) = (q-1)^{\ell} \geq (q-1).$$

Ce qui fournit une contradiction avec le point précédent. Ainsi $n = 1$ et $k = Z$ est commutatif.

□

Proposition 24. *Soit K un corps fini de caractéristique $p \neq 0$. Alors l'homomorphisme de Frobenius $Frob : K \longrightarrow K, \quad x \longmapsto x^p$ est un automorphisme.*

Preuve. L'homomorphisme de Frobenius est un homomorphisme de corps, donc il est injectif. Comme K est fini, il est aussi surjectif et donc bijectif. □

Remarque 22. Si $K = \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$, alors $Frob = id$. En effet, soit $x \in \mathbb{F}_p$, $x \neq 0$. Le groupe $\mathbb{F}_p^{\times} = \mathbb{F}_p^*$ des éléments inversibles est d'ordre $p - 1$. On en déduit $x^{p-1} = 1$ et donc $x^p = x$. D'où $Frob(x) = x$ pour tout $x \in \mathbb{F}_p$ et par suite $Frob = id$.

Le résultat suivant des corps finis joue un rôle important en cryptographie ainsi que pour la construction de certains codes correcteurs d'erreurs.

Théorème 41. *Soient K un corps commutatif et H un sous-groupe fini de $K^* = K^{\times}$, le groupe des éléments inversibles de K. Alors H est un groupe cyclique.*

Preuve. Soit d un diviseur de l'ordre de H. L'ensemble $U_d = \{x \in H \mid x^d = 1\}$ coïncide avec l'ensemble des racines distinctes du polynôme $X^d - 1 = 0$. Comme ce polynôme de $K[X]$ admet au plus d racines dans K, alors $card(U_d) \leq d$ (théorème 27 (page 31)), par suite le théorème 21 (page 25) implique que H est cyclique. □

Puisque tout corps fini est commutatif, on a le corollaire suivant.

Corollaire 28. *Soit K un corps fini. Alors le groupe $K^* = K^{\times}$ des éléments inversibles de K est cyclique.*

Preuve. D'après le théorème de Wedderburn, K est un corps commutatif. Donc le groupe K^* est un groupe abélien fini cyclique. □

Remarque 23. Il résulte du corollaire 28 que si K est un corps à q éléments, alors le groupe cyclique K^* est fini d'ordre $n = q - 1$ et possède $\varphi(q-1)$ générateurs. De plus,

par le théorème 19, si a est un générateur de K^*, alors l'ensemble des générateurs de K^* est

$$\{a^k \mid 1 \leq k \leq q-1 \text{ et } \text{pgcd}(k, q-1) = 1\}.$$

Définition 19. Les générateurs du groupe K^* sont appelés **éléments primitifs** de K (en réalité sont les racines primitives n$^{\text{ième}}$ de l'unité, avec $n = q-1$).

Remarque 24. L'importance d'un élément primitif $a \in K^*$ tient au fait qu'on peut décrire tous les éléments du groupe K^* en termes des $(q-1)$ premières puissances positives de a. Ce qui implique que si un sous-corps L de K contient un élément primitif a, alors $L = K$.

Exemples 4.

1. Pour $K = \mathbb{Z}/3\mathbb{Z} = \mathbb{F}_3$, on a $K^* = \{\overline{1}, \overline{2}\}$. Il est cyclique $K^* = \langle\overline{2}\rangle$. Il est isomorphisme au groupe (additif) $\mathbb{Z}/2\mathbb{Z}$.
2. Pour $K = \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$, p un nombre premier. On a $K^* = \{\overline{1}, \overline{2}, \cdots, \overline{p-1}\}$. Il est cyclique engendré par $\overline{p-1}$: $K^* = \langle\overline{p-1}\rangle$. Il est isomorphisme au groupe (additif) $\mathbb{Z}/(p-1)\mathbb{Z}$.

Ces exemples se généralisent aisément au résultat suivant (voir le Corollaire 16).

