Gymnase Auguste Piccard
Loïc Devanthéry

3M3
Travail de maturité

Constructions de corps finis

Noémie Mousquès

Le 28 octobre 2019

Table des matières

Chapitre 1

Introduction

Qui d'entre vous a déjà entendu parler de chiffrement RSA ou AES ? Et pourtant, vous êtes amenés à utiliser régulièrement ces protocoles.
En effet, à l'époque du commerce électronique, de l'utilisation de cartes de crédit, du stockage de données dans le "nuage", chacun de nous utilise des algorithmes de cryptographie sans en avoir conscience. Ces algorithmes nous permettent de nous identifier, de garantir la confidentialité de données personnelles.

Mais savez-vous que ces méthodes de cryptographie reposent sur des théories mathématiques pures ?
La cryptographie ou "science du secret" est ainsi l'un des domaines d'application de la théorie des nombres ainsi que de la théorie des groupes.
La théorie des nombres étudie les propriétés des nombres entiers, elle s'intéresse ainsi aux problèmes de divisibilité et aux nombres premiers.
La théorie des groupes, c'est la partie de l'algèbre qui étudie les structures algébriques appelées groupes.

L'augmentation constante de la capacité de calcul des ordinateurs a cependant remis en cause la sécurité des protocoles existants. De nouveaux algorithmes basés sur des structures algébriques plus complexes, les corps finis, ont donc dû être développés. Actuellement, la cryptographie continue de réfléchir à l'élaboration de nouveaux algorithmes basés sur cette théorie. Mais comment construire des corps finis ?

Il existe des ouvrages élémentaires de cryptographie qui expliquent comment répondre à cette question mais plutôt selon une approche descriptive, un peu à la façon d'une recette de cuisine en caricaturant. On peut ainsi apprendre assez vite à construire un corps fini, mais sans comprendre pourquoi l'on procède ainsi car il manque les bases mathématiques de la théorie.

Ce travail de maturité a pour objectif ambitieux, mais réaliste j'espère, de répondre à cette question et d'expliquer à des gymnasiens les méthodes de construction de corps finis à l'aide de notions fondamentales d'algèbre et d'arithmétique.

Le public visé et le nombre limité de pages (2 contraintes imposées) ont nécessité un important travail de simplification d'autant plus grand de par l'origine des sources à disposition. En effet, si pour la théorie des groupes et des nombres on trouve de nombreux ouvrages adaptés à des gymnasiens, il en est différemment pour la théorie de structures algébriques plus complexes telles que les anneaux et les corps. Comme indiqué dans la bibliographie et la sitographie, les principales sources utilisées sont des cours d'algèbre destinés à des élèves de bachelor voire de master.

La forme retenue pour ce TM est donc celle d'un cours de mathématiques avec ses définitions,

ses exemples, ses théorèmes et ses quelques preuves (courage ...).
Même si dans un premier temps j'ai dû passer par cette étape, il ne s'agit pas d'une compilation allégée de divers cours d'algèbre où l'on énoncerait les notions les unes après les autres.
La perspective adoptée se veut autre. Ainsi, tout au long de ce rapport, j'ai essayé de conserver un fil conducteur et d'avancer un peu comme dans une enquête policière.

Sans vouloir "spoiler" la fin et les résultats, voici une présentation des principales parties de ce rapport.
Après une brève présentation des principales structures algébriques de base que sont les groupes, anneaux et corps, nous expliquerons comment réduire la taille de ces structures à partir de deux techniques.

Nous étudierons ensuite une famille d'anneaux particulière, celle des polynômes à coefficients dans un corps. Munis d'une division euclidienne, ces anneaux possèdent des proriétés arithmétiques semblables à celles des entiers relatifs dans $\mathbb{Z}$. Nous verrons comment construire des corps finis à partir de ces anneaux.

Nous essaierons aussi de construire des corps finis de petite taille par simple recherche intuitive.

Nous analyserons les résultats obtenus à l'aide d'éléments de théorie et présenterons des propriétés remarquables des corps finis fort utiles pour la détermination des éléments d'un corps.

Enfin, nous terminerons par une application pratique, la construction d'un corps fini à huit éléments, qui nous permettra d'illustrer les différentes notions présentées précédemment.

J'espère que vous prendrez du plaisir et de l'intérêt à lire ce rapport.

Chapitre 2

Eléments de théorie

2.1 Présentation des structures algébriques

2.1.1 Les groupes

Les groupes sont les structures algébriques les plus simples utilisées en cryptographie.

Définition 1. Un **groupe** est un ensemble G muni d'une loi interne $*$, c'est-à-dire le résultat de l'opération $*$ sur un couple (g, h) d'éléments de G donnent un élément qui est aussi dans G. On le note $g * h$ et l'on appelle le *composé* de g et h.
On impose à la loi $*$ de vérifier également les propriétés suivantes :

1. la loi $*$ est associative : $\forall g, h$ et $f \in G$, on a $g * (h * f) = (g * h) * f$.
2. il existe un élément neutre $e \in G : \forall g \in G, e * g = g * e = g$.
3. pour chaque élément $g \in G$ il existe un élément que l'on note $g' \in G$ et qu'on appelle *l'inverse de a*, tel que $g * g' = g' * g = e$.

Si la loi $*$ est en plus commutative, le groupe est dit *commutatif* ou abélien.

Propriétés :

1. l'élément neutre e est unique.
2. le symétrique d'un élément de G est unique.
3. $x * y = x * z \Rightarrow y = z$ et $y * x = z * x \Rightarrow y = z$.
   Cette propriété est intéressante pour la résolution d'équations.
   Elle implique aussi que les composés d'un élément donné x par des éléments distincts ne peuvent être égaux.

Démonstration.

1. Raisonnons par l'absurde et supposons qu'un groupe $(G, *)$ possède 2 éléments neutres distincts e_1 et e_2.
   Soit g un élément quelconque de G. On a :
   $$\begin{aligned} g * e_1 &= g * e_2 \\ g' * g * e_1 &= g' * g * e_2 \\ e_1 &= e_2 \end{aligned}$$
   Ce qui montre que l'élément neutre d'un groupe est unique.
2. Raisonnons par l'absurde et supposons que g possède 2 symétriques g' et g'' dans G.
   On a :

$$\begin{aligned} g * g' &= g * g'' \\ g' * g * g' &= g' * g * g'' \\ e * g' &= e * g'' \\ g' &= g'' \end{aligned}$$

Ce qui montre que le symétrique d'un élément $g \in G$ est unique.

3. Si $x * y = x * z \Rightarrow x' * (x * y) = x' * (x * z) \Rightarrow (x' * x) * y = (x' * x) * z \Rightarrow e * y = e * z \Rightarrow y = z$.

□

Exemple 1. Voici des ensembles de nombres déjà bien connus.

1. $\mathbb{N}$ muni de l'addition n'est pas un groupe car à part 0, ses éléments ne possèdent pas de symétrique.
2. L'ensemble des entiers relatifs $\mathbb{Z}$ est un groupe s'il est muni de l'addition : son élément neutre est 0, les symétriques sont les opposés et l'addition est bien sûr associative.
   Par contre, $\mathbb{Z}$ n'est pas un groupe pour la multiplication bien qu'il possède un élément neutre 1 et que la loi soit associatives. En effet, seuls 1 et -1 possèdent des inverses.
   Ainsi, un ensemble peut être un groupe pour une opération mais pas pour une autre.

Exemple 2. Il existe aussi des groupes finis. On appelle *cardinal* le nombre de leurs éléments.
Soit $\Omega = \{1; i; -1; -i\}$, un sous-ensemble de $\mathbb{C}$. Ω muni de la multiplication est un groupe fini de cardinal 4.

— la multiplication étant associative dans $\mathbb{C}$, elle l'est aussi dans tout sous-ensemble de $\mathbb{C}$ et donc dans Ω.

— pour vérifier les autres propriétés, on peut utiliser une **table de Cayley**. C'est tableau carré à double entrée obtenu en inscrivant à la i-ème ligne et à la j-ème colonne l'élément $x_i * x_j$. Elle contient donc autant de lignes et de colonnes que le cardinal du groupe.

Table de Cayley pour Ω muni de la multiplication :

$*$	1	i	-1	$-i$
1	1	i	-1	$-i$
i	i	-1	$-i$	1
-1	-1	$-i$	1	i
$-i$	$-i$	1	i	-1

Cette table confirme que 1 est l'élément neutre.
Elle nous donne le symétrique de chaque élément : $(1)' = 1$ / $(i)' = -i$ / $(-1)' = -1$ / $(-i)' = i$.
On remarque qu'un élément de Ω ne figure qu'une et une seule fois dans chaque ligne et dans chaque colonne. C'est une conséquence de la propriété (3) : les composés d'un élément donné g par des éléments distincts ne peuvent être égaux.
La table est symétrique par rapport à la diagonale des carrés car le groupe est commutatif.

2.1.2 Les anneaux

Même si l'existence d'un symétrique dans un groupe induit finalement l'existence d'une opération symétrique dans G (par exemple la soustraction par ajout de l'opposé), il est intéressant de pouvoir disposer d'une loi interne supplémentaire dans un ensemble.
Si les deux lois sont liées alors c'est encore mieux. C'est ce que permet un anneau.

Définition 2. Un **anneau** est un triplet $(A, \perp, *)$ formé par un ensemble A non vide et deux lois de composition interne $\perp$ et $*$, vérifiant les propriétés :

1. l'ensemble A muni de la première loi, $(A, \perp)$, est un groupe commutatif.

2. la deuxième loi est associative et admet un élément neutre e_* :
   pour tout $x \in A$, on a $x * e_* = e_* * x = x$.
3. la deuxième loi est distributive à droite et à gauche par rapport à la première :
   pour tout $x, y, z \in A$, on a $x * (y \perp z) = (x * y) \perp (x * z)$ et $(x \perp y) * z = (x * z) \perp (y * z)$.

Si la deuxième loi est commutative, l'anneau est dit **commutatif**.

Remarque : par la suite, par souci de simplification, on adoptera une notation additive pour la première loi et une notation multiplicative pour la deuxième.

Ci-dessous un tableau récapitulatif des notations additive et multiplicative :

Conventions	Notation additive	Notation multiplicative
élément neutre e	0	$e = 1$
symétrique de $h = h'$	$h' = -h$ (opposé)	$h' = h^{-1}$ (inverse)
	$n \cdot 0 = 0$	$h^0 = 1$
$h * h * ... * h$ (n fois) : composé $n^{\text{ième}}$ de h	nh (multiple)	h^n (puissance)
$h' * h' * ... * h'$ (n fois) : composé $n^{\text{ième}}$ de h'	$-nh$	h^{-n}

Exemple 3.

1. $\mathbb{Z}$ muni de l'addition et de la multiplication est un anneau commutatif :
   — on a déjà vu que $(\mathbb{Z}, +)$ est un groupe commutatif.
   — la multiplication dans $\mathbb{Z}$ est associative, commutative et distributive par rapport à l'addition.
   Son élément neutre est 1.
   Les seuls éléments de $\mathbb{Z}$ qui possèdent un inverse sont -1 et 1.
2. $\mathbb{Q}$ muni de l'addition et de la multiplication est aussi un anneau commutatif.
   Tous ses éléments à part 0 possèdent un inverse.

Propriétés :

1. pour tout élément $a \in A$, on a $0 \cdot a = a \cdot 0 = 0$.
2. si A est non réduit à $\{0\}$, alors 0 est différent de 1.
3. pour tout $a, b \in A$, alors $a \cdot (-b) = (-a) \cdot b = -a \cdot b$.
4. pour tout $a, b, c \in A$, on a $a \cdot (b - c) = ab - ac$ et $(b - c) \cdot a = ba - ca$.
5. l'élément neutre de la deuxième loi est unique.

Démonstration.

1. Soit $a \in A$. Montrons que $0 \cdot a = 0$.
   On a $a = 1 \cdot a = (1 + 0) \cdot a = 1 \cdot a + 0 \cdot a = a + 0 \cdot a$ donc $0 \cdot a = 0$.
2. Raisonnons par l'absurde. Si $0 = 1$, alors pour tout $a \in A$, on aurait $a = 1 \cdot a = 0 \cdot a = 0$ ce qui est impossible.
3. $(-a) \cdot b + ab = (-a + a) \cdot b = 0 \cdot b = 0$ donc $(-a) \cdot b = -ab$.
   $a \cdot (-b) + ab = a \cdot (-b + b) = a \cdot 0 = 0$ donc $a \cdot (-b) = -ab$.

4. $a \cdot (b-c) + ac = a \cdot ((b-c)+c) = a \cdot (b-c+c) = a \cdot (b+0) = ab \Rightarrow a \cdot (b-c) = ab - ac$.
   $(b-c) \cdot a + ca = ((b-c)+c) \cdot a = (b-c+c) \cdot a = (b+0) \cdot a = ba \Rightarrow (b-c) \cdot a = ba - ca$.
5. Raisonnons par l'absurde. Supposons qu'il existe deux éléments neutres distincts pour la $2^{\text{ème}}$ loi 1_1 et 1_2.
   On a $1_1 \cdot (1_1 - 1_2) = 1_1 \cdot 1_1 - 1_1 \cdot 1_2 = 1_1 - 1_1 = 0$.
   Mais $1_1 \cdot (1_1 - 1_2) = 1_1 \cdot 1_1 - 1_1 \cdot 1_2 = 1_1 - 1_2 \Rightarrow 1_1 - 1_2 = 0 \Rightarrow 1_1 - 1_2 + 1_2 = 1_2 \Rightarrow 1_1 = 1_2$ ce qui est impossible.

□

Propriété d'intégrité : un anneau A est dit intègre si pour tout $a, b \in A$ alors $ab = 0 \Rightarrow a = 0$ ou $b = 0$.
Cette propriété permet de résoudre les équations $ax = ay$ avec $a \neq 0$ même si a n'est pas inversible.
En effet, $ax = ay \Rightarrow ax - ay = 0 \Rightarrow a(x-y) = 0 \Rightarrow a = 0$ ou $x - y = 0 \Rightarrow x - y = 0 \Rightarrow x = y$.

Exemple 4.

1. $\mathbb{Z}$ est intègre car le produit de deux éléments non nuls ne peut être nul.
2. l'anneau M_2 des matrices carrées d'ordre 2 n'est pas intègre car :
   $\begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$

2.1.3 Les corps

On a vu qu'il existe des anneaux dont les éléments non nuls sont inversibles comme $\mathbb{Q}$. Ces anneaux sont des corps.

Définition 3. Un **corps** est un anneau non réduit à $\{0\}$ dont tous les éléments non nuls sont inversibles.
Si on pose $K^* = K \setminus \{0\}$ alors K^* est différent d'un ensemble vide et pour tout $k \in K$, il existe $k^{-1} \in K$ tel que $k \cdot k^{-1} = 1$.
Si la deuxième loi est commutative, on dit que le corps est commutatif.

Avec un corps, on dispose donc de deux groupes : un groupe additif avec $(K, +)$ et un groupe multiplicatif avec $(K^*, \cdot)$. Ces deux groupes sont liés par la propriété de distributivité.

Exemple 5. L'ensemble des réels $\mathbb{R}$ et celui des complexes $\mathbb{C}$ munis de l'addition et de la multiplication sont des corps. Ils disposent de quatre opérations : addition et soustraction par addition d'opposé, multiplication et division par multiplication par l'inverse.

Propriété : tous les corps sont **intègres**.

Démonstration.
Soient k, $l \in K$. Supposons que $k \cdot l = 0$.
1^{er} cas : $k = 0$.
$2^{\text{ème}}$ cas : $k \neq 0$ alors k est inversible.
$\Rightarrow k \cdot l = 0 \Rightarrow k^{-1} \cdot k \cdot l = k^{-1} \cdot 0 \Rightarrow 1 \cdot l = 0 \Rightarrow l = 0$. □

Finalement, sans le savoir, nous travaillions avec des corps depuis déjà bien longtemps. Ces ensembles de nombres $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont tous infinis.
Pour construire des corps finis, nous allons devoir réduire la taille des structures algébriques.

2.2 Comment construire des structures algébriques de taille réduite ?

Pour réduire la taille des structures algébriques, on dispose de deux principales méthodes :

1. on peut construire, définir un sous-ensemble d'une structure algébrique qui conserve les propriétés de cette structure et qui soit donc lui-même une structure algébrique. On crée ainsi une sous-structure.
2. On peut utiliser une relation de congruence pour construire une nouvelle structure algébrique à partir d'une structure existante en la "quotientant", par la technique de l'ensemble quotient.