Corollaire 29. *Soit K un corps fini de cardinal q. Alors le groupe multiplicatif K^* est isomorphe au groupe $\mathbb{Z}/(q-1)\mathbb{Z}$.*

Exemple 7 (Exemple d'un corps à 4 éléments). On a par l'exemple 2 (page 34) que le polynôme $P(X) = X^2 + X + 1$ est le seul polynôme irréductible de degré 2 de l'algèbre $\mathbb{F}_2[X]$. Donc, par le corollaire 26 (page 39), $\mathbb{K} = \mathbb{F}_2[X]/\langle P\rangle$ est un corps, sa caractéristique est celle de $\mathbb{F}_2$ à savoir 2 et son cardinal est $2^{\deg(P)} = 2^2 = 4$. Désignons par α la classe d'équivalence du polynôme X dans $\mathbb{K} = \mathbb{F}_2[X]/\langle P\rangle$, alors le théorème 38 (page 41) implique que

$$\mathbb{K} = \mathbb{F}_2[X]/\langle P\rangle = \{a + b\alpha \mid a, b \in \mathbb{F}_2\} = \{0, 1, \alpha, 1+\alpha\}.$$

Le groupe $\mathbb{K}^*$ est cyclique d'ordre 3, il admet $\varphi(3) = 2$ générateurs qui sont α et α^2, car $\alpha^0 = 1$, $\alpha^1 = \alpha$ et $\alpha^2 = 1 + \alpha$. En tenant compte de l'égalité $P(\alpha) = 0 \Longleftrightarrow \alpha^2 = 1 + \alpha$, on a la table de multiplication de ce corps :

$\times$	0	1	α	$1+\alpha$
0	0	0	0	0
1	0	1	α	$1+\alpha$
α	0	α	$1+\alpha$	1
$1+\alpha$	0	$1+\alpha$	1	α

Exemple 8. Considérons le polynôme $P(X) = X^3 + X + 1 \in \mathbb{F}_5[X]$. Posons $K = \mathbb{F}_5[X]/\langle P\rangle$.

1. Montrer que K est un corps.
2. Donner la caractéristique et le cardinal de K.
3. Donner l'ordre et le nombre des générateurs du groupe K^*.
4. Donner une base du $\mathbb{F}_5$-espace vectoriel K.
5. Posons α la classe de X mod P, vérifier 2α est un générateur de K^*.

Exemple 9. On considère le polynôme $P(X) = X^4 + X + 1 \in \mathbb{F}_2[X]$.

1. Montrer que l'anneau $K = \mathbb{F}_2[X]/\langle P\rangle$ est un corps.
2. Quels sont la caractéristique et le cardinal de K ?
3. Soit α la classe de X modulo P. Montrer que α est un générateur de K^*. Combien y a-t-il de générateurs dans K^* ? Déterminer leurs coordonnées dans la base $\{1, \alpha, \alpha^2, \alpha^3\}$ de K sur $\mathbb{F}_2$.

5.3. **Construction des corps finis.** Pour ne pas alourdir le cours, nous allons admettre, dans ce paragraphe, quelques résultats. Commençons par le théorème suivant.

Proposition 25. *Soit K un corps fini (il est donc de caractéristique premier p). Soit a un élément primitif de K. L'ensemble des polynômes qui ont a comme racine est un idéal premier de $\mathbb{F}_p[X]$.*

Preuve. Soit I cet idéal, soient P et Q deux polynômes dans $K[X]$. Alors on a :

$$PQ \in I \iff PQ(a) = 0 \iff P(a) = 0 \text{ ou } Q(a) = 0 \iff P \in I \text{ ou } Q \in I.$$

Donc I est premier, et par suite maximal. □

Remarque 25. Le générateur de cet idéal est le polynôme minimal de a qui est un polynôme irréductible.

Proposition 26. *Soit K un corps fini (il est donc de caractéristique premier p). Soit a un élément primitif de K. Soit P le polynôme minimal de a dans $\mathbb{F}_p[X]$. Alors*

$$K \simeq \mathbb{F}_p[X]/\langle P\rangle.$$

Preuve. L'homomorphisme d'anneaux $f : \begin{array}{ccc} \mathbb{F}_p[X] & \longrightarrow & K \\ g(X) & \longmapsto & g(a) \end{array}$ se factorise $\overline{f} : \begin{array}{ccc} \mathbb{F}_p[X]/\langle P\rangle & \longrightarrow & K \\ g(\alpha) & \longmapsto & g(a) \end{array}$
qui est un homomorphisme de corps. Il est
- injectif (en tant qu'homomorphisme de corps)
- surjectif (son image contient tous les éléments de K^*, car elle contient a, a^2, $\cdots$, a^i, $\cdots$). D'où le résultat. □

Théorème 42. *Pour tout nombre premier p et tout entier positif n, il existe un polynôme irréductible de degré n dans l'anneau $\mathbb{F}_p[X]$.*

Preuve. Admis. □

Théorème 43. *Pour tout nombre premier p et tout entier positif n, il existe un corps à $q = p^n$ éléments.*

Preuve. Par le Théorème 42, il existe $P \in \mathbb{F}_p[X]$ un polynôme irréductible de degré n, donc le corps $K = \mathbb{F}_p[X]/\langle P\rangle$ est une extension de $\mathbb{F}_p$ telle que $[K : \mathbb{F}_p] = \deg(P) = n$, d'où le théorème 39 implique que K possède p^n éléments. □

Le théorème précédent peut s'énoncer comme suit :

Théorème 44. *Soit K un corps fini de cardinal p^n. Il existe un polynôme $P \in \mathbb{F}_p[X]$ irréductible de degré n tel que les corps K et $\mathbb{F}_p[X]/\langle P\rangle$ soient isomorphes.*

Les corps finis de cardinal p^n s'obtiennent donc exclusivement à partir des polynômes irréductibles de degré n dans $\mathbb{F}_p[X]$. Autrement dit :

Proposition 27. *Soient p un nombre premier et n un entier ≥ 1. Les deux propriétés suivantes sont équivalentes :*

1. *il existe un corps à p^n éléments.*
2. *il existe un polynôme irréductible de degré n dans $\mathbb{F}_p[X]$.*

Remarque 26. Par ce résultat, on peut affirmer qu'il exister des corps contenant 2, 3, $4 = 2^2$, 5, 7, 8, 9, $\cdots$, etc éléments ; mais il n'existe pas de corps à 6 éléments, 10 éléments.

Comme résumé, on donne le théorème suivant.

Théorème 45 (Existence de corps finis). *Soit n un entier positif et soit p un nombre premier, il existe un corps à p^n éléments.*

Plus précisément, soit $P \in \mathbb{F}_p[X]$ un polynôme irréductible de degré n et soit le corps $K = \mathbb{F}_p[X]/\langle P \rangle$, on désigne par α la classe d'équivalence du polynôme X dans K.

1. *Le corps K est constitué des éléments de la forme $R(\alpha)$, où R décrit l'espace vectoriel $\mathbb{F}_p[X]^{(n)}$ des polynômes de degré $\leq n-1$ de $\mathbb{F}_p[X]$ (c-à-d, $R \in \mathbb{F}_p[X]$ et $\deg(R) < n$).*
2. *Si $\beta \in K$, alors il existe un seul polynôme $R \in \mathbb{F}_p[X]^{(n)}$ tel que $\beta = R(\alpha)$.*
3. *La famille $\{1, \alpha, \alpha^2, \cdots, \alpha^{n-1}\}$ est une base de l'espace vectoriel K sur $\mathbb{F}_p$, donc $\dim_{\mathbb{F}_p}(K) = \deg(P)$.*
4. $\mathrm{card}(K) = p^n$.

Preuve.

1., 2. et 3. résultent du théorème 38 page 41.

4. Résulte de théorème 39. □

5.3.1. **Règles de calcul dans un corps fini.**

Proposition 28. *Soit K un corps fini de caractéristique p.*

1. $\forall (x, y) \in K^2, (x+y)^p = x^p + y^p$.
2. $\forall (x, y) \in K^2, \forall m \in \mathbb{N} - \{0, 1\}, (x+y)^{p^m} = x^{p^m} + y^{p^m}$.
3. $\mathbb{F}_p = \{x \in K \mid x = x^p\}$.
4. *Soit $Q \in K[X]$, on a l'équivalence*

$$Q \in \mathbb{F}_p[X] \Longleftrightarrow [Q(X)]^p = Q(X^p).$$

Preuve.