2.2.1 Méthode 1 : construction d'une sous-structure

2.2.1.1 Les sous-groupes

(a) Définitions

Définition 4. Un **sous-groupe** $(H, *)$ d'un groupe $(G, *)$ est un sous-ensemble non vide H de G tel que $(H, *)$ est un groupe.

Propriétés :

1. l'élément neutre de $(H, *)$ est le même que celui de $(G, *)$.
2. pour tout $h \in H$, son symétrique h' dans G est aussi son symétrique dans H.

Démonstration.

1. Soit e_H l'élément neutre de H. Alors pour tout $h \in H$, on a $e_H * h = h * e_H = h$.
   Mais $h \in G \Rightarrow e_G * h = h * e_G = h$.
   Donc e_G est aussi un élément neutre de H. Si $e_G \neq e_H$, cela contredirait l'unicité de l'élément neutre dans H donc $e_G = e_H$.
2. Soient $h \in H$ et h'_H son symétrique dans H. Alors $h * h'_H = h'_H * h = e_H = e$ d'après (1).
   Mais h et h'_H sont aussi dans G donc h'_H est un symétrique de h dans G. Par unicité du symétrique dans G, on a $h'_H = h'_G$.

□

Exemple 6.

1. Soit $2\mathbb{Z}$, le sous-ensemble de $\mathbb{Z}$ constitué des multiples de 2. On a $2\mathbb{Z} = \{..., -6, -4, -2, 0, 2, 4, 6, ...\}$.
   $2\mathbb{Z}$ muni de l'addition est un sous-groupe commutatif de $(\mathbb{Z}, +)$ car :
   - si on additionne deux multiples de 2, on obtient un multiple de 2.
   - l'opposé d'un multiple de 2 reste un multiple de 2.
   - 0, l'élément neutre de $(\mathbb{Z}, +)$, est aussi l'élément neutre de $2\mathbb{Z}$.
   - l'addition induite sur $2\mathbb{Z}$ conserve ses propriétés d'associativité et de commutativité.
2. Plus généralement, les ensembles de la forme $n\mathbb{Z}$, $n \in \mathbb{N}$, muni de l'addition sont des sous-groupes de $(\mathbb{Z}, +)$.
   Soit $n \in \mathbb{N}$, alors $n\mathbb{Z} = \{\forall\ a \in \mathbb{Z},\ \exists\ b \in \mathbb{Z} \mid b = na\}$. Autrement dit, ce sont les multiples de n.
   Ce sont les seuls d'ailleurs.

Si G est un groupe fini, on ne peut pas construire des sous-groupes de n'importe quelle taille. C'est ce que nous dit le théorème de Lagrange que l'on démontrera ultérieurement car nous avons besoin de notions pas encore vues.

Théorème de Lagrange : Soient G un groupe fini et H un sous-groupe de G. Alors le cardinal de H divise celui de G.

(b) Sous-groupe engendré par un élément

Il n'est pas forcément évident de trouver un sous-ensemble qui conserve la structure de groupe et qui vérifie les propriétés requises pour être lui-même un groupe. En effet, comment choisir les éléments de ce sous-ensemble ?

Une méthode consiste à choisir un élément h de g et à se demander quels autres élémens il faudrait rajouter pour que le sous-ensemble contenant h conserve la structure de groupe.
Si H est un sous-groupe de $(G, +)$ contenant h alors il doit contenir e, h et son symétrique h'.
Par stabilité de la loi interne, avec une notation additive, il doit contenir :
$h + h$ mais aussi $h + h + h$, $h + h + h + h$, $h + h + ... + h$ (soient tous les "multiples" de h, les nh avec $n \in \mathbb{N}$).
$(-h) + (-h)$, $(-h) + (-h) + (-h)$, ... (soient tous les multiples de $(-h)$, les $n \cdot (-h)$ avec $n \in \mathbb{N}$).
Soit $H_h = \{g \in G \mid g = nh,\ n \in \mathbb{Z}\}$ avec la convention $0 \cdot h = 0_G = 0_H$.

1. on vient de voir que tout sous-groupe contenant h contient tous les éléments de H_h.
2. cet ensemble muni de l'addition est un groupe abélien. En effet, par construction, il y a stabilité de la loi interne, H_h contient l'élément neutre et chaque élément possède son symétrique dans H_h.

H_h est donc le plus petit sous-groupe de G contenant h.

Définition 5. Soient un groupe $(G, *)$ et $g \in G$. On appelle **sous-groupe engendré par** h le plus petit sous-groupe contenant h. On le note $< h >$.

— avec une notation additive, on a $< h >= \{h \in G \mid g = nh,\ n \in \mathbb{Z}\}$.

— avec une notation multiplicative, on aurait $< h >= \{h \in G \mid g = h^n,\ n \in \mathbb{Z}\}$.

On dit que h est un **générateur** de H.

Exemple 7.

1. $2\mathbb{Z}$ est le sous-groupe de $\mathbb{Z}$ engendré par 2.
   A noter que 2 n'est pas le seul générateur de $2\mathbb{Z}$, il y aussi (-2). Donc $2\mathbb{Z} =< 2 >=< -2 >$.
2. Plus généralement, $n\mathbb{Z} =< n >=< -n >$.

Remarque : si G est fini, alors d'après le théorème de Lagrange, le cardinal du sous-groupe engendré par un élément est un diviseur du cardinal de G.

(c) Ordre d'un élément et groupe cyclique

Soit $g \in (G, *)$. Il existe parfois un composé $n^{\text{ième}}$ de g égal à l'élément neutre.
Si G est fini, c'est le cas pour tous ses éléments. Si G est infini, il n'y a pas de règles.

Définition 6. On appelle **ordre de** g, s'il existe, le plus petit entier tel que son composé $n^{\text{ième}}$ soit égal à e. On le note $ord(g)$.
Le sous-groupe engendré par h est alors fini et son cardinal est égal à n.

Avec une notation multiplicative, on a $g^n = e$ et $< g >= \{g^m,\ m \in \mathbb{N}\} = \{1, g, g^2, ..., g^{n-1}\}$.
En effet, on a $g^{n+1} = g^n \cdot g = e \cdot g$, $g^{n+2} = g^n \cdot g^2 = e \cdot g^2 = g^2$ et plus généralement, pour tout $m \geqslant n$, on a $g^m = g^{m-n}$.
$\Rightarrow < g >= \{g^m,\ m \in \mathbb{N}\} = \{1, g, g^2, ..., g^{n-1}\}$.

Avec une notation additive, on a $ng = e$ et $< g >= \{mg,\ m \in \mathbb{N}\} = \{0, g, 2g, ..., (n-1)g\}$.

Propriété : Soit G un groupe fini. Alors l'ordre de tout élément divise le cardinal de G.

Démonstration.
L'ordre d'un élément est aussi égal au cardinal du sous-groupe qu'il engendre. Or, si G est fini, d'après le théorème de Lagrange, le cardinal de tout sous-groupe de G divise le cardinal de G donc l'ordre de g divise le cardinal de G. □

Conséquence : Soit G un groupe fini de cardinal n. Alors, pour tout $g \in G$, $g^n = e$.

Démonstration.
On vient de voir que $ord(g)$ divise n donc il existe $k \in \mathbb{N} \mid n = ord(g) \cdot k$.
$g^n = g^{k \cdot ord(g)} = (g^{ord(g)})^k = e^k = e$. □

Exemple 8. Soit un sous-groupe engendré par i dans $\mathbb{C}^*$ muni de la multiplication

- ⁕ On a $i^1 = i$, $i^2 = -1$, $i^3 = -i$, $i^4 = 1 \Leftrightarrow < i >= \{i^n,\ n \in \mathbb{N}\} = \{i, -1, -i, 1\}$.
  Le cardinal du sous-groupe engendré par i est bien égal à l'ordre de i soit 4.
- ⁕ 1 et (-1) sont d'ordre 2 qui divise 4 ; $(-i)$ et i sont d'ordre 4.
  On a donc pu construire un groupe fini à partir d'un élément d'un groupe infini.
  On retrouve Ω présenté précédemment. On dit que Ω est cyclique.

Définition 7. Un groupe G est dit **cyclique** s'il est fini et engendré par un de ses éléments.

Dans l'exemple précédent, $(-i)$ est aussi générateur de Ω car $(-i)^2 = -1$, $(-i)^3 = i$, $(-i)^4 = 1$. On a $\Omega =< -i >$.
Un groupe peut posséder ainsi plusieurs générateurs qui sont liés entre eux.

Théorème 1. Soit x un générateur d'un groupe G de cardinal n. Alors x^k générateur $\Leftrightarrow k$ premier avec n.

On en déduit que le nombre de générateurs d'un groupe cyclique G ne dépend que de son cardinal. Il est égal au nombre d'éléments premiers avec n compris entre 1 et n. On note ce nombre $\phi(n)$ et on l'appelle l'*indicatrice d'Euler* du nom du célèbre mathématicien suisse.

Exemple 9. $\Omega = \{i, -1, -i, 1\}$ de cardinal 4 possède $\phi(4) = \text{Card}(\{1, 3\}) = 2$ générateurs.
i est un générateur de Ω alors i^k est générateur si k est premier avec 4. Cela est vrai pour $k = 1$ et $k = 3$, ce qui nous donne comme générateur i^1 et $i^3 = -i$.

2.2.1.2 Les sous-anneaux et les sous-corps

Définition 8. Un **sous-anneau** B d'un anneau $(A, +, \cdot)$ est un sous-ensemble non vide de A tel que :

1. $(B, +)$ est un groupe abélien.
2. B est stable pour la multiplication.
3. $1_B = 1_A$ où $1_A \in B$.

Le plus petit sous-anneau de A est l'anneau nul ($= \{0\}$). On a $0 = 1$.

Sous-anneau engendré par un élément
Soit $a \in A$. On suppose que a est distinct de 0 et 1. Alors un anneau qui contient a doit contenir 0, 1 et $(-a)$.
Par stabilité additive, il doit contenir tous les multiples de a, soient les na, $n \in \mathbb{Z}$.
Par stabilité multiplicative, il doit contenir toutes les puissances de a, soient les a^n, $n \in \mathbb{Z}$.
Et par stabilité additive, il doit contenir les sommes des multiples de a et de ses puissances :

$$[a] = \{c_0 \cdot 1_A + c \cdot a + ... + c_i \cdot a^i + ... \text{ où } i \in \mathbb{N} \text{ et } c_i \in \mathbb{Z}\} = \{\sum_{i \in \mathbb{N}} (c_i \cdot a^i), \text{ avec } c^i \in \mathbb{Z}\}$$

On obtient une "combinaison linéaire" de puissances de a, ce qui nous fait penser à une structure polynômiale.

Exemple 10. Soit un sous-anneau engendré par i dans $(\mathbb{C}, +, \cdot)$.
On a $[i] = \{\sum(c_k \cdot i^k)$, avec $c_k \in \mathbb{Z}\}$. Comme $i^2 = -1$ alors $[i] = \{u + vi$, avec $u, v \in \mathbb{Z}\}$.
On appelle cet ensemble l'anneau des entiers de Gauss.

Définition 9. Un **sous-corps** K d'un corps $(L, +, \cdot)$ est un sous-ensemble non vide de L tel que :

1. K est un sous-anneau de L.
2. K est un corps $\Rightarrow K_{inv} = K^*$ (on dit que L est une extension de K).

Exemple 11. $\mathbb{Q}$ est un sous-corps de $\mathbb{R}$ qui est lui-même un sous-corps de $\mathbb{C}$.

La construction d'un corps à partir d'un élément k est plus complexe car il faut que les combinaisons linéaires des puissances de k soient inversibles dans K. Leur inverse dans L ne sera pas forcément un élément de K.

Exemple 12. L'anneau A des entiers de Gauss engendré par i n'est pas un corps car tous ses éléments ne sont pas inversibles dans A. Ainsi, $2i$ possède un inverse dans $\mathbb{C}$ égal à $\frac{-i}{2}$ car $2i \cdot (\frac{-i}{2}) = -i^2 = 1$.
Mais cet inverse n'est pas dans A car $\frac{-1}{2} \notin \mathbb{Z}$.

Conclusion : *Cette première méthode, même si elle est intéressante pour les groupes, ne nous permettra donc pas de construire un corps fini.*

2.2.2 Méthode 2 : construire une nouvelle structure à l'aide d'une relation de congruence / d'équivalence

2.2.2.1 Un peu de théorie des ensembles

Dans un ensemble, on peut chercher à regrouper les éléments qui possèdent des propriétés communes. on définit pour cela des relations d'équivalence.

Définition 10. Soit E un ensemble. Une **relation d'équivalence** $\mathcal{R}$ est une relation binaire (*i.e.* entre deux éléments de E) qui vérifie les propriétés suivantes :

1. $\mathcal{R}$ est réflexive : pour tout $x \in E$, on a $x\mathcal{R}x$.
2. $\mathcal{R}$ est transitive : pour tout $x, y, z \in E$ alors $x\mathcal{R}y$ et $y\mathcal{R}z \Rightarrow x\mathcal{R}z$.
3. $\mathcal{R}$ est symétrique : pour tout $x, y \in E$ alors $x\mathcal{R}y \Rightarrow y\mathcal{R}x$.

Définition 11. Soit $x \in E$ muni de $\mathcal{R}$. On appelle **classe d'équivalence de** x par $\mathcal{R}$ l'ensemble des éléments de E qui sont en relation avec x. On la note $\overline{x}$.
On a $x = \{y \in E \mid x\mathcal{R}y\}$.
A noter que deux éléments en relation appartiennent à la même classe : $x\mathcal{R}y \Leftrightarrow \overline{x} = \overline{y}$.
x et y ne sont finalement que des *représentants* de la classe.

Les classes d'équivalence définissent une **partition** de E c'est-à-dire un ensemble de parties non vides de E disjointes deux à deux et dont la réunion est égale à E.
Ainsi chaque élément de E appartient à une et une seule classe d'équivalence.

L'ensemble des classes d'équivalences forme **l'ensemble quotient de** E **par** $\mathcal{R}$. On le note E/R.
C'est un ensemble d'ensembles dont le nombre d'éléments est égal ou inférieur à celui de E.

Exemple 13. Soit l'ensemble formé par les 21 élèves de la 3M3.
On montre facilement que dans la 3M3 la relation "avoir le même âge" est une relation d'équivalence.

- Si Julie et Jonathan ont tous les deux 18 ans alors la classe de Julie est égale à celle de Jonathan. C'est l'ensemble des élèves ayant 18 ans. Notons-le G_{18}.
- Une classe d'équivalence est donc un groupe d'élèves ayant tous le même âge. Elle ne dépend pas du choix de son représentant.
- Si les âges possibles sont 16, 17, 18 et 19 ans alors on peut partager la 3M3 en 4 classes d'équivalence.
  L'ensemble quotient s'écrit 3M3/"avoir le même âge" $= \{G_{16}, G_{17}, G_{18}, G_{19}\}$.

Exemple 14. *un peu d'arithmétique dans l'ensemble des entiers relatifs* $\mathbb{Z}$
Dans $\mathbb{Z}$, on connaît la **relation** $\mathcal{R}$ **de congruence modulo** n définie par :
$a = b \bmod(n) \Leftrightarrow$ il existe $k \in \mathbb{Z}$ tel que $a = b + kn \Leftrightarrow$ il existe $k \in \mathbb{Z}$ tel que $(a - b) = kn$.
Autrement dit a et b sont congrus modulo n s'ils ont le même reste par la division euclidienne par n.
$\mathcal{R}$ est une relation d'équivalence car :

- elle est symétrique : $a = a + 0 \cdot n \Rightarrow a = a \bmod(n)$ avec $k = 0$.
- elle est réflexive : $a = b \bmod(n) \Rightarrow$ il existe $k \in \mathbb{Z}$ tel que $a = b + kn \Rightarrow b = a - kn \Rightarrow b = a + (-k)n \Rightarrow b = a \bmod(n)$.
- elle est transitive : si $a = b \bmod(n)$ et $b = c \bmod(n)$ alors il existe $k \in \mathbb{Z}$ tel que $a = b + kn$ et $k' \in \mathbb{Z}$ tel que $b = c + k'n$
  $\Rightarrow a = b + kn = c + k'n + kn = c + (k + k')n \Rightarrow a = c \bmod(n)$.

Les classes d'équivalence sont les classes des restes de la division euclidienne par n. Ces restes sont compris entre 0 et $n - 1$. $\mathcal{R}$ définit une partition de $\mathbb{Z}$ en n classes d'équivalence.
L'ensemble quotient de $\mathbb{Z}$ par la relation de congruence est $\mathbb{Z}/\mathcal{R} = \{\overline{0}, \overline{1}, \overline{2}, ..., \overline{n-1}\}$. On le note $\mathbb{Z}/n\mathbb{Z}$.

Application : prenons $\mathbb{Z}/3\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}\}$.
On a $\overline{0} = \{..., -6, -3, 0, 3, 6, ...\} = 3\mathbb{Z}$ = ensemble des multiples de 3.
$\overline{1} = \{..., -7, -4, 1, 4, 7, ...\}$ et $\overline{2} = \{..., -8, -5, 2, 5, 8, ...\}$.

2.2.2.2 Les groupes quotients

G est un ensemble donc on peut construire un ensemble quotient avec une relation d'équivalence $\mathcal{R}$.
Mais comment définir $\mathcal{R}$ pour doter cet ensemble des propriétés algébriques d'un groupe ?

(a) Définition de la relation d'équivalence $\mathcal{R}$
Dans $\mathbb{Z}$, la relation de congruence modulo n est définie par $a = b \bmod(n) \Leftrightarrow a - b \in n\mathbb{Z}$.
$n\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$ donc on va définir une relation de congruence dans G à partir d'un de ses sous-groupes.

Théorème 2. Soit H un sous-groupe de $(G, *)$ commutatif.
La relation $\mathcal{R}_H$ définie par $x\mathcal{R}_H y \Leftrightarrow x * y' \in H$ est une relation d'équivalence dans G.

Démonstration.

- $\mathcal{R}_H$ est symétrique : $g * g' = e \in H \Rightarrow g\mathcal{R}_H g$.
- $\mathcal{R}_H$ est réflexive : $g\mathcal{R}_H j \Leftrightarrow g * j' \in H \Leftrightarrow$ il existe $h \in H$ tel que $g * j' = h$.
  $\Rightarrow g * j' * j = h * j \Rightarrow g = h * j \Rightarrow h' * g = h' * h * j \Rightarrow h' * g = j \Rightarrow h' * g * g' = j * g' \Rightarrow j * g' = h'$.
  Mais $h \in H \Rightarrow h' \in H$ car H est un groupe donc $j * g' \in H \Rightarrow j\mathcal{R}_H g$.
- $\mathcal{R}_H$ est transitive : $g\mathcal{R}_H j$ et $j\mathcal{R}_H k \Rightarrow$ il existe $h, i \in H$ tels que $g * j' = h$ et $j * k' = i$.
  $\Rightarrow g * k' = g * j' * j * k' = h * i$.
  Mais par stabilité de H, $h, i \in H \Rightarrow h * i \in H$ donc $g * k' \in H \Rightarrow g\mathcal{R}_H k$.

□

On peut donc définir des classes d'équivalence et l'ensemble quotient $G/\mathcal{R}_H$.
On a $\overline{g} = \{k \in G \mid \exists h \in H \mid k = h * g\}$. On le note aussi $\overline{g} = Hg$.
En effet, si $j \in \overline{g}$ alors $j\mathcal{R}_H g \Rightarrow j * g' \in H \Rightarrow j * g' = h$, $h \in H' \Rightarrow j = h * g$.

Propriété : Si H est fini alors son cardinal est égal au cardinal de toute classe par $\mathcal{R}_H$.

Démonstration.
Soient $g \in G$ et f qui va de H dans $H * g$ qui à $h \in H$ associe $f(h) = h * g$.

1. f est injective. En effet, $f(h_1) = f(h_2) \Rightarrow h_1 * g = h_2 * g \Rightarrow h_1 * g * g' = h_2 * g * g' \Rightarrow h_1 * e = h_2 * e \Rightarrow h_1 = h_2$.
2. f est surjective. Soit $y \in Hg$ alors il existe $h \in H$ tel que $y = h * g$ donc $f^{-1}(y) = h$.

f est donc une bijection entre deux ensembles finis donc leur cardinaux sont égaux.
On a $\mathrm{Card}(H) = \mathrm{Card}(g * H)$. □

Si H est fini, toutes les classes d'équivalence par $\mathcal{R}_H$ ont donc le même cardinal. Or une relation d'équivalence définit une partition de G.
Si G est fini, on a donc $\mathrm{Card}(G) = \sum(\mathrm{Card}(\overline{g})) = \mathrm{Card}(H) \cdot$ nombre de classes d'équivalence.
Donc le cardinal de tout sous-groupe de G divise le cardinal de G. On vient de démontrer le théorème de Lagrange.

(b) Définition de la loi interne

Pour définir la loi interne de $G/\mathcal{R}_H$, nous allons utiliser la loi $*$ de G. On pose $\overline{x} * \overline{y} = \overline{x * y}$.

Pour que cette loi existe, il faut vérifier que le résultat de cette opération ne dépende pas du choix des représentants de la classe de x ou de y c'est-à-dire que si $\overline{x} = \overline{x_1}$ et $\overline{y} = \overline{y_1}$ alors $\overline{x * y} = \overline{x_1 * y_1}$.
Il faut donc montrer que si $x\mathcal{R}_H x_1$ et $y\mathcal{R}_H y_1$ alors $(x * y)\mathcal{R}_H(x_1 * y_1)$.

⁕ $x\mathcal{R}_H x_1 \Rightarrow$ il existe h_1 tel que $x_1 = h_1 * x$ et $y\mathcal{R}_H y_1 \Rightarrow$ il existe h_2 tel que $y_1 = h_2 * y$.
On a $(x*y)*(x_1*y_1)' = (x*y)*(h_1*x*h_2*y)'$.
Or $(h_1*x*h_2*y)' = y'*h_2'*x'*h_1'$ car $(y'*h_2'*x'*h_1')*(h_1*x*h_2*y) = e$.

$$\begin{aligned}(y'*h_2'*x'*h_1') &= y'*h_2'*x'*(h_1'*h_1)*x*h_2*y\\ &= y'*h_2'*x'*e*x*h_2*y\\ &= y'*h_2'*(x'*x)*h_2*y\\ &= y'*(h_2'*h_2)*y = y'*y = e\end{aligned}$$

donc $(x*y)*(x_1*y_1)' = (x*y)*y'*h_2'*x'*h_1' = x*y*y'*h_2'*x'*h_1' = (x*h'2*x')*h_1'$.

⁕ Si $x*h_2'*x \in H$, alors comme $h_1' \in H \Rightarrow (x*y)*(x_1*y_1)' \in H \Rightarrow (x*y)\mathcal{R}_H(x_1*y_1)$.
H doit donc vérifier la propriété suivante : pour tout $x \in G$, pour tout $h \in H$ alors $x*h*x' \in H$.
On dit que H est un *sous-groupe normal*.
A noter que si G est un groupe commutatif alors tous ses sous-groupes sont commutatifs et la propriété de normalité est toujours vérifiée. En effet, on a $x*h'*x' = x*x'*h' = e*h' = h' \in H$.

(c) Vérification des propriétés algébriques de groupe

On montre facilement que $G/\mathcal{R}_H$ muni de $*$ est un groupe.

— $(\overline{x}*\overline{y})*\overline{z} = \overline{x*y}*\overline{z} = \overline{(x*y)*z} = \overline{x}*\overline{y*z} = \overline{x}*(\overline{y}*\overline{z})$.

— pour tout $x \in G$, on a $\overline{x}*\overline{e} = \overline{x*e} = \overline{x}$ et donc $\overline{e}*\overline{x} = \overline{e*x} = \overline{x}$.
Donc $\overline{e}$ est l'élément neutre.
A noter que $\overline{e} = \{\forall\ k \in G, \exists\ h \in H \mid k = e*h = h\} = H$.

— pour tout $x \in G$, on a $\overline{x}*\overline{x'} = \overline{x*x'} = \overline{e}$ et $\overline{x'}*\overline{x} = \overline{x'*x} = \overline{e} \Rightarrow \overline{x'} = (\overline{x})'$.

2.2.2.3 Les anneaux quotients

(a) Principes de construction

⁕ Soient $(A, +, \cdot)$ un anneau commutatif et I un sous-groupe additif de A.
Soit $\mathcal{R}$ la relation définie par $x\mathcal{R}y \Leftrightarrow x - y \in I$.
On vient de voir que l'ensemble quotient $A/\mathcal{R}$ muni de l'addition $\overline{x}+\overline{y} = \overline{x+y}$ est un groupe avec pour élément neutre la classe de 0 (qui est égale à l'ensemble I).

⁕ On définit une *deuxième loi de composition interne* de la même manière que pour l'addition.
On pose $\overline{x}\cdot\overline{y} = \overline{xy}$.
Pour que cette loi existe, il faut que le résultat ne dépende pas du choix des représentants de la classe de x ou de y c'est-à-dire que si $x\mathcal{R}x'$ et $y\mathcal{R}y'$ alors $xy\mathcal{R}x'y' \Leftrightarrow xy - x'y' \in I$.
Si $x\mathcal{R}x'$ et $y\mathcal{R}y'$ alors il existe $i_1, i_2 \in I$ tels que $x' = x + i_1$ et $y' = y + i_2$.
Donc $x'y' = (x+i_1)\cdot(y+i_2) = xy + i_1\cdot y + x\cdot i_2 + i_1\cdot i_2 \Rightarrow x'y' - xy = i_1\cdot i_2 + i_1\cdot y + x\cdot i_2$.
Comme par stabilité multiplicative $i_1\cdot i_2 \in I$, il faudrait que $i_1\cdot y + x\cdot i_2$ soit dans I ou que chacun de ces termes soit dans I et cela pour tout x et y.
Le sous-groupe I doit donc vérifier une propriété supplémentaire, il doit être un "idéal".
Si I est un idéal, alors $(i_1\cdot y)$ et $(x\cdot i_2)$ sont des éléments de I donc $x'y' - xy \in I$.

Définition 12. Soit A un anneau commutatif.
Un **idéal** I est un sous-groupe additif de A tel que quelques soient $x \in I$ et $a \in A$, alors $x*a \in I$.
On dit que I est "absorbant" pour la multiplication.

Il reste à vérifier que A/I possède les autres *propriétés algébriques* d'un anneau.

— la multiplication est associative et distributive par rapport à l'addition.
$\overline{x}\cdot(\overline{y}\cdot\overline{z}) = \overline{x}\cdot\overline{y\cdot z} = \overline{x\cdot(y\cdot z)} = \overline{(x\cdot y)\cdot z} = \overline{x\cdot y}\cdot\overline{z} = (\overline{x}\cdot\overline{y})\cdot\overline{z}$.
$\overline{x}\cdot(\overline{y}+\overline{z}) = \overline{x}\cdot\overline{y+z} = \overline{x\cdot(y+z)} = \overline{(xy)+(xz)} = \overline{xy}+\overline{xz} = \overline{x}\cdot\overline{y}+\overline{x}\cdot\overline{z}$.

— on a $\overline{x} \cdot \overline{1} = \overline{1 \cdot x} = \overline{x}$ donc $\overline{1}$ est l'élément neutre de la deuxième loi.

Théorème 3. Soient A un anneau commutatif et I un idéal de A. Alors l'ensemble quotient A/I muni de l'addition et de la multiplication est un anneau.

(b) Les anneaux quotient $\mathbb{Z}/n\mathbb{Z}$

On a vu que $n\mathbb{Z}$ est un sous-groupe additif de $\mathbb{Z}$ engendré par n. C'est même un idéal de $\mathbb{Z}$.
En effet, soient $a \in \mathbb{Z}$ et $x \in n\mathbb{Z}$.
Alors il existe $z \in \mathbb{Z}$ tel que $x = nz \Rightarrow ax = anz = (az) \cdot n \in n\mathbb{Z}$.
Donc l'ensemble quotient $\mathbb{Z}/n\mathbb{Z}$ muni de l'addition et de la multiplication est un anneau.

Exemple 15. Soit $\mathbb{Z}/4\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$.
Par commodité, on enlève les "barres".
$\Rightarrow \mathbb{Z}/4\mathbb{Z} = \{0, 1, 2, 3\}$.
Table d'addition

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Table de multiplication

·	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

détail de calcul : $2 + 3 = 2 + 3 = 5 = 1$ et $2 \cdot 3 = 2 \cdot 3 = 6 = 2$.

On remarque que 2 n'est pas inversible car si on le multiplie par un autre élément de $\mathbb{Z}/4\mathbb{Z}$, on n'obtient jamais 1. L'anneau $\mathbb{Z}/4\mathbb{Z}$ n'est donc pas un corps.
Par contre 3 est inversible car $3 \cdot 3 = 1$. Son inverse est 3.

Exemple 16. Soit $\mathbb{Z}/3\mathbb{Z} = \{0, 1, 2\}$.
Table d'addition

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

Table de multiplication

·	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

On voit que tous les éléments non nuls de $\mathbb{Z}/3\mathbb{Z}$ sont inversibles : $2 \cdot 2 = 1$ et $1 \cdot 1 = 1$.
Donc l'anneau $\mathbb{Z}/3\mathbb{Z}$ est aussi un corps.

(c) Pourquoi ne construit-on pas le quotient d'un corps ?
Un corps étant un anneau, on devrait le quotienter par un de ses idéaux.
Mais les seuls idéaux d'un corps K sont $\{0\}$ ou K.

Démonstration. Soit I un idéal de K.
1er cas : $I = \{0\} \Rightarrow$ c'est un sous-groupe additif de K et est absorbant pour la multiplication donc c'est un idéal.
2eme cas : I non réduit à $\{0\}$. Il existe $a \in I$ non nul. a est inversible $\Rightarrow a^{-1} \in K$.
On a $a \cdot a^{-1} \in I$ car I est un idéal $\Rightarrow a \cdot a^{-1} = 1 \in I$.
Mais alors pour tout $k \in K$ on a $k \cdot 1 \in K \Rightarrow k \in I \Rightarrow I = K$. □

On obtient deux ensembles quotient K/K qui ne possède qu'une seule classe, celle de K et $K \setminus \{0\}$ qui possède autant de classes que d'éléments dans K. Ces structures ne sont pas intéressantes pour la construction de corps finis.

(d) Comment obtenir un anneau quotient qui soit un corps
L'exemple de $\mathbb{Z}/3\mathbb{Z}$ nous montre que des anneaux quotient peuvent être des corps. On peut se demander quelle propriété doit satisfaire l'idéal $3\mathbb{Z}$ pour que $\mathbb{Z}/3\mathbb{Z}$ soit un corps.
On remarque que contrairement à $4\mathbb{Z}$, $3\mathbb{Z}$ ne peut être contenu dans aucun autre anneau que $\mathbb{Z}$.
En effet, $3\mathbb{Z} \subset n\mathbb{Z} \Rightarrow n$ divise $3 \Rightarrow n = 1$ ou $n = 3 \Rightarrow n\mathbb{Z} = \mathbb{Z}$. Cette propriété s'appelle la maximalité.

Définition 13. Un **idéal I maximal** de A est un idéal différent de A qui vérifie :
$\forall\ J \subset A$, on a $I \subset J \subset A \Rightarrow J = I$ ou $J = A$.
Le plus grand idéal dans lequel I peut être inclus strictement est A.
Tout idéal contenant I strictement n'est autre que A.

On peut généraliser le résultat obtenu pour $\mathbb{Z}/3\mathbb{Z}$ en démontrant le théorème suivant :

Théorème 4. L'anneau quotient A/I est un corps si et seulement si I est un idéal maximal.

Démonstration.

1. Soit I, idéal maximal de A. Soit $a \in A$ tel que $\overline{a} \neq \overline{0}$ et montrons que $\overline{a}$ est inversible dans A/I.
   Soit $J_a = \{j \in A \mid j = ab + i \text{ avec } b \in A \text{ et } i \in I\}$.
   - ⁕ Montrons que J_a est un idéal de A.
     - — J_a est un sous-groupe additif de A car J_a est un sous-ensemble non vide de A tel que $(J_a, +)$ est un groupe. En effet :
       - — Soit $j \in J_a$ tel que $j = ab + i \Rightarrow -j = -(ab + i) = a \cdot (-b) + (-i)$. Comme A et I sont des groupes additifs, on a $(-b) \in A$ et $(-i) \in I \Rightarrow (-j) \in J_a$.
       - — Soit $k \in J_a$ tel que $k = ac + i' \Rightarrow j + k = ab + i + ac + i' = a \cdot (b + c) + (i + i') \in J_a$ car par stabilité additive, on a $b + c \in A$ et $i + i' \in I$.
     - — Soit $d \in A$. Alors $dj = d \cdot (ab + i) = dab + di = a(db) + di$.
       $di \in I$ par idéalité de I et $db \in A$ par stabilité de la multiplication donc $dj \in J_a$ et J_a est un idéal.
   - ⁕ On a $I \subset J_a$.
     Soit $i \in I$ alors $i = a \cdot 0 + i$. Or $0 \in A$ donc $i = ab + i$ avec $b = 0$. Donc $i \in J_a$.