1. Par application de l'automorphisme de Frobenius.

2. Par récurrence sur m à partir de la question précédente.

3. Il est connu que le groupe $\mathbb{F}_p^*$ est d'ordre $p-1$, donc tout élément $x \in \mathbb{F}_p^*$ vérifie $x^{p-1} = 1$, d'où $x^p = x$, cette relation est aussi vérifiée par 0, donc $\mathbb{F}_p \subset \{x \in K \mid x = x^p\}$.

Réciproquement, le polynôme $X^p - X$ possédant au plus p racines dans K, on a donc l'inégalité $\mathrm{card}(\{x \in K \mid x = x^p\}) \leq p$, d'où l'égalité $\mathbb{F}_p = \{x \in K \mid x = x^p\}$.

4. Soit $Q(X) = a_0 + a_1 X + \cdots + a_n X^n$. D'après 1. on a

$$[Q(X)]^p = a_0^p + a_1^p X^p + \cdots + a_n^p (X^p)^n,$$

le résultat découle alors de 3. ci-dessus. □

Le théorème qui suit nous permettra d'effectuer des calculs pratiques dans un corps fini.

Théorème 46. *Soit K un corps fini à q éléments, de caractéristique p.*

1. *Si n est la dimension de l'espace vectoriel K sur $\mathbb{F}_p$, alors on a $q = p^n$.*
2. *Tout $x \in K^*$ vérifie $x^{q-1} = 1$, ce qui implique $x^{-1} = x^{q-2}$.*
3. *Tout $x \in K$ vérifie $x^q = x$.*
4. *Dans l'anneau $K[X]$, on a l'égalité : $X^{q-1} - 1 = \prod_{a \in K^*} (X - a)$.*
5. *Soit $a \in K$ un élément primitif de K. La famille*

$$B = \{1, a, a^2, \cdots, a^{n-1}\}$$

est une base de l'espace vectoriel K sur $\mathbb{F}_p$, c'est-à-dire que tout élément $x \in K$ s'écrit d'une façon unique $x = R(a)$, avec $R \in \mathbb{F}_p[X]^{(n)}$ (c-à-d, $R \in \mathbb{F}_p[X]$ et $\deg(R) < n$).

Preuve. 1. Conséquence du théorème 39 page 47.

2. et 3. Le groupe K^* est d'ordre $q-1$ donc tout $x \in K^*$ vérifie $x^{q-1} = 1 = xx^{q-2}$, d'où $x^q = x$, relation qui est aussi vérifiée par 0.

4. Résulte de 2. et du théorème 4.5 page 48.

5. Le corps K étant un espace vectoriel de dimension n sur $\mathbb{F}_p$, il suffit de montrer que la famille $B = \{1, a, a^2, \cdots, a^{n-1}\}$ est libre.
   Supposons le contraire, une relation linéaire non identiquement nulle entre les a_i équivaut à l'existence d'un polynôme non constant $P \in \mathbb{F}_p[X]^{(n)}$ tel que $P(a) = 0$. Soit B le sous $\mathbb{F}_p$-espace vectoriel de K engendré par la famille B. D'après notre hypothèse, $\dim(B) < n$ (la famille B est liée) donc B est strictement inclus dans K. On en déduit que $B \backslash \{0\}$ est strictement inclus dans K^*.
   Si on montre que B est un anneau, comme $B \backslash 0$ contient a, $B \backslash 0$ contiendra toutes les puissances positives de a et cela prouvera que a n'est pas un générateur de K^*.
   Par définition de B, on peut écrire

$$B = \{R(a) \mid R \in \mathbb{F}_p[X]^{(n)}\}. \tag{2}$$

   Soit $A = \{Q(a) \mid Q \in \mathbb{F}_p[X]\}$, montrons que $B = A$, ce qui prouvera que B est un anneau. Or il résulte de l'égalité (2) que $B \subset A$. Réciproquement, soit $Q \in \mathbb{F}_p[X]$, et soit $Q = PQ_1 + R_1$, avec $R_1 \in \mathbb{F}_p[X]^{(n)}$, la division euclidienne de Q par P, on a d'une part $Q(a) = R_1(a)$ puisque $P(a) = 0$, et d'autre part $R_1(a) \in B$ puisque $R_1 \in \mathbb{F}_p[X]^{(n)}$, ce qui prouve que $A \subset B$ et l'égalité.

□

Remarque 27. Comme pour tout $a \in K$, $a^q = a$, alors le point 4 du théorème 46 peut être remplacer par :

$$X^q - X = \prod_{a \in K} (X - a).$$

Le théorème suivant montre qu'il existe, à isomorphisme de corps près, un et un seul corps de cardinal p^n. On le note $\mathbb{F}_{p^n}$.

Théorème 47 (**Isomorphisme**). *Deux corps qui ont le même nombre d'éléments q sont isomorphes, ce qui permet de parler du corps $\mathbb{F}_q$ à q éléments.*

Preuve. Soient K et L deux corps ayant $p^n = q$ éléments. Soient a un élément primitif de K et P son polynôme minimal. Donc on a :

$$K \simeq \mathbb{F}_p[X]/\langle P \rangle.$$

Comme $a \in K$, a est racine de $X^q - X$, donc $P(X)$ divise $X^q - X$.
On a aussi

$$X^q - X = \prod_{a \in L} (X - a).$$

Donc il existe un élément $b \in L$ qui est aussi une racine de $P(X)$. Donc le polynôme minimal de b, soit $Q(X)$ est un diviseur de $P(X)$. Puisque $P(X)$ est irréductible et unitaire, on en déduit que $P(X) = Q(X)$. Donc

$$K \simeq \mathbb{F}_p[X]/\langle P \rangle = \mathbb{F}_p[X]/\langle Q \rangle.$$

On a un homomorphisme

$$\begin{array}{rccc} \varphi : & \mathbb{F}_p[X]/\langle Q \rangle & \longrightarrow & L \\ & h(\alpha) & \longmapsto & h(a) \end{array}$$

c-à-d un homomorphisme

$$\begin{array}{rccc} \varphi : & \mathbb{F}_p[X]/\langle P \rangle = \mathbb{F}_p[X]/\langle Q \rangle & \longrightarrow & L \\ & h(\alpha) & \longmapsto & h(a) \end{array}$$

Cet homomorphisme est injectif (car il est homomorphisme entre corps) et donc surjectif car $card(K) = card(L)$. Par suite K et L sont isomorphe. □

Remarque 28. On peut reformuler le résultat précédent comme ceci : deux corps finis contenant $\mathbb{F}_p$ et ayant le même degré ($[K : \mathbb{F}_p] = \dim_{\mathbb{F}_p}(K)$) sont isomorphes.
Ceci n'est plus vrai si les corps ne sont pas finis.

Corollaire 30. *Tout corps ayant p^n éléments est isomorphe à un corps de la forme $\mathbb{F}_p[X]/\langle P\rangle$ où P est un polynôme irréductible de degré n.*

Preuve. Soit a un élément primitif de K et P son polynôme minimal. Alors $K = \mathbb{F}(a) \simeq \mathbb{F}_p[X]/\langle P\rangle$. □

Exemple 10. $\mathbb{F}_8 \simeq \mathbb{F}_2[X]/\langle X^3+X+1\rangle$, $\mathbb{F}_{81} \simeq \mathbb{F}_3[X]/\langle X^4+X^3+2\rangle$, $\mathbb{F}_{125} \simeq \mathbb{F}_5[X]/\langle X^3+X+1\rangle$, $\mathbb{F}_{p^2} \simeq \mathbb{F}_p[X]/\langle X^2+1\rangle$, où p est un nombre premier.

5.4. **Problème du logarithme discret.**
Soit $\mathbb{K}$ un corps fini de cardinal $q = p^n$. On sait que $(\mathbb{K}^*,\times)$ est un groupe cyclique d'ordre $q-1$. Soit $b \in \mathbb{K}$ un élément primitif, c'est-à-dire un élément de $\mathbb{K}^*$ qui engendre $\mathbb{K}^*$. On a alors

$$\mathbb{K}^* = \{b^k \mid 0 \leq k \leq q-2\} = \{1, b, b^2, \cdots, b^k, \cdots, b^{q-2}\}.$$

Ce qui nous permet d'introduire la définition suivante.