⁕ Mais $\overline{a} \neq \overline{0} \Rightarrow a \notin I$. Or $a \in J_a$ car $a = a \cdot 1 + 0$ avec $1 \in A$ et $0 \in I$ donc $I \neq J_a$.

⁕ On a donc $I \subset J_a \subset A$ et $J_a \neq I$.
Comme I est maximal, alors $J_a = A$.
Or $1 \in A \Rightarrow 1 \in J_a \Rightarrow$ il existe $b \in A$ et $i \in I$ tels que $1 = ab + i$ d'où $\overline{1} = \overline{ab} + \overline{0} = \overline{a} \cdot \overline{b}$ donc $\overline{b}$ est l'inverse de $\overline{a}$.

2. Réciproquement. soit I un idéal de A tel que A/I soit un corps.
Soit J, un idéal de A tel que $I \subset J \subset A$.

— Si $J \neq I$ alors il existe $a \in J$ qui n'appartient pas à I donc $\overline{a}$ est non nulle et ainsi $\overline{a}$ est inversible dans le corps A/I.

— $\exists\, b \in A \mid \overline{1} = \overline{a} \cdot \overline{b}$ donc $\overline{1} = \overline{ab} \Rightarrow \overline{1} - \overline{ab} = \overline{0} \Rightarrow \overline{1 - ab} = \overline{0} \Rightarrow 1 - ab \in I$
$\Rightarrow \exists\, c \in I \mid 1 - ab = c \Rightarrow 1 = c + ab$.

— Mais $a \in J \Rightarrow ab \in J$ par idéalité de J. Et $c \in I \Rightarrow c \in J$. Par stabilité additive, $1 = ab + c \in J$.

— Mais un idéal qui contient l'unité est égal à A donc $J = A$.

J est donc un idéal maximal de A. □

Exemple 17. si p est premier, alors $\mathbb{Z}/p\mathbb{Z}$ est un corps.

— dans $\mathbb{Z}$, les idéaux maximaux non réduits à $\{0\}$ sont les $p\mathbb{Z}$ avec p premier.
En effet, si $n\mathbb{Z} \subset d\mathbb{Z}$ alors d divise n (ainsi $6\mathbb{Z} \subset 2\mathbb{Z}$).
Les idéaux maximaux sont ceux qui n'ont donc comme diviseur que 1 ou eux-mêmes. Ce sont les nombres premiers. Donc ce sont les $p\mathbb{Z}$ avec p un entier naturel premier.

— comme $\mathbb{Z}$ est un anneau et $p\mathbb{Z}$ un idéal maximal, l'ensemble quotient $\mathbb{Z}/p\mathbb{Z}$ est un corps.

On dispose donc d'une technique de construction de corps en quotientant un anneau par un idéal maximal ainsi que d'une première famille de corps finis, les $\mathbb{Z}/p\mathbb{Z}$.

On verra qu'ils jouent un rôle très important pour la construction des autres corps finis.

On aimerait bien trouver une famille d'anneaux qui aient les mêmes propriétés que $\mathbb{Z}$ et à partir desquels on pourrait construire de nouveaux corps.
Cette famille existe et nous en connaissons déjà quelques exemples.
Ce sont les anneaux de polynômes à coefficients dans un corps.

Chapitre 3

Construction de corps à partir d'anneaux de polynômes

3.1 Présentation des anneaux de polynômes

Définition 14. Soit A un anneau commutatif. Un **polynôme** P de degré n à coefficients dans A est un élément de la forme $P = a_n + a_1 \cdot X + a_2 \cdot X^2 + ... + a_n \cdot X^n$ avec $a_i \in A$ et $a_n \neq 0$.

On note $\deg(P)$ le degré n de P et on appelle a_n, le coefficient dominant de P.
$A[X]$ est l'ensemble des polynômes à coefficients dans A.

On connaît déjà $\mathbb{R}[X]$, l'ensemble des polynômes à coefficients dans $\mathbb{R}$.

On définit l'addition et la multiplication de deux polynômes P et Q de la même façon que dans $\mathbb{R}[X]$.

On montre que $A[X]$ muni de l'addition et de la multiplication est un anneau commutatif tel que :

- l'élément neutre pour l'addition est le polynôme constant égal à 0.
- l'opposé de P est $(-P)$.
- l'élément neutre pour la multiplication est le polynôme constant égal à 1.
- les inversibles sont les constantes non nulles inversibles dans A.

Exemple 18. $\mathbb{Z}/3\mathbb{Z}[X]$ est l'ensemble des polynômes à coefficient dans $\mathbb{Z}/3\mathbb{Z}$ à savoir $\overline{0}$, $\overline{1}$ ou $\overline{2}$.
$(\mathbb{Z}/3\mathbb{Z}, +, \cdot)$ est un anneau commutatif.
Soient $Q = \overline{1} + \overline{2} \cdot X$ et $R = \overline{2} + \overline{1} \cdot X^2$.
Alors :
$Q + R = (\overline{1} + \overline{2}) + \overline{2} \cdot X + \overline{1} \cdot X^2 = \overline{3} + \overline{2} \cdot X + \overline{1} \cdot X^2 = \overline{0} + \overline{2} \cdot X + \overline{1} \cdot X^2 = \overline{2} \cdot X + \overline{1} \cdot X^2$.

$$\begin{aligned} QR &= (\overline{1} + \overline{2} \cdot X)(\overline{2} + \overline{1} \cdot X^2) \\ &= \overline{1} \cdot \overline{2} + (\overline{1} \cdot \overline{1})X^2 + \overline{2} \cdot \overline{2} \cdot X + \overline{2} \cdot \overline{1} \cdot X^3 \\ &= \overline{1 \cdot 2} + \overline{1 \cdot 1} \cdot X^2 + \overline{2 \cdot 2} \cdot X + \overline{2 \cdot 1} \cdot X^3 \\ &= \overline{2} + \overline{4} \cdot X + \overline{1} \cdot X^2 + \overline{2} \cdot X^3 \\ &= \overline{2} + \overline{1} \cdot X + \overline{1} \cdot X^2 + \overline{2} \cdot X^3. \end{aligned}$$

On a bien $Q + R$ et QR dans $\mathbb{Z}/3\mathbb{Z}[X]$.

On admettra que si A est intègre, alors $A[X]$ est intègre.

Propriété : Si A est intègre alors pour tout $P, Q \in A[X]$ alors $\deg(PQ) = \deg(P) + \deg(Q)$.

Démonstration.
Par la définition de la multiplication, le potentiel coefficient dominant est égal à $a_n b_m$. Comme A est intègre, si $a_n \neq 0$ et $b_m \neq 0$ alors $a_n b_m \neq 0$ donc $a_n b_m$ est bien le coefficient dominant et $\deg(PQ) = n + m$. □

3.2 Division euclidienne dans $K[X]$

3.2.1 Division euclidienne dans $A[X]$

Dans $A[X]$, on ne peut pas effectuer de division par multiplication de l'inverse car tous ses éléments ne sont pas inversibles. On peut cependant dans certains cas effectuer une division euclidienne analogue à celle dans $\mathbb{Z}$.

Théorème 5. Soient A un anneau intègre et F et G deux polynômes de $A[X]$. Alors si le coefficient dominant de G est inversible dans A, il existe un unique couple (Q, R) de polynômes tels que :
$F = GQ + R$ avec $\deg(R) < \deg(G)$.

Démonstration.

- ⁕ <u>existence :</u> soit $G = g_0 + g_1 X^2 + ... + g_d X^d$ avec g_d inversible dans A. Alors $\deg(G) = d$.
  Soit $F = f_0 + f_1 X + f_2 X^2 + ... + f_n X^n$.
  Si $n < d$ alors le couple $(Q, R) = (0, F)$ convient.
  Sinon, posons $H_1 = F - f_n \cdot g_d^{-1} \cdot X^{n-d} \cdot G$ avec $m_1 = \deg(H_1)$ et h_{m_1}, coefficient dominant de H_1.
  On a $F = H_1 + f_n \cdot g_d^{-1} \cdot X^{n-d} \cdot G$ avec $\deg(H_1) = m_1 < n$.
  Si $m_1 < d$, alors le couple $(Q, R) = (f_n \cdot g_d^{-1} \cdot X^{n-d}, H_1)$ convient.

  Sinon posons $H_2 = H_1 - h_{m_1} \cdot g_d^{-1} \cdot X^{m_1-d} \cdot G$ avec $m_2 = \deg(H_2)$ et h_{m_2}, coefficient dominant de H_2.
  On a $F = H_1 + f_n \cdot g_d^{-1} \cdot X^{n-d} \cdot G = H_2 + h_{m_1} \cdot g_d^{-1} \cdot X^{m_1-d} \cdot G + f_n \cdot g_d^{-1} \cdot X^{n-d} \cdot G$.
  D'où $F = H_2 + (h_{m_1} \cdot g_d^{-1} \cdot X^{m_1-d} + f_n \cdot g_d^{-1} \cdot X^{n-d}) \cdot G$ avec $\deg(H_2) = m_2 < m_1 < n$.
  Si $m_2 < d$ alors le couple $(Q, R) = (h_{m_1} \cdot g_d^{-1} \cdot X^{m_1-d} + f_n \cdot g_d^{-1} \cdot X^{n-d}, H_2)$ convient.

  Sinon posons $H_3 = H_2 - h_{m_2} \cdot g_d^{-1} \cdot X^{m_2-d} \cdot G$ avec $m_3 = \deg(H_3)$ et h_{m_3}, coefficient dominant de H_3.
  On a $F = H_3 + (h_{m_2} \cdot g_d^{-1} \cdot X^{m_2-d} \cdot h_{m_1} \cdot g_d^{-1} \cdot X^{m_1-d} + f_n \cdot g_d^{-1} \cdot X^{n-d}) \cdot G$ avec $\deg(H_3) = m_3 < m_2 < m_1 < n$.

  On voit qu'à chaque itération, on diminue le degré de H_i.
  On continue jusqu'à ce que $\deg(H_i) < d$.
  On aura alors $F = R + QG$ avec $R = H_i$ et
  $Q = h_{m_{i-1}} \cdot g_d^{-1} \cdot X^{m_{i-1}-d} + h_{m_{i-2}} \cdot g_d^{-1} \cdot X^{m_{i-2}-d} + ... + h_{m_1} \cdot g_d^{-1} \cdot X^{m_1-d} + f_n \cdot g_d^{-1} \cdot X^{n-d}$.
- ⁕ <u>unicité :</u> supposons que $F = G \cdot Q_1 + R_1 = G \cdot Q_2 + R_2$ avec $\deg(R_1) < \deg(G)$ et $\deg(R_2) < \deg(G)$.
  Alors $G(Q_1 - Q_2) = R_2 - R_1$.
  Si $(R_2 - R_1) \neq 0$, comme A est intègre, alors $Q_1 - Q_2 \neq 0$.
  On aurait alors $\deg(G(Q_1 - Q_2)) = \deg(G) + \deg(Q_1 - Q_2) = \deg(R_2 - R_1) < \deg(G)$.
  Mais $\deg(Q_1 - Q_2) \geqslant 0$ donc on aurait $\deg(G) \leqslant \deg(G) + \deg(Q_1 - Q_2) < \deg(G)$ ce qui est impossible.
  Donc $R_2 - R_1 = 0$ et par intégrité de A, $Q_1 - Q_2 = 0$ d'où $R_2 = R_1$ et $Q_1 = Q_2$.

□

3.2.2 Division euclidienne dans l'anneau de polynômes à coefficients dans un corps K

Tout corps K est intègre donc on peut appliquer le théorème précédent.
Tous les éléments de K étant inversibles, le coefficient dominant de tout polynôme de $K[X]$ l'est aussi.
On peut donc effectuer la division euclidienne de tout couple de polynômes dans $K[X]$.
On dit que $K[X]$ est un *anneau euclidien.*

Le fait de prendre des coefficients dans un corps K permet donc de doter $K[X]$ d'une opération supplémentaire et de propriétés d'arithmétique. Comme dans $\mathbb{Z}$, on peut ainsi définir l'existence d'un *pgcd*, de nombres premiers et utiliser le théorème de Bezout.

3.2.3 Racines de polynômes

Théorème 6. Soient P un polynôme de $K[X]$ et $\alpha \in A$. On a α racine de $P \Leftrightarrow (X-\alpha)$ divise P.

Démonstration. Effectuons la division euclidienne de P par $X-\alpha$.
Il existe $Q, R \in A[X]$ tel que $P = Q \cdot (X-\alpha) + R$ avec $\deg(R) < \deg(X-\alpha) = 1$ donc $\deg(R) = 0$ et R est un polynôme constant.
Il existe $c \in A$ tel que $R = c$.
Supposons que α soit une racine de P alors $0 = P(\alpha) = Q(\alpha) \cdot (\alpha - \alpha) + R(\alpha) = R(\alpha) \Rightarrow c = 0 = R$ $\Rightarrow (X-\alpha)$ divise P.
Réciproquement, si $(X-\alpha)$ divise P alors il existe $Q \in A[X]$ tel que $P = (X-\alpha) \cdot Q$ donc $P(\alpha) = Q(\alpha) \cdot (\alpha - \alpha) = 0$. □

Théorème 7. Soit $\alpha_1, \alpha_2, ..., \alpha_k$ racines distinctes d'un polynôme P de $A[X]$, A étant intègre.
Alors le produit $(X-\alpha_1) \cdot (X-\alpha_2) \cdot ... \cdot (X-\alpha_k)$ divise P.

Démonstration.

1. Ancrage : Vérifions que c'est vrai pour $k = 1$ (déjà vu au théorème précédent).
2. Hypothèse : Supposons que c'est vrai pour k racines distinctes : $(X-\alpha_1) \cdot (X-\alpha_2) \cdot ... \cdot (X-\alpha_k)$ divise P.
3. Pas d'induction : au rang $k+1$: $(H) \Rightarrow$ il existe $Q \in A[X]$ tel que $P = (X-\alpha_1) \cdot (X-\alpha_2) \cdot ... \cdot (X- \alpha_k) \cdot Q$.
   Comme α_{k+1} est une racine, alors $P(\alpha_{k+1}) = (\alpha_{k+1}-\alpha_1) \cdot (\alpha_{k+1}-\alpha_2) \cdot ... \cdot (\alpha_{k+1}-\alpha_k) \cdot Q(\alpha_{k+1}) = 0$.
   Comme A est intègre, on en déduit que $Q(\alpha_{k+1}) = 0$ donc $X - \alpha_{k+1}$ divise Q.
   Il existe $Q' \in A[X]$ tel que $Q = Q' \cdot (X - \alpha_{k+1}) \Rightarrow P = (X-\alpha_1) \cdot (X-\alpha_2) \cdot ... \cdot (X-\alpha_k) \cdot (X-\alpha_{k+1}) \cdot Q'$.
   Donc $(X-\alpha_1) \cdot (X-\alpha_2) \cdot ... \cdot (X-\alpha_k) \cdot (X-\alpha_{k+1})$ divise P.

□

Théorème 8. Le nombre de racines distinctes d'un polynôme à coefficients dans un anneau intègre est égal au plus à son degré n.

Démonstration.
Si $\alpha_1, \alpha_2, ..., \alpha_k$ sont k racines d'un polynôme P, alors d'après le théorème précédent, il existe Q tel que $P = (X-\alpha_1) \cdot (X-\alpha_2) \cdot ... \cdot (X-\alpha_k) \cdot Q$.
Comme A est intègre, on a $\deg(P) = \deg(X-\alpha_1) + \deg(X-\alpha_2) + ... + \deg(X-\alpha_k) + \deg(Q) = \sum_{i=1}^{k} (\deg(X-\alpha_i) + \deg(Q))$.
D'où $\deg(P) = k \cdot 1 + \deg(Q)$ donc $k \leqslant n$. □

3.3 Recherche des idéaux dans $K[X]$

3.3.1 Idéal engendré par un polynôme

Définition 15. L'**idéal engendré par un polynôme** P est le plus petit idéal contentant P. C'est l'intersection de tous les idéaux contenant P. On le note (P).
Ce sont les "multiples" de P ou produit de P par un élément de $K[X]$.