Définition 20. Soit $y \in \mathbb{K}^*$, le logarithme discret de y dans la base b, noté $\log_b(y)$, est l'unique entier naturel $0 \leq k \leq q-2$ tel que $b^k = y$.

Exemple 11. Si $\mathbb{K} = \mathbb{F}_5 = \mathbb{Z}/5\mathbb{Z}$, alors on a :

$$2^0 = 1,\ 2^1 = 2,\ 2^2 = 4 \text{ et } 2^3 = 3.$$

Donc 2 est un élément primitif de $\mathbb{K}$, on a alors

$$\log_2(3) = 3,\ \log_2(4) = 2,\ \log_2(2) = 1.$$

Vérifier que 3 est un élément primitif de $\mathbb{K}$ et calculer $\log_3(4)$, $\log_3(3)$, $\log_3(2)$.

Le problème du logarithme discret est le suivant :
étant donné un élément primitif b de $\mathbb{K}^*$ et soit $y \in \mathbb{K}$. Trouver k tel que $b^k = y$.
Ce problème peut-être reformulé de la façon suivante :

soit b un élément primitif de $\mathbb{K}^*$. Connaissant b^x et b^y trouver b^{xy}
(Problème de Diffie-Hellman).

Certains algorithmes de cryptographie sont basés sur le fait que, pour certains corps finis de grand cardinal q, ce problème est difficile à résoudre. C'est le cas si l'on ne sait pas factoriser $q-1$, sur tout si $q-1$ possède un grand diviseur premier. Nous allons reprendre ce problème dans la suite.

Exemple 12. Étudions le problème du logarithme discret pour un corps fini déterminé par un polynôme. Soit le corps

$$\mathbb{K} = \mathbb{F}_3[X]/\langle P\rangle,\ P(X) = X^3 + 2X + 1.$$

$\mathbb{K}$ est bien un corps de caractéristique 3, car P est irréductible puisque il n'admet pas de racines dans $\mathbb{F}_3$, et son cardinal est $\text{card}(\mathbb{K}) = 3^3 = 27$. Donc $\mathbb{K}^*$ est cyclique d'ordre $27 - 1 = 26$. Les ordres des éléments de $\mathbb{K}^*$ sont donc 1, 2, 13 ou 26. Le seul élément d'ordre 1 est 1, et le seul élément d'ordre 2 est $-1 = 2$ (car $2^2 = 4 = 3+1 = 1$). Notons par α la classe de X modulo P, donc

$$P(\alpha) = 0 \Longleftrightarrow \alpha^3 + 2\alpha + 1 = 0 \Longleftrightarrow \alpha^3 = \alpha - 1.$$

(Notons que la caractéristique de $\mathbb{K}$ est 3, $3 = 0$, $-2 = 1$ et $-1 = 2$.)
Montrons que α est un générateur de $\mathbb{K}^*$, c'est-à-dire que α est d'ordre 26. On a

$$\begin{aligned}
\alpha^3 &= \alpha - 1\\
\alpha^9 &= (\alpha^3)^3 = (\alpha - 1)^3\\
&= \alpha^3 - 1 = \alpha - 2 = \alpha + 1 \text{ (ne pas oublier que } 3 = 0)\\
\alpha^{12} &= \alpha^9 \times \alpha^3 = (\alpha + 1)(\alpha - 1) = \alpha^2 - 1\\
\alpha^{13} &= \alpha(\alpha^2 - 1) = \alpha^3 - \alpha = -1\\
\alpha^{26} &= (-1)^2 = 1.
\end{aligned}$$