Démonstration.
Soit $I = \{PQ, Q \in K[X]\}$.
Alors I est un idéal : c'est un sous-groupe additif de $K[X]$ et il est absorbant pour la multiplication : Soient $S \in K[X]$ et $T \in I$ alors il existe Q tel que $T = PQ \Rightarrow ST = SPQ = (SQ) \cdot P \in I$.
Soit J un idéal contenant P. Alors J doit contenir tous les PQ, $Q \in K[X] \Rightarrow J$ contient I. □

Un idéal qui est engendré par un de ses éléments est dit *principal*.

3.3.2 Autres idéaux

Théorème 9. Tous les idéaux de $K[X]$ sont principaux.
Soit I un idéal de $K[X]$ alors il existe $P \in K[X]$ tel que $I = (P)$.

Démonstration.
Soit P un polynôme de $K[X]$ alors (P) est un idéal.
Soit J un idéal de $K[X]$.
Premier cas : $J = \{0\}$ alors J est l'idéal engendré par le polynôme nul.
Deuxième cas : J non réduit à 0. Alors il existe un polynôme Q non nul de degré q appartenant à J.
Soit A, l'ensemble des degrés possibles des éléments de J. A est non vide car $q \in A$.
Posons p le plus petit degré possible dans A. Alors il existe $P \in K[X]$ tel que $\deg(P) = p$.
Montrons que $J = (P)$:

- Si J contient P alors il contient (P) car J est un idéal (il contient tous les multiples de P). Donc $(P) \subset J$.
- Soit $S \in J$. Alors $\deg(S) = s \geqslant \deg(P) = p$ par minimalité de p.
  Divisons S par P. Il existe $Q, R \in K[X]$ tel que $S = PQ + R$ avec $0 \leqslant \deg(R) < \deg(P) = p$.
  Comme $PQ \in (P)$ et $(P) \in J$ alors $PQ \in J$. Mais $S \in J$ donc $R = S - PQ \in J$. $\deg(R)$ doit être égal à 0 sinon cela contredirait la minimalité de p. On a donc $S = PQ \in (P)$.
  D'où $J \subset (P)$.

□

Remarque : dans $\mathbb{Z}$, les idéaux $n\mathbb{Z}$ sont aussi principaux. On a $n\mathbb{Z} =< n >$.

3.4 Construction de l'anneau quotient de $K[X]$ par un idéal (P)

3.4.1 Définition de la relation de congruence

Soit P de degré n dans $K[X]$. Comme (P) est un idéal, on peut définir l'anneau quotient $K[X]/(P)$.
La relation d'équivalence $\mathcal{R}$ s'écrit ici $Q_1 \mathcal{R} Q_2 \Leftrightarrow Q_1 - Q_2 \in (P) \Leftrightarrow$ il existe $S \in K[X]$ tel que $Q_1 - Q_2 = PS$.
On dit que Q_1 et Q_2 sont congrus modulo P.

3.4.2 Expression des éléments de $K[X]/(P)$

Les éléments de l'anneau quotient sont les classes d'équivalence. Une classe est composée de l'ensemble de polynômes qui ont le même reste par la division euclidienne par P.
Soient $Q \in K[X]$ et R de degré r, son reste par la division euclidienne par P. On a $r \leqslant n-1$.
Alors $R = \sum_{i=0}^{r}(r_i \cdot X^i)$ avec $r_i \in K$.
Alors $\overline{Q} = \overline{R} = \overline{\sum_{i=0}^{r}(r_i \cdot X^i)} = \sum_{i=0}^{r}(\overline{r_i \cdot X^i}) = \sum_{i=0}^{r}(\overline{r_i} \cdot \overline{X}^i)$.
Tout élément de l'anneau s'écrit comme un polynôme de $\overline{X}$ de degré inférieur ou égal à $n-1$.
Réciproquement, si $a = \sum_{i=0}^{r}(a_i \cdot \overline{X}^i)$ alors a est la classe du polynôme $A = \sum_{i=0}^{r}(a_i \cdot X^i)$ donc $a \in K[X]/(P)$.
On aimerait donc écrire $K[X]/(P) = \{\sum_{i=0}^{n-1}(k_i \cdot \overline{X}^i),\ k_i \in K\}$.

Mais prenons deux polynômes P_1 et P_2 de même degré n. Alors on aurait $K[X]/(P_1) = \{\sum_{i=0}^{n-1}(k_i \cdot \overline{X}^i),\ k_i \in K\}$ et $K[X]/(P_2) = \{\sum_{i=0}^{n-1}(r_i \cdot \overline{X}^i),\ k_i \in K\}$.
Cela pourrait donner la fausse impression que ces deux anneaux sont égaux.
Il ne faut pas oublier que $\overline{X}$ ne désigne pas le même ensemble.
En fait, il manque l'information que $\overline{P_i} = 0$. En effet, si $P = \sum_{i=0}^{n-1}(p_i \cdot X^i)$ alors $\overline{P} = 0 \Rightarrow \sum_{i=0}^{n-1}(p_i \cdot \overline{X}^i) = 0$.

Si l'on intègre cette condition alors l'anneau quotient s'écrit :
$K[X]/(P) = \{\sum_{i=0}^{n-1}(k_i \cdot \overline{X}^i),\ k_i \in K \text{ avec } \sum_{i=0}^{n-1}(p_i \cdot \overline{X}^i) = 0\}$.

3.4.3 Opérations dans $K[X]/(P)$

- l'addition s'effectue normalement dans $K[X]$.
  En effet, si on additionne deux polynômes de degré strictement inférieur à n, alors on obtient un polynôme de degré strictement inférieur à n.
- la multiplication s'effectue normalement puis on effectue la division euclidienne du résultat par P. Le reste de cette division est le produit de la multiplication.

Exemple 19. Soient $K = \mathbb{R}[X]$ et $P = X^2 + 1$. Alors $K[X]/(P) = \mathbb{R}[X]/(X^2+1) = \{a \cdot \overline{X} + b,\ (a,b) \in \mathbb{R}^2 \text{ avec } \overline{X}^2 + 1 = 0\}$.
Soient $R = 3\overline{X} + 1$ et $S = \overline{X} + 8$.
On a :

- $R + S = (3\overline{X} + 1) + (\overline{X} + 8) = 4\overline{X} + 9$.
- $RS = (3\overline{X} + 1) \cdot (\overline{X} + 8) = 3\overline{X}^2 + 25\overline{X} + 8 = 3(\overline{X}^2 + 1) + (25\overline{X} + 5) = 25\overline{X} + 5$.

Pour calculer RS on aurait pu utiliser le fait que $\overline{X}^2 + 1 = 0 \Rightarrow \overline{X}^2 = -1$.
$RS = 3\overline{X}^2 + 25\overline{X} + 8 = 3(-1) + 25\overline{X} + 8 = 25\overline{X} + 5$.

A noter que c'est au niveau de la multiplication que l'on verra une différence de résultats dans un anneau quotienté par deux polynômes de même degré.

Reprenons l'exemple précédent avec $P = \overline{X}^2 + 2$. Alors $\mathbb{R}[X]/(X^2+2) = \{a\overline{X} + b,\ (a,b) \in \mathbb{R}^2$ avec $\overline{X}^2 + 2 = 0\}$.
Soient $R = 3\overline{X} + 1$ et $S = \overline{X} + 8$.
On a :

— $R + S = (3\overline{X} + 1) + (\overline{X} + 8) = 4\overline{X} + 9$.

— $RS = (3\overline{X} + 1) \cdot (\overline{X} + 8) = 3\overline{X}^2 + 25\overline{X} + 8$.
Or $\overline{X}^2 + 2 = 0 \Rightarrow \overline{X}^2 = -2 \Rightarrow RS = 3 \cdot (-2) + 25\overline{X} + 8 = 25\overline{X} + 2$.

3.5 Recherche d'idéaux maximaux

Dans $\mathbb{Z}$, les idéaux maximaux sont engendrés par p premier. Dans $\mathbb{R}[X]$, on a vu que ce sont les polynômes irréductibles qui jouent le rôle de nombres premiers. On les utilise pour la factorisation des autres polynômes un peu comme selon le principe de décomposition d'un entier relatif en nombres premiers.
On a appris qu'un polynôme irréductible est un polynôme que "l'on ne peut pas factoriser".
Il existe une défintion plus précise.

Définition 16. P est **irréductible** dans $K[X]$ s'il est non-constant (non inversible) et si ses seuls diviseurs sont les inversibles de $K[X]$ c'est-à-dire les polynômes constants non nuls et les polynômes qui lui sont associés c'est-à-dire les polynômes de la forme λP, $\lambda \in K^*$.
Autrement dit, on ne peut pas écrire P sous la forme d'un produit de deux polynômes Q et R de degré supérieur ou égal à 1.

Théorème 10. Soit $P \in K[X]$. Si P est irréductible dans $K[X]$ alors (P) est maximal.

Démonstration.
En effet, si (P) n'est pas maximal, il est contenu dans un idéal I tel que $I \neq K[X]$. Comme l'anneau $K[X]$ est principal, I est un idéal principal. Il existe donc $Q \in K[X]$ tel que $I = (Q)$. Comme $(P) \subset (Q)$ alors $P \in (Q)$ donc il existe $R \in K[X]$ tel que $P = QR$.
Si l'inclusion (P) dans (Q) est stricte, alors le degré de R est supérieur ou égal à 1 et P n'est pas irréductible ce qui est impossible. □

3.6 Recherche de polynômes irréductibles

Exemple 20. les polynômes de degré 1 sont toujours tous irréductibles.
Soit $P = aX + b$ de degré 1. Si $P = QR$, alors $(\deg(Q), \deg(R)) = (1,0)$ ou $(\deg(Q), \deg(R)) = (0,1)$.
Supposons que $(\deg(Q), \deg(R)) = (1,0)$ alors Q est un polynôme constant c non nul et $R = dX + e$.
Par identification des coefficients on a $a = cd$ et $b = ce$ donc $R = c^{-1} \cdot P$.
R est donc un polynôme associé à P.

On a pris l'habitude pour tester l'irréductibilité d'un polynôme de vérifier s'il a des racines. En effet, un polynôme irréductible n'a pas de racine a sinon $(X - a)$ divise P.
Mais la réciproque n'est pas toujours vraie. Elle l'est seulement pour des polynômes de degré 2 ou 3.

Théorème 11. Soit $P \in K[X]$ et de degré égal à 2 ou 3.
On a l'équivalence : P irréductible sur $K[X] \Leftrightarrow P$ n'a pas de racines dans K.

Démonstration.
On a vu que quand P est irréductible, il n'a pas de racines.
Réciproquement, montrons que quand P n'a pas de racines, il est irréductible.

Il suffit de montrer que P est réductible $\Rightarrow$ P a au moins une racine.
Supposons que P est réductible. Alors il existe Q et R tel que $P = QR$ avec $\deg(Q) \geqslant 1$ et $\deg(P) \geqslant 1$.
Premier cas : $\deg(P) = 2$.
On a $\deg(P) = \deg(Q) + \deg(R)$ donc $\deg(Q) = \deg(R) = 1$.
Si Q et R sont associés, on a une racine de multiplicité 2.
Si Q et R ne sont pas associés, on a 2 racines distinctes.
Deuxième cas : $\deg(P) = 3$.
On a $\deg(P) = \deg(Q) + \deg(R)$ donc $(\deg(Q), \deg(R)) = (1, 2)$ ou $(\deg(Q), \deg(R)) = (2, 1)$.
Supposons que $\deg(Q) = 1$ alors il existe $a, b \in A$ tel que $Q = aX + b$ avec $a \neq 0$.
K est un corps $\Rightarrow$ a est inversible $\Rightarrow$ $\tilde{Q}(-b \cdot a^{-1}) = 0 \Rightarrow \tilde{P}(-b \cdot a^{-1}) = 0 \Rightarrow P$ admet une racine $-b \cdot a^{-1}$. □

On dispose ainsi d'un *critère d'irréductibilité* pour les polynômes de degré 2 ou 3.

Exemple 21. Soit l'anneau $\mathbb{Z}/2\mathbb{Z}[X]$ des polynômes à coefficients dans $\mathbb{Z}/2\mathbb{Z} = \{0, 1\}$.
Pour tester l'irréductibilité des polynômes de degré 2, il suffit de chercher les éventuelles racines.
Si $P = X^2 + 1 \in \mathbb{Z}/2\mathbb{Z}[X] \Rightarrow P(1) = 1 + 1 = 0$ et $P(0) = 0 + 1 \Rightarrow P$ admet une racine $\Rightarrow$ il n'est pas irréductible.
Si $P = X^2 + X + 1 \in \mathbb{Z}/2\mathbb{Z}[X] \Rightarrow P(1) = 1 + 1 + 1 = 1$ et $P(0) = 0 + 0 + 1 = 1 \Rightarrow P$ sans racine $\Rightarrow$ il est irréductible.

3.7 Construction de corps par la relation de congruence sur des polynômes irréductibles

Théorème 12. Si P est irréductible alors l'anneau quotient $K[X]/(P)$ est un corps.

Démonstration. si P est irréductible, (P) est maximal donc l'anneau quotient $K[X]/(P)$ est un corps. □

On peut dresser un tableau récapitulant les analogies entre $\mathbb{Z}$ et $K[X]$:

Analogie	$\mathbb{Z}$	$K[X]$
idéaux	$n\mathbb{Z}$	(P)
nombre premier	p	P_{irr}
idéal maximal	$p\mathbb{Z}$	(P_{irr})
corps	$\mathbb{Z}/p\mathbb{Z}$	$K[X]/(P_{irr})$

Il est à noter que dans le nouveau corps $K[X]/(P)$, P n'est plus irréductible.
On a $P(\overline{X}) = 0$ donc $\overline{X}$ est racine de P

- ⁕ **Application : construction de $\mathbb{C}$: anneau quotient de $\mathbb{R}[X]$ par $(X^2 + 1)$**
  On a vu que l'anneau quotient $\mathbb{R}[X]/(X^2 + 1)$ s'identifie à l'ensemble des classes $(a \cdot \overline{X} + b)$ où $a, b \in \mathbb{R}$.
  Mais $X^2 + 1$ est de degré 2 et sans racine dans $\mathbb{R}$ donc il est irreductible dans $\mathbb{R}[X]/(X^2 + 1)$.
  L'anneau quotient $\mathbb{R}[X]/(X^2 + 1)$ est donc un corps.

  On a $\overline{aX + b} = \overline{a} \cdot \overline{X} + \overline{b} = a \cdot \overline{X} + b$ car la classe d'un réel est égal à lui-même.
  (si $P = a$ alors $P = a + 0 \cdot (X^2 + 1)$ donc $r = a = P$)
  L'addition et la multiplication sont données par :
  - $\overline{aX + b} + \overline{cX + d} = (a + b\overline{X}) + (c + d\overline{X}) = (a + c) + (b + d)\overline{X}$.

— $\overline{aX+b}\cdot\overline{cX+d} = (a+b\overline{X})\cdot(c+d\overline{X}) = (ac)+(ad+bc)\overline{X}+bd\overline{X^2} = (ac-bd)+(ad+bc)\overline{X}$ car $(\overline{X})^2 = -1$.

Si l'on pose $\overline{X} = i$, on a $i^2 = -1$ et les éléments de l'anneau quotient s'écrivent $ai + b$ avec $a, b \in \mathbb{R}$.
On reconnaît l'ensemble des complexes !
On obtient ainsi une nouvelle construction du corps $\mathbb{C}$, vu comme un anneau quotient de $\mathbb{R}[X]$ par l'idéal engendré par le polynôme $X^2 + 1$.

A noter que dans $\mathbb{C}$, $X^2 + 1$ n'est plus irréductible puisqu'il admet i comme racine.

⁕ **Construction de corps finis**
Soit $Q \in K[X]/(P_{irr})$ alors on a vu que $Q = a_0 + a_1 \cdot \overline{X} + ... + a_{n-1} \cdot \overline{X^{n-1}}$.

Tout élément de l'anneau quotient est donc entièrement défini, déterminé par ses coefficients. Si P est de degré n, on doit choisir n coefficients parmi les éléments de K.

Si K est un corps fini de cardinal q, cela nous donne q^n possibilités. Le corps $K[X]/(P_{irr})$ est alors fini et son cardinal égal à q^n.

Pour construire un corps fini, il suffit donc de quotienter par un polynôme irréductible un anneau de polynômes dans un corps K fini.

On connaît déjà une famille de corps finis. Ce sont les anneaux quotient de $\mathbb{Z}$, les $\mathbb{Z}/p\mathbb{Z}$ avec p premier.
On pourrait donc à partir d'eux construire de nouveaux corps finis, les $\mathbb{Z}/p\mathbb{Z}[X]/(P_{irr})$.
Ils seraient tous de cardinal la puissance d'un nombre premier. Mais en existe-t-il d'autres ?

Chapitre 4

Construction de corps finis

4.1 Construction de quelques corps par recherche intuitive

4.1.1 Corps fini à deux éléments $\mathbb{F}_2$

Recherche intuitive
Le plus petit corps comprend deux éléments, l'élément neutre pour l'addition (0) et l'élément neutre pour la multiplication (1).
On a $\mathbb{F}_2 = \{0, 1\}$.

Table d'addition
0 est neutre pour l'addition $\Rightarrow 0 + 1 = 1 + 0 = 1$ / $0 + 0 = 0$.
$1 + 1 \neq 1$ sinon $1 = 0$ ce qui est impossible donc $1 + 1 = 0$.

$+$	0	1
0	0	1
1	1	0

Table de multiplication
On a $0 \cdot 1 = 1 \cdot 0 = 0$ et $1 \cdot 1 = 1$ par définition de l'élément neutre de la multiplication.

$\cdot$	0	1
0	0	0
1	0	1

Le groupe des inversibles est $\mathbb{F}_2^* = \mathbb{F}_2 \setminus \{0\} = \{1\}$. Seul 1 est inversible, c'est son propre inverse.

A noter que l'on retrouve les mêmes tables que pour $\mathbb{Z}/2\mathbb{Z}$.

4.1.2 Corps fini à trois éléments $\mathbb{F}_3$

- $\mathbb{F}_3$ contient les deux éléments neutres 0 et 1 ainsi qu'un 3^{eme} élément x distinct de 0 et de 1. On a $\mathbb{F}_3 = \{0, 1, x\}$.
- $\mathbb{F}_3$ muni de l'addition est un groupe additif de cardinal 3. L'ordre additif de ses éléments est donc un diviseur de 3 soit 1 ou 3. Seul l'élément neutre de l'addition, 0, est d'ordre 1.
  1 et x sont donc d'ordre 3.
- Le groupe des inversibles est $\mathbb{F}_3^* = \mathbb{F}_3 \setminus \{0\} = \{0, 1\}$. Il est d'ordre 2 car l'ordre multiplicatif de chacun de ses éléments divise 2. Seul 1 est d'ordre 1 donc x est d'ordre 2. On a $x \cdot x = 1$ et $< x >= \mathbb{F}_3^*$.
  $\mathbb{F}_3^*$ est donc un groupe cyclique de générateur 2.

⁕ On a :
- $1+1 \neq 0$ sinon 1 serait d'ordre additif 2.
- $1+1 \neq 1$ sinon $1+1=1 \Rightarrow 1+1-1=0 \Rightarrow 1=0$ impossible.

donc $1+1=x$.

⁕ On a :
- $x+x \neq 0$ sinon x serait d'ordre additif 2.
- $x+x \neq x$ sinon $x=0$, ce qui est impossible.

donc $x+x=1$.

⁕ On a :
- $0 \cdot 0 = 1 \cdot 0 = x \cdot 0 = 0 \cdot x = 0$ car 0 est l'élément absorbant de la multiplication.
- $1 \cdot x = x \cdot 1 = 1$ par définition de l'élément neutre de la multiplication.

Cela nous donne les tables suivantes :

Table d'addition

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

Table de multiplication

$\cdot$	0	1	x
0	0	0	0
1	0	1	x
x	0	x	1

$\mathbb{F}_3$ est donc un corps commutatif. On retrouve les mêmes tables que pour $\mathbb{Z}/3\mathbb{Z}$ en prenant $x=2$.

4.1.3 Corps fini à quatre éléments $\mathbb{F}_4$

⁕ $\mathbb{F}_4$ contient les deux éléments neutres 0 et 1, un troisième élément x distinct de 0 et 1 et un quatrième élément y distinct de 0, 1 et x.

⁕ $\mathbb{F}_4$ muni de l'addition est un groupe additif de cardinal 4. L'ordre additif de ses éléments est donc un diviseur de 4 soient 1, 2 ou 4. Seul l'élément neutre de l'addition 0 est d'ordre 1.
1, x et y sont donc d'ordre 2 ou 4.
- supposons que $ord(1)=4$ alors $4 \cdot 1 = 1+1+1+1 = 0$.
  Mais $1+1+1+1 = (1+1)\cdot(1+1) = (2\cdot 1)\cdot(2\cdot 1) = 0$ donc par intégrité de K on aurait $2 \cdot 1 = 0$ ce qui contredit la minimalité de 4 donc $ord(1)=2$.
- on a $x+x = 1\cdot x + 1 \cdot x = (1+1)\cdot x = 0$ car 1 est d'ordre additif 2 $\Rightarrow x+x=0$ et x est aussi d'ordre additif 2.
  Ce raisonnement est aussi valable pour le $4^{\text{ième}}$ élément y qui est donc aussi d'ordre 2.

⁕ Par **stabilité additive**, $\mathbb{F}_4$ contient les multiples de ces éléments mais comme l'ordre additif est 2, les multiples possibles pour chaque élément ne peuvent être que 0 ou l'élément lui-même.
En effet :

$$\begin{aligned}(2k)x &= \underbrace{x+x+x+...+x}_{2k\times} \\ &= k(2x) = \underbrace{2x+2x+...+2x}_{k\times} \\ &= \underbrace{0+0+...+0}_{k\times} \\ &= 0\end{aligned}$$

De même, on montre que $(2k+1)x = (2k)x + 1 \cdot x = 0 + x$.
Les multiples n'apportent donc pas d'élément supplémentaire.

⁕ Par stabilité additive, $\mathbb{F}_4$ contient les sommes de ces éléments entre eux soit $0+1 = 1$, $0+x = x$ et $1+x$.
$1+x$ distinct de 0 sinon $1+x = 0 \Rightarrow 1+1+x = 1+0 \Rightarrow 0+x = 1 \Rightarrow x = 1$ impossible.
$1+x$ distinct de 1 sinon $1+x = 1 \Rightarrow x = 0$ impossible.
Donc $1+x$ est le quatrième élément de $\mathbb{F}_4$.
On vérifie que la caractéristique de $\mathbb{F}_4$ étant de 2, les autres sommes n'apportent pas d'élément supplémentaire.

Si $\mathbb{F}_4$ existe alors $\mathbb{F}_4 = \{0, 1, x, 1+x\}$.

⁕ $\mathbb{F}_4^* = \{1, x, 1+x\}$ donc l'ordre multiplicatif de x et $1+x$ est un diviseur de 3 différent de 1 donc c'est 3.

⁕ Par **stabilité multiplicative**, $\mathbb{F}_4$ contient les puissances de ses éléments.
Mais pour tout n, $0^n = 0$ et $1^n = 1$.
$\mathbb{F}_4$ contient x^2.
$\Rightarrow x^2 \neq 0$ sinon par intégrité $x \cdot x = 0 \Rightarrow x = 0$.
$\Rightarrow x^2 \neq 1$ sinon $x^2 = 1 \Rightarrow x^3 = x \Rightarrow 1 = x$ car les éléments de $\mathbb{F}_4^*$ sont d'ordre 3.
$\Rightarrow$ par élimination, $x^2 = x + 1$.

Si F_4 existe alors $\mathbb{F}_4 = \{0, 1, x, 1+x\}$ avec $1 + x = x^2$.

On remarque que $\mathbb{F}_4^* = \{1, x, x^2\}$ est un groupe *cyclique* de générateur x.
Les autres puissances des éléments de $\mathbb{F}_4^*$ et leurs produits n'apporteront donc pas d'éléments supplémentaires.

Le corps à 4 éléments $\mathbb{F}_4$ existe donc.

⁕ On a :
- $(1+x) + x = 1 + 2x = 1 + 0 = 1$.
- $(1+x) + 1 = 2 \cdot 1 + x = 0 + x = x$.
- $(1+x) + (1+x) = 2 \cdot 1 + 2x = 0 + 0 = 0$.

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

Cela nous donne les tables suivantes :

Table d'addition

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

Table de multiplication

$\cdot$	0	1	x	$1+x$
0	0	0	0	0
1	0	1	x	$1+x$
x	0	x	$1+x$	1
$1+x$	0	$1+x$	1	x

4.1.4 Tentative de construction du corps fini à six éléments $\mathbb{F}_6$

⁕ $\mathbb{F}_6$ muni de l'addition est un groupe additif de cardinal 6. L'ordre additif de 1 est donc un diviseur de 6 soit 1, 2, 3 ou 6.
A noter que comme on l'a vu précédemment, tous les éléments non nuls de $\mathbb{F}_6$ auront le même ordre que 1.
On a $ord(1) \neq 1$ sinon $1 = 0$.

⁕ Supposons que $ord(1) = 6$ alors $6 \cdot 1 = 0$.
Mais $6 \cdot 1 = (2 \cdot 1) \cdot (3 \cdot 1) \Rightarrow$ par intégrité de K on aurait $2 \cdot 1 = 0$ ou $3 \cdot 1 = 0$ ce qui contredirait la minimalité de 6.

⁕ Supposons que $ord(1) = 2$
$\mathbb{F}_6$ contient alors 0, 1 et un troisième élément x distinct de 0 et 1. Par stabilité additive, il contient aussi $1 + x$. On a :

— $1 + x \neq 0$ sinon $1 + x = 0 \Rightarrow 1 + 1 + x = 1 + 0 \Rightarrow 2 \cdot 1 + x = 1 \Rightarrow 0 + x = 1 \Rightarrow x = 1$ (impossible).

— $1 + x \neq 1$ sinon $1 + x = 1 \Rightarrow x = 0$ (impossible).

— $1 + x \neq x$ sinon $1 + x = x \Rightarrow 1 = 0$ (impossible).

donc $1 + x$ est le quatrième élément de $\mathbb{F}_6$.

Comme tous les éléments non nuls sont d'ordre additif 2 alors les combinaison linéaires de 0, 1, x et $1 + x$ n'apportent pas d'éléments supplémentaires.
Il existe donc un $5^{\text{ème}}$ élément y distinct.

Par stabilité additive, $\mathbb{F}_6$ contient $1+y$ et on montre que $1+y$ est distinct des autres éléments :

— $1 + y \neq 0$ sinon $1 + y = 0 \Rightarrow 1 + 1 + y = 1 \Rightarrow 0 + y = 1 \Rightarrow y = 1$ (impossible).

— $1 + y \neq 1$ sinon $1 + y = 1 \Rightarrow y = 0$ (impossible).

— $1 + y \neq x$ sinon $1 + y = x \Rightarrow y = 1 + x$ (impossible).

— $1 + y \neq y$ sinon $1 + y = y \Rightarrow 1 = 0$ (impossible).

donc $\mathbb{F}_6 = \{0, 1, x, 1 + x, y, 1 + y\}$.

Mais par stabilité additive, $\mathbb{F}_6$ contient $x + y$. Or, on a :

— $x + y \neq 0$ sinon $x + y = 0 \Rightarrow x + y = 2x = 0$ car $ord(x) = 0 \Rightarrow y = x$ (impossible).

— $x + y \neq 1$ sinon $x + y = 1 \Rightarrow y = 1 + x$ (impossible).

— $x + y \neq x$ sinon $x + y = x \Rightarrow y = 0$ (impossible).

— $x + y \neq y$ sinon $x + y = y \Rightarrow x = 0$ (impossible).

— $x + y \neq 1 + x$ sinon $x + y = 1 + x \Rightarrow y = 1$ (impossible).

— $x + y \neq 1 + y$ sinon $x + y = 1 + y \Rightarrow x = 1$ (impossible).

$\mathbb{F}_6$ contiendrait un $7^{\text{ème}}$ élément ce qui est impossible donc $ord(1) \neq 2$.

⁕ Supposons que $ord(1) = 3$
$\mathbb{F}_6$ contient 0, 1, 2 car 2 distinct de 1 et 0 car $2 = 1 \Rightarrow 1 = 0$ et $2 = 0$ contredit la minimalité de l'ordre de 1.
$\mathbb{F}_6$ contient un quatrième élément x distinct de 0,1 et 2.
Par stabilité additive, $\mathbb{F}_6$ contient $x + 1$ et $x + 2$ qui sont distincts des autres éléments de $\mathbb{F}_6$.
On a :

— $1 + x \neq 1$ sinon $1 + x = 1 \Rightarrow x = 0$ (impossible).
— $1 + x \neq 2$ sinon $1 + x = 2 \Rightarrow x = 1$ (impossible).
— $1 + x \neq x$ sinon $1 + x = x \Rightarrow 1 = 0$ (impossible).
— $1+x \neq 0$ sinon $1+x = 0 \Rightarrow 2+1+x = 2 \Rightarrow 3+x = 2 \Rightarrow 0+x = 2 \Rightarrow x = 2$ (impossible).

On a :

— $2 + x \neq 0$ sinon $2 + x = 0 \Rightarrow 1 + 2 + x = 1 + 0 \Rightarrow x = 1$ (impossible).
— $2 + x \neq 1$ sinon $2 + x = 1 \Rightarrow 1 + 2 + x = 1 + 1 \Rightarrow x = 2$ (impossible).
— $2 + x \neq 2$ sinon $2 + x = 2 \Rightarrow 1 + 2 + x = 1 + 2 \Rightarrow x = 0$ (impossible).
— $2 + x \neq x$ sinon $2 + x = x \Rightarrow 2 = 0$ (impossible).

donc $F_6 = \{0, 1, 2, x, 1 + x, 2 + x\ \}$.

Mais par stabilité additive, $\mathbb{F}_6$ contient $2x$. Or, on a :

— $2x \neq 0$ sinon $x + x = 0$ ce qui contredirait la minimalité de l'ordre additif de x égale à 3.
— $2x \neq 2$ sinon $2x = 2 \Rightarrow 2(x-1) = 0 \Rightarrow x-1 = 0$ par intégrité de $K \Rightarrow x = 1$ (impossible).
— $2x \neq x$ sinon $2x = x \Rightarrow x = 0$ (impossible).
— $2x \neq 1$ sinon $2x = 1 \Rightarrow 3x = x + 1 \Rightarrow 0 = x + 1 \Rightarrow 2 = x + 1 + 2 \Rightarrow x = 2$ (impossible).
— $2x \neq x + 1$ sinon $2x = x + 1 \Rightarrow x = 1$ (impossible).
— $2x \neq x + 2$ sinon $2x = x + 2 \Rightarrow x = 2$ (impossible).

$\mathbb{F}_6$ contiendrait un $7^{\text{ème}}$ élément ce qui est impossible donc $ord(1) \neq 3$.

⁕ *on a montré que l'ordre additif de 1 ne peut être égal à un diviseur de 6, ce qui impossible* donc le corps à 6 éléments $\mathbb{F}_6$ n'existe pas.

Il n'existe donc pas de corps fini de cardinal n pour tout $n \in \mathbb{N}^*$.

4.2 Cardinal et construction d'un corps fini / Propriétés d'un corps fini

4.2.1 Caractéristique d'un corps

On a vu lors de la recherche intuitive de corps que l'ordre additif de l'unité joue un rôle important dans la construction d'un corps.
On a aussi vu que cet ordre additif est le même pour tous les éléments non nuls du corps. On l'appelle la caractéristique du corps.

Définition 17. Soit K un corps fini. On appelle **caractéristique du corps** K le plus petit entier positif non nul vérifiant $n \cdot 1_K = 1_K + 1_K + ... + 1_K = 0_K$ (additionné n fois).
C'est l'ordre additif de 1 et aussi celui de tous les éléments non nuls de K.

Exemple 22. le corps $\mathbb{Z}/p\mathbb{Z}$ a une caractéristique égale à p.

Propriété : la caractéristique d'un corps fini p est forcément un nombre premier.

Démonstration.
Si p n'est pas premier alors il existe $i, j \in \mathbb{N}^*$ tel que $p = i \cdot j$.
Mais alors $p \cdot 1 = 0 \Rightarrow (i \cdot j) \cdot 1 = (i \cdot 1) \cdot (j \cdot 1) = 0 \Rightarrow$ par intégrité du corps K, on a $i \cdot 1 = 0$ ou $j \cdot 1 = 0$, ce qui contredit la minimalité de p donc p est premier. □

4.2.2 Sous-corps premier

On vient de voir qu'il n'existe pas de corps fini de toutes les tailles.
Avant de déterminer l'expression générale du cardinal d'un corps fini, il faut d'abord introduire les notions de corps premiers et de caractéristique.