Par suite le résultat, c-à-d,

$$\mathbb{K}^* = \langle\alpha\rangle.$$

Résolvons maintenant le problème du logarithme discret de base α dans $\mathbb{K}^*$, c'est-à-dire pour chaque $x \in \mathbb{K}^*$ cherchons l'entier k $(0 \leq k \leq 25)$ tel que $x = \alpha^k$. On sait que chaque $x \in \mathbb{K}^*$ s'écrit sous la forme $a + b\alpha + c\alpha^2$, a, b, c dans $\mathbb{F}_3$, donc pour chacun de ces éléments cherchons k tel que

$$a + b\alpha + c\alpha^2 = \alpha^k,\quad 0 \leq k \leq 25.$$

Tout revient donc à calculer les puissances α^k pour $0 \leq k \leq 25$, c'est-à-dire calculer les éléments de $\mathbb{K}^*$.

k	0	1	2	3	4	5	6	7	8
α^k	1	α	α^2	$\alpha - 1$	$\alpha^2 - \alpha$	$2\alpha^2 + \alpha + 2$	$\alpha^2 + \alpha + 1$	$\alpha^2 + 2\alpha + 2$	$2\alpha^2 + 2$

k	9	10	11	12	13	14	15	16	17	18
α^k	$\alpha+1$	$\alpha^2+\alpha$	$\alpha^2+\alpha+2$	α^2+2	2	2α	$2\alpha^2$	$2\alpha+1$	$2\alpha^2+\alpha$	$\alpha^2+2\alpha+1$

k	19	20	21	22	23	24	25
α^k	$2\alpha^2+2\alpha+2$	$2\alpha^2+\alpha+1$	α^2+1	$2\alpha+2$	$2\alpha^2+2\alpha$	$2\alpha^2+2\alpha+1$	$2\alpha^2+1$

Ces tableaux nous permettrons de calculer le logarithme discret de n'importe quel élément x de $\mathbb{K}^*$. Par exemple si $x = 2\alpha^2 + 2$, alors $\log_\alpha(x) = 8$.

Remarque 29. Remarquons que les générateurs de $\mathbb{K}^*$ sont les éléments primitifs de $\mathbb{K}^*$, c-à-d, les éléments de la forme α^k où $1 \leq k \leq 25$ et k est premier avec 26. Donc ces générateurs sont :

$$\{\alpha^k \mid k = 1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25\}.$$

Références

[1] J. Dixmier, *Cours de mathématiques du premier cycle : première année*, Gauthier Villars (1973).

[2] J. Lelong-Ferrand et J. M. Arnaudiès, *Cours de mathématiques Tome* 1 *: Algèbre,* 3^e *édition*, Dunod Université (1978).

[3] Roger Codment, *Cours d'Algèbre,* (1996).

[4] M. Demazure, *Cours d'algèbre,* éditions Cassini, (1997).

[5] Serge Lang, *Algebra,* éditions Addison-Welsey.

[6] P. Samuel, *Théorie des nombres,* Collection Méthodes, éditions Hermann.

[7] J. P. Serre, *Cours d'arithmétique,* éditions PUF.

[8] Daniel Perrin, *Cours d'algèbre*, Ellipses, 1996.

[9] Alain Bouvier, Denis Richard, *Groupes. Observation, théorie, pratique,* Hermann, 1994.

[10] Josette Calais. *Éléments de théorie des groupes,* Puf, 1998.

[11] Eric Lehman. *Mathématiques pour l'étudiant de première année. Algèbre et géométrie,* Belin, 1984.

[12] Pierre Wassef. *Arithmétique, Application aux codes correcteurs et à la cryptographie, Cours et* 122 *exercices corrigés,* Licence de Mathématiques, Vuibert, 2008.

[13] S. Francinou, H. Gianella. *Exercices de mathématiques pour l'agrégation. Algèbre 1,* Masson (1994).

[14] J. Delcourt. *Théorie des groupes.* Dunod, (2001).

[15] M. E. Charkani, *Notes sur les Codes correcteurs : Cours et Exercices*, Master MIM 2008-09, Faculté des Sciences, Fés, Maroc.
https ://www.researchgate.net/publication/315682133_Notes_sur_les_Codes_correcteurs

[16] El Mamoun SOUIDI, *Théorie des codes correcteurs d'erreurs*, Master spécialisé Codes, Cryptographie et sécurité de l'information 2011. http ://www.souidi.net/masters/polyCodes.pdf .

[17] Alain Kraus. *Cours d'arithmétique, LM*220*,* Université de Paris VI 2006/07.