Définition 18. Un corps est dit **premier** s'il n'a pas de sous-corps autre que lui-même.

Exemple 23. Les $\mathbb{Z}/p\mathbb{Z}$ avec p premier sont des corps premiers finis.
Un sous-corps L est un sous-groupe additif de $\mathbb{Z}/p\mathbb{Z}$. Par le théorème de Lagrange, son cardinal est donc un diviseur du cardinal de $\mathbb{Z}/p\mathbb{Z}$ donc un diviseur de p. Mais p étant premier, ses seuls diviseurs sont 1 et lui-même. Donc L peut avoir pour cardinal 1 ou p. Le seul sous-groupe additif de $\mathbb{Z}/p\mathbb{Z}$ est $\{e\}$ qui n'est pas lui-même un corps. Donc $\mathbb{Z}/p\mathbb{Z}$ n'a pas de sous-corps autre que lui-même.

Définition 19. On appelle **sous-corps premier de** K le plus petit sous-corps L qu'il peut contenir, soit l'intersection de tous les sous-corps de K.

Propriété : K est un espace vectoriel sur son sous-corps premier L muni de l'addition dans K et de la multiplication qui à $k \in K$, $\lambda \in L$ associe $\lambda \cdot k \in K$.

Démonstration.
$(K, +)$ est un groupe additif car K est un corps.
La multiplication est bien définie : soit $k \in K$ et $\lambda \in L$ alors $\lambda \in K \Rightarrow \lambda \cdot k \in K$ par stabilité multiplicative de K. Elle vérifie les lois d'un espace vectoriel car elle vérifie les lois du corps K. □

4.2.3 Cardinal d'un corps

Soit K un corps fini de caractéristique k. On montre qu'il existe une bijection entre le sous-corps premier L de K et le corps premier $\mathbb{Z}/p\mathbb{Z}$.

Conséquence : $\text{Card}(L) = \text{Card}(\mathbb{Z}/p\mathbb{Z}) = p$.

Théorème 13. Soit K un corps fini de caractéristique p. Alors il existe $n \in \mathbb{N}$ tel que $\text{Card}(K) = p^n$.

Démonstration.
K étant un espace vectoriel et possédant un nombre fini d'éléments, il possède une dimension finie n. Soit $B = (e_1, e_2, ..., e_n)$ une base de K. Tout élément de K peut donc s'écrire sous la forme d'une unique combinaison linéaire de cette famille de vecteurs de K.
Soit $k \in K$. Alors il existe $\lambda_1, \lambda_2, ..., \lambda_n \in L$ tels que $k = \lambda_1 \cdot e_1 + \lambda_2 \cdot e_2 + ... + \lambda_n \cdot e_n$.
k est entièrement déterminé par le choix de ces n coordonnées dans B. Pour chaque λ_i, il y a p possibilités parmi les éléments de L ce qui nous donne au total p^n possibilités pour k. □

Le cardinal d'un corps K fini ne peut donc être égal qu'à la puissance d'un nombre premier.
Cela explique pourquoi il n'existe pas de corps à 6 éléments.

4.2.4 Unicité et existence des corps finis

On a montré au chapitre 3 que les familles de corps obtenues par le quotient de l'anneau de polynômes à coefficients dans $\mathbb{Z}/p\mathbb{Z}[X]$ par un polynôme irréductible de degré n donnent des corps finis de cardinal p^n. Mais toute puissance d'un nombre premier est-elle le cardinal d'un corps ? Et si oui, existe-t-il plusieurs corps de même cardinal ?

On a vu lors de la construction d'un corps à trois éléments que les tables de Cayley de $\mathbb{F}_3$ et de $\mathbb{Z}/3\mathbb{Z}$ étaient ainsi similaires en remplaçant l'élément x par 2.
On peut élargir cette constatation entre tout corps K de cardinal p^n et un corps $\mathbb{Z}/p\mathbb{Z}[X]/(P)$ avec P irréductible de degré n.

Regardons d'abord la question des liens entre des corps de même cardinal.

Théorème 14. Soit K un corps fini de cardinal p^n. Il existe un polynôme irréductible P de degré n tel que K et $\mathbb{Z}/p\mathbb{Z}[X]/(P)$ soient isomorphes.

Démonstration.
La preuve de ce théorème est accessible à des gymnasiens mais nécessite de connaître les notions de morphisme et d'isomorphisme qui n'ont été délibérément pas développées dans ce cours faute de place. Un isomorphisme est une bijection entre deux structures qui conserve les propriétés algébriques. C'est une relation très forte, quasiment une égalité entre ces deux ensembles. C'est pourquoi on parle d'unicité à un isomorphisme près. □

Ce théorème souligne le rôle clé des familles d'anneaux $\mathbb{Z}/p\mathbb{Z}[X]$. Pour construire un corps fini de cardinal p^n, on n'a donc besoin "que" d'un polynôme de degré n irréductible sur $\mathbb{Z}/p\mathbb{Z}[X]$.
La question de l'existence de corps finis de cardinal p^n est finalement équivalente à celle de l'existence de polynômes irréductibles de degré n dans $\mathbb{Z}/p\mathbb{Z}[X]$.

Théorème 15. Soit p, premier. Alors pour tout $n \in \mathbb{N}^*$, il existe un polynôme irréductible de degré n dans $\mathbb{Z}/p\mathbb{Z}[X]$-

Démonstration.
Les preuves de cette existence sont particulièrement complexes pour un gymnasien. Elles nécessitent de comprendre en plus des isomorphismes des notions telles que les corps de rupture, les éléments algébriques ... □

On vérifie enfin que si P et Q sont deux polynômes irréductibles de degré n dans $\mathbb{Z}/p\mathbb{Z}[X]$ alors les corps $\mathbb{Z}/p\mathbb{Z}[X]/(P)$ et $\mathbb{Z}/p\mathbb{Z}[X]/(Q)$ sont isomorphes.

Il existe donc un corps de cardinal la puissance d'un nombre premier et il est unique à "un isomorphisme près".

4.2.5 Principes de construction

Les $\mathbb{Z}/p\mathbb{Z}[X]$ suffisent donc à construire des corps de tout cardinal.

Soit K un corps fini de cardinal p^n.
1er cas : $n = 1$ alors $\mathrm{Card}(K) = p$.
Il suffit de prendre $K = \mathbb{Z}/p\mathbb{Z}$. On obtient les corps premiers.
Les autres corps de cardinal p sont isomorphes à $\mathbb{Z}/p\mathbb{Z}$.

Exemple : $p = 3 \Rightarrow K = \mathbb{Z}/3\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}\}$.

$2^{\text{ème}}$ cas : $n > 1$ alors $\text{Card}(K) = p^n$.

- on prend le corps $\mathbb{Z}/p\mathbb{Z}[X]$ des polynômes à coefficients dans $\mathbb{Z}/p\mathbb{Z}$.
- on choisit un polynôme irréductible P de $\mathbb{Z}/p\mathbb{Z}[X]$ de degré n.
  Soit $I = (P) = \{Q \in \mathbb{Z}/p\mathbb{Z}[X] \mid \exists\ D \in \mathbb{Z}/p\mathbb{Z}[X] \mid Q = D \cdot P\}$
  l'idéal engendré par le polynôme P.
- on quotiente $\mathbb{Z}/p\mathbb{Z}[X]$ par I.

$\Rightarrow$ on a $K = \mathbb{Z}/p\mathbb{Z}[X]/(P)$.

Pour p donné, en faisant varier le degré de n, on fait varier la puissance n.

4.2.6 Double représentation

(a) Représentation polynomiale
Tous les éléments de K peuvent s'écrire sous la forme de combinaisons linéaires des puissances de X.
Soit $k \in K$. Alors il existe un n-uplet d'éléments de K $(a_0, a_1, ..., a_{n-1})$ tel que $k = a_0 \cdot 1 + a_1 \cdot X + ... + a_{n-1} \cdot X^{n-1}$.
$k = \sum_{i=0}^{n-1} (a_i \cdot (X)^i)$.
Cette notation polynômiale est pratique pour l'addition.

(b) Représentation sous forme de puissance d'un élément de K
Mais il existe une autre propriété remarquable du groupe des inversibles que l'on a déjà contasté lors de la construction intuitive de $\mathbb{F}_3$ et $\mathbb{F}_4$, la cyclicité.

Pour démontrer cette propriété, on admettra le résultat suivant : soit $n \in \mathbb{N}^*$. Alors $\sum_{d/n} (\phi(d)) = n$

Exemple 24. Soit $n = 4$. Ses diviseurs sont 1, 2 et 4.
Si ϕ est l'indicatrice d'Euler alors $\phi(1) = 1$, $\phi(2) = \text{Card}(\{1\}) = 1$, $\phi(4) = \text{Card}(\{1, 2\}) = 2$.
On a bien $\sum_{d/n} (\phi(d)) = \phi(1) + \phi(2) + \phi(4) = 1 + 1 + 2 = 4$.

Théorème 16. Le groupe multiplicatif des éléments inversibles d'un corps fini K est cyclique.

Démonstration.
Soit $n = \text{Card}(K^*)$.

- Soit $P = X^d - 1 \in K[X]$. Comme K est un corps donc un anneau intègre, P de degré d admet au plus d racines dans K.
  Soit N_d l'ensemble des éléments de K^* d'ordre (multiplicatif) d dans K^*.
  Soit N_d est un ensemble vide, soit N_d contient au moins un élément x. Mais alors x engendre un sous-groupe cyclique H_d de K_{inv} qui contient donc d éléments, chacun vérifiant $x^d = 1$ (cf. théorème du chapitre des groupes cycliques).
  $\Rightarrow$ Les racines de P sont donc toutes inclues dans ce sous-groupe.
- Si y est un élément d'ordre $d \Rightarrow y$ est une racine de $P \Rightarrow y \subset H_d$.
  H_d contient tous les éléments d'ordre d de K^*.
- Or, on connaît le nombre de ces éléments. Il s'agit du nombre de générateurs de H_d qui est égal à $\phi(d)$.
  On vient de montrer que $\text{Card}(N_d) = 0$ ou $\text{Card}(N_d) = \phi(d)$.

La relation "avoir le même ordre" est une relation d'équivalence dans K_{inv} donc elle établit une partition de cet ensemble. On a $Card(K^*)$ = somme des cardinaux des classes d'équivalences.
Les classes d'équivalences sont composées des éléments qui ont le même ordre. Les ordres possibles étant les diviseurs de n, le nombre de classes est égal au plus au nombre de diviseurs de n.
On a donc $n = \sum_{d|n}(\text{Card}(N_d)) \leq \sum_{d|n} \phi(d)$.
Mais on a vu que $\sum_{d|n} \phi(d) = n$ (cf. théorème) d'où $\sum_{d|n} \phi(d) \leq \sum_{d|n}(\text{Card}(N_d)) \leq \sum_{d|n} \phi(d)$.
Donc $\text{Card}(N_d) = \phi(d) > 0$ pour tout d. Aucun N_d n'est vide.
En particulier, N_n n'est pas vide donc N_n possède au moins un élément d'ordre n et donc au moins un générateur. Il est cyclique. □

K^* est cyclique donc il possède au moins un générateur g. On a $K^* =< g >= \{1, g, g^2, ..., g^{n-2}\}$.
On a $K = \{0\} \cup K^* = \{0, 1, g, g^2, ..., g^{n-2}\}$.
On peut définir tout élément non nul de K comme une puissance d'un générateur du groupe des inversibles $K^* = K \setminus \{0\}$.
Cette notation est pratique pour la multiplication ou bien pour le calcul d'un inverse.

4.3 Application : construction de $\mathbb{F}_8$

4.3.1 Existence de $\mathbb{F}_8$

- ⁕ On veut que $\text{Card}(K) = 8$.
  Si l'on décompose 8 en facteurs de nombres premiers, on obtient $8 = 2^3$.
  Cette décomposition est unique.
  C'est une puissance d'un nombre premier 2 donc K existe.
- ⁕ Le cardinal de K s'écrit donc sous la forme p^n avec $p = 2$ et $n = 3$.
  p nous donne la caractéristique de K qui est égale à 2.

Avertissement : par commodité, pour alléger les notations, nous n'utiliserons plus les barres qui indiquent les classes pour les éléments de $\mathbb{Z}/2\mathbb{Z}$. Ainsi, on notera 0 et 1 pour respectivement $\overline{0}$ et $\overline{1}$.

4.3.2 Recherche des polynômes irréductibles de degré 3 dans $\mathbb{Z}/2\mathbb{Z}[X]$

- ⁕ On a $\mathbb{Z}/2\mathbb{Z} = \{0, 1\}$.
  Un polynôme de degré 3 possède 4 coefficients.
  - pour le choix des coefficients des termes en X^0, X^1 et X^2 il y a deux possibilités.
  - pour le choix du coefficient du terme en X^3 il n'y a qu'une possibilité (0 doit être éliminé).

  Cela fait donc au total $2 \cdot 2 \cdot 2 \cdot 1 = 8$ possibilités.
- ⁕ Parmi ces 8 polynômes de degré 3, nous devons trouver ceux qui sont irréductibles.
  On a vu que cela revient à trouver ceux qui n'ont pas de racines dans $\mathbb{Z}/2\mathbb{Z}$.
  Pour chaque polynôme P de degré 3, on calcule donc sa valeur polynomiale en 0 et 1.
  - si l'une de ces valeurs est égale à 0 alors P admet au moins une racine dans $\mathbb{Z}/2\mathbb{Z}$ et P n'est pas irréductible.
  - si aucune de ces valeurs n'est égale à 0 alors P est irréductible.

  Exemple 1 : $Q = X^3 + X^2 + X$.
  $Q(0) = 0 \Rightarrow 0$ est racine de Q donc Q n'est pas irréductible.
  Exemple 2 : $P = X^3 + X^2 + 1$.
  On a $P(1) = 1 + 1 + 1 = 1 \neq 0$ et $P(0) = 0 + 0 + 1 = 1 \neq 0$.

P n'a pas de racines dans $\mathbb{Z}/2\mathbb{Z}$ donc P est irréductible.

Au total on a 2 polynômes irréductibles de degré 3 :
- X^3+X^2+X+1 (réductible car 1 est racine).
- X^3+X^2+X (réductible car 0 est racine).
- X^3+X+1 (**irréductible**).
- X^3+X (réductible car 0 est racine).
- X^3+1 (réductible car 1 est racine).
- X^3+X^2+1 (**irréductible**).
- X^3+X^2 (réductible car 0 et 1 sont racines).

On choisit X^3+X+1 qui ne comporte pas de terme au carré pour simplifier les calculs des tables d'addition et de multiplication.
A noter que comme dans $\mathbb{Z}/2\mathbb{Z}$ on a $1=-1$ alors $X^3+X+1=0 \Rightarrow X^3=X+1$.

4.3.3 Définition de $K=\mathbb{F}_8$

On peut définir $\mathbb{F}_8$ comme l'anneau quotient du corps des polynômes $\mathbb{Z}/2\mathbb{Z}[X]$ par l'idéal engendré par le polynôme irréductible X^3+X+1.
$\Rightarrow \mathbb{F}_8=\mathbb{Z}/2\mathbb{Z}[X]/(X^3+X+1)$.

Pour rappel, l'idéal engendré par X^3+X+1 est l'ensemble des polynômes à coefficients dans $\mathbb{Z}/2\mathbb{Z}$ qui sont ses multiples.
On le note $I=(X^3+X+1)=\{P\in\mathbb{Z}/2\mathbb{Z}[X] \mid \exists\, Q\in\mathbb{Z}/2\mathbb{Z}[X] \text{ avec } P=Q\cdot(X^3+X+1)\}$.
Par exemple X^4+X^2+X est dans I car il peut s'écrire sous la forme $X^4+X^2+X=(X^3+X+1)\cdot X$.
Ici $Q=X$.

Soit $P\in\mathbb{Z}/2\mathbb{Z}[X]$. Alors comme cet anneau est euclidien, il existe un unique couple (Q,R) d'éléments de $\mathbb{Z}/2\mathbb{Z}[X]$ tel que $P=Q\cdot(X^3+X+1)+R$ avec $\deg(R)<\deg(X^3+X+1)=3$.
La classe de P dans $\mathbb{F}_8$ est égale à celle de R.
Le corps K est l'ensemble des classes des restes de la division euclidienne des polynômes de $\mathbb{Z}/2\mathbb{Z}[X]$ par (X^3+X+1).

4.3.4 Recherche des éléments de $K=\mathbb{F}_8$

- On a vu que tout élément de $\mathbb{F}_8$ a une représentation sous la forme d'un polynôme de α de degré inférieur ou égal à 2 et à coefficients dans $\mathbb{Z}/2\mathbb{Z}$.

  $\Rightarrow \mathbb{F}_8=\mathbb{Z}/2\mathbb{Z}[\overline{X}]=\{P(\overline{X}),\ P\in\mathbb{Z}/2\mathbb{Z}[X] \text{ et } \deg(P)<3\}$.

  Un élément de $\mathbb{F}_8$ est entièrement déterminé par ses 3 coefficients. Pour chaque a_i, on a deux possibilités à savoir 0 ou 1. Cela nous donc $2\cdot2\cdot2=8$ éléments possibles. On retrouve le cardinal de K.

  Si on pose $\alpha=\overline{X}$, alors :
  $\mathbb{F}_8=\{a\cdot1+b\alpha+c\cdot\alpha^2\,;\ a,b,c\in\mathbb{Z}/2\mathbb{Z} \text{ avec } \alpha^3+\alpha+1=0\}$.
- Liste des éléments de $\mathbb{F}_8$:
  $\mathbb{F}_8=\{0,1,\alpha,1+\alpha,\alpha^2,\alpha^2+1,\alpha^2+\alpha,\alpha^2+\alpha+1\}$.

4.3.5 Double représentation des éléments de $\mathbb{F}_8$

⁕ On vient de voir que tout élément de $\mathbb{F}_8$ a une représentation sous la forme d'un polynôme de α de degré inférieur ou égal à 2 et à coefficients dans $\mathbb{Z}/2\mathbb{Z}$.

⁕ Mais si on trouve un générateur du groupe cyclique des inversibles de $\mathbb{F}_8$, à savoir $\mathbb{F}_8^*$ alors on disposera d'une autre représentation des éléments de $\mathbb{F}_8$.
Pour trouver un générateur de $\mathbb{F}_8^*$ il faut trouver un élément qui soit d'ordre 7.
Les autres ordres possibles pour les éléments de $\mathbb{F}_8^*$ sont les diviseurs de 7 à savoir 1 et 7.
A part 1, tous les éléments de $\mathbb{F}_8^*$ sont d'ordre 7 et sont donc des générateurs.
Choisissons $\alpha = \overline{X}$ comme *générateur* de $\mathbb{F}_8^*$.

⁕ On peut donc les éléments non nuls de K^* commes des *puissances* de α.
On a $\mathbb{F}_8 = \mathbb{F}_8^* \cup \{0\} = \{0, 1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6\}$.

4.3.6 Problème du logarithme discret

⁕ On dispose donc de 2 représentations des éléments de $\mathbb{F}_8^*$:

— une représentation polynômiale.

— une représentation avec les puissances de α.

Il serait intéressant d'établir une correspondance entre ces deux notations. On dit que l'on cherche à résoudre *le problème du logarithme discret de base α dans K^**.
Pour tout élément de K^* qui s'écrit sous la forme $a+b\alpha+c\alpha^2$, il existe i tel que $a+b\alpha+c\alpha^2 = \alpha^i$ avec $0 \leqslant i \leqslant 6$:

Dans notre cas présent, on peut calculer les puissances de α en tenant compte du fait que α est racine de $X^3 + X + 1$ dans F_8 donc $\alpha^3 + \alpha + 1 = 0$. Nous avons alors :
$\alpha = \alpha$;
$\alpha^2 = \alpha^2$;
$\alpha^3 = -\alpha - 1 = \alpha + 1$; car $-1 = 1$ modulo 2 ;
$\alpha^4 = \alpha \cdot \alpha^3 = \alpha \cdot (\alpha + 1) = \alpha^2 + \alpha$;
$\alpha^5 = \alpha \cdot \alpha^4 = \alpha \cdot (\alpha^2 + \alpha) = \alpha^3 + \alpha^2 = \alpha^2 + \alpha + 1$;
$\alpha^6 = \alpha \cdot \alpha^5 = \alpha \cdot (\alpha^2 + \alpha + 1) = \alpha^3 + \alpha^2 + \alpha = \alpha + 1 + \alpha^2 + \alpha = \alpha^2 + 2\alpha + 1 = \alpha^2 + 1$;
$\alpha^7 = \alpha \cdot \alpha^6 = \alpha \cdot (\alpha^2 + 1) = \alpha^3 + \alpha = \alpha + 1 + \alpha = 2\alpha + 1 = 1$.
α est bien d'ordre 7.
Voici le tableau de correspondance entre ces 2 notations :

puissances de α	1	α	α^2	α^3	α^4	α^5	α^6
notation polynomiale	1	α	α^2	$1+\alpha$	$\alpha+\alpha^2$	$1+\alpha+\alpha^2$	$1+\alpha^2$

⁕ Selon le type d'opérations que l'on souhaite pratiquer dans $\mathbb{F}_8$, on peut choisir l'une ou l'autre de ces représentations.

— la notation en polynômes est pratique pour l'addition.

— la notation en puissances de α est pratique pour les multiplications ou pour trouver l'inverse de chaque élément de $\mathbb{F}_8^*$. On a ainsi $(\alpha^p)^{-1} = \alpha^{7-p}$.

puissances de α	1	α	α^2	α^3	α^4	α^5	α^6
inverse en puissances de α	1	α^6	α^5	α^4	α^3	α^2	α
inverse en polynômes de α	1	$1+\alpha^2$	$1+\alpha+\alpha^2$	$\alpha+\alpha^2$	$1+\alpha$	α^2	α

4.3.7 Tables d'addition et de multiplication

4.3.7.1 Table d'addition

Pour établir la table d'addition, on utilise la notation polynomiale.
On ajoute les coefficients obtenus en tenant compte de l'ordre additif de $\mathbb{Z}/2\mathbb{Z}$ qui est de 2 pour simplifier les calculs.
On utilise la commutativité de l'addition dans $\mathbb{F}_8$ pour effectuer moins de calculs.

On obtient la table d'addition suivante :

$+$	0	1	α	$1+\alpha$	α^2	$\alpha+\alpha^2$	$1+\alpha^2$	$1+\alpha+\alpha^2$
0	0	1	α	$1+\alpha$	α^2	$\alpha+\alpha^2$	$1+\alpha^2$	$1+\alpha+\alpha^2$
1	1	0	$1+\alpha$	α	$1+\alpha^2$	$1+\alpha+\alpha^2$	α^2	$\alpha+\alpha^2$
α	α	$1+\alpha$	0	1	$\alpha+\alpha^2$	α^2	$1+\alpha+\alpha^2$	$1+\alpha^2$
$1+\alpha$	$1+\alpha$	α	1	0	$1+\alpha+\alpha^2$	$1+\alpha^2$	$\alpha+\alpha^2$	α^2
α^2	α^2	$1+\alpha^2$	$\alpha+\alpha^2$	$1+\alpha+\alpha^2$	0	α	1	$1+\alpha$
$1+\alpha^2$	$1+\alpha^2$	α^2	$1+\alpha+\alpha^2$	$\alpha+\alpha^2$	1	$1+\alpha$	0	α
$1+\alpha+\alpha^2$	$1+\alpha+\alpha^2$	$\alpha+\alpha^2$	$1+\alpha^2$	α^2	$1+\alpha$	1	α	0

$(\mathbb{F}_8, +)$ étant un groupe additif, on vérifie bien qu'un élément de F_8 ne figure qu'une et seule fois par ligne et par colonne.
On peut aussi vérifier que l'addition est associative.

4.3.7.2 Table de multiplication

Pour établir la table de multiplication, on utilise la table de correspondance entre notation polynômiale et représentation par puissance de α.

- on "convertit" chaque élément de k en puissance de α.
- on effectue la multiplication en additionnant les puissances de α.
  Si l'on obtient une puissance de α supérieure ou égale à son ordre multiplicatif (7), on peut "réduire" cette puissance en utilisant la propriété suivante vérifiée par α :
  $\alpha^n = \alpha^7 \cdot \alpha^{n-7} = \alpha^{n-7}$ pour tout $n \leqslant 7$ car $\alpha^7 = 1$.
- on "reconvertit" à partir du tableau de correspondance la puissance de α en notation polynômiale.

exemple 1 : $(1+\alpha)\cdot(\alpha+\alpha^2) = \alpha^3 \cdot \alpha^4 = \alpha^7 = 1$.
exemple 2 : $(\alpha^2+\alpha+1)\cdot(1+\alpha^2) = \alpha^5 \cdot \alpha^6 = \alpha^{11} = \alpha^{11-7} = \alpha^4 = \alpha+\alpha^2$.

On obtient la table de multiplication suivante :

$\cdot$	0	1	α	$1+\alpha$	α^2	$\alpha+\alpha^2$	$1+\alpha^2$	$1+\alpha+\alpha^2$
0	0	0	0	0	0	0	0	0
1	0	1	α	$1+\alpha$	α^2	$\alpha+\alpha^2$	$1+\alpha^2$	$1+\alpha+\alpha^2$
α	0	α	α^2	$\alpha+\alpha^2$	$1+\alpha$	$1+\alpha+\alpha^2$	1	$1+\alpha^2$
$1+\alpha$	0	$1+\alpha$	$\alpha+\alpha^2$	$1+\alpha^2$	$1+\alpha+\alpha^2$	1	α^2	α
α^2	0	α^2	$1+\alpha$	$1+\alpha+\alpha^2$	$\alpha+\alpha^2$	$1+\alpha^2$	α	1
$\alpha+\alpha^2$	0	$\alpha+\alpha^2$	$1+\alpha+\alpha^2$	1	$1+\alpha^2$	α	$1+\alpha$	α^2
$1+\alpha^2$	0	$1+\alpha^2$	1	α^2	α	$1+\alpha$	$1+\alpha+\alpha^2$	$\alpha+\alpha^2$
$1+\alpha+\alpha^2$	0	$1+\alpha+\alpha^2$	$1+\alpha^2$	α	1	α^2	$\alpha+\alpha^2$	$1+\alpha$

$(\mathbb{F}_8^*, \cdot)$ étant un groupe multiplicatif, on vérifie bien que dans le sous-tableau formé par les 26 éléments de K^*, un élément de K^* ne figure qu'une et une seule fois par ligne et par colonne.

Chapitre 5

Conclusion

Si vous êtes arrivés au bout de ce rapport, félicitations, vous pouvez maintenant comprendre les principes de construction des corps finis.

Vous connaissez les deux techniques utilisées pour réduire la taille des structures algébriques que sont les groupes, anneaux et corps. Vous savez que la première méthode consiste à créer un sous-ensemble qui conserve les propriétés de ces structures tandis que la deuxième fait appel aux relations d'équivalence qui permettent de construire des ensembles quotients.
Si la première méthode est utile pour la construction des groupes cycliques, elle ne permet pas de construire aisément des sous-corps. Par contre, la deuxième est un outil plus puissant.
En définissant une relation d'équivalence à partir d'un sous-ensemble de la structure et en choisissant correctement ce sous-ensemble, on peut alors munir l'ensemble quotient d'opérations et construire de nouvelles structures algébriques de taille réduite.
Avec cette méthode, on a obtenu aussi une première famille de corps finis les $\mathbb{Z}/p\mathbb{Z}$ avec p premier.

Vous avez ensuite appris que pour construire d'autres corps finis, on choisit comme famille d'anneaux les ensembles de polynômes à coefficients dans corps K notés $K[X]$ que l'on peut munir en plus d'une division euclidienne. Cela permet de disposer de propriétés arithmétiques semblables à celles utilisées dans l'ensemble $\mathbb{Z}$ des entiers relatifs et de définir une relation de congruence modulo un polynôme. Dans $K[X]$, les idéaux maximaux sont ceux engendrés par des polynômes irréductibles qui jouent le rôle d'éléments premiers. Si K est fini et P irréductible, alors l'ensemble quotient $K[X]/(P)$ est un corps fini. Si on prend K égal à $\mathbb{Z}/p\mathbb{Z}$ et P de degré n, alors on obtient des corps finis de cardinal p^n.

La construction par recherche intuitive de corps finis nous a permis de trouver des corps à 2, 3, 4 éléments mais nous a montré qu'il n'existe pas de corps à 6 éléments.
C'est ce que nous a confirmé une explication théorique faisant appel à la notion de caractéristique d'un corps qui nous montre que le cardinal d'un corps fini ne peut être égal qu'à la puissance d'un nombre premier.
Cela nous permet donc d'utiliser les $\mathbb{Z}/p\mathbb{Z}$ pour obtenir des corps $\mathbb{Z}/p\mathbb{Z}[X]/(P)$ de toute taille en faisant varier p et le degré n de P.

Vous avez vu que la relation de congruence modulo un polynôme permet de définir les éléments de ces corps comme des polynômes de degré $n-1$. Mais grâce à une propriété remarquable du groupe des inversibles à savoir la cyclicité, on dispose d'une deuxième représentation des éléments non nuls du corps. On peut ainsi les définir comme des puissances distinctes d'un générateur.

Enfin, l'application pratique vous a permis de construire pas à pas un corps à 8 éléments et de mettre en pratique les différentes notions présentées précédemment dans ce cours.

J'espère vous aurez pris du plaisir et de l'intérêt à lire ce rapport.
J'espère aussi vous avoir montré que les maths sont utiles et que des sujets de mathématiques pures peuvent être à la portée de gymnasiens.

Chapitre 6

Bilan

6.1 Motivations

Lorsque j'ai choisi ce sujet de TM, j'avais plusieurs objectifs en tête.

Dans le cadre de mes choix d'orientation, je voulais tester mon goût et mes aptitudes pour les maths.
Je voulais savoir si j'étais prête à étudier des livres de maths et des démonstrations pendant des heures.

Je voulais aussi faire un TM qui montre que les mathématiques sont utiles et qui puisse faire aimer les mathématiques.
C'est pourquoi j'ai parlé de cryptographie sans trop savoir ce qu'il y avait derrière. J'aime bien les casses-têtes, les énigmes mathématiques et M.Devanthéry nous avait initié en fin de première année de gymnase à des algorithmes simples de cryptographie basés sur la théorie des nombres premiers. Mais je ne savais pas trop ce qu'il y avait derrière.
C'est alors que M.Devanthéry m'a proposé un sujet sur la construction de corps finis.

6.2 Déroulement du TM

— **Première phase : phase de recherche**
J'ai commencé par lire un ouvrage sur la théorie des groupes. Ce fut difficile au début, comprendre les preuves m'a demandé de relire plusieurs fois les mêmes pages mais je me suis rendue compte que j'aimais ça. Je découvrais la construction d'ensembles de nombres bien connus.

Sur la théorie des groupes, j'ai pu trouver des cours plutôt accessibles. Mais pour la théorie des anneaux et des corps, je n'ai quasiment trouvé que des cours d'algèbre de niveau bachelor. J'ai consacré beaucoup de temps à la compréhension des notions de base.
J'ai également dû réécrire les preuves en ajoutant nombres d'explications afin qu'elles soient plus claires. En effet, des notions qui semblent évidentes à un élève de bachelor sont loins de l'être pour moi.

— **Deuxième phase : rédaction d'une synthèse des lectures**
Une autre difficulté était l'organisation des idées de mon rapport. Comment enchaîner ces éléments de théorie, ces théorèmes et définitions ?
Les cours que j'ai trouvés étaient de progression séquentielle : les groupes, les anneaux, les corps.
Un cours sur les corps supposent que les connaissances sur les groupes et les anneaux sont déjà

connues.
Je suis donc partie de la conclusion à savoir la construction de corps finis et je suis repartie en arrière en ajoutant à chaque fois des éléments nouveaux. D'où vient ce théorème auquel il est fait référence, quelles sont les notions utiles pour le démontrer ?
À la fin, j'ai remis les idées dans un ordre séquentiel en repartant du début, ensembles, groupes, anneaux et corps. J'ai rédigé un cours qui contenait tous les éléments nécessaires à la compréhension de la construction de corps finis. Cela a finalement donné une synthèse des cours d'algèbre que j'avais trouvés.
Cette première étape m'a pris énormément de temps (jusqu'à fin juillet).

Mais ma "synthèse" faisait quand même 70 pages ! Et surtout il fallait attendre plus de la moitié du rapport pour découvrir une ligne sur les corps finis. Et il manquait un lien.

— **Troisième phase : rédaction du rapport**
J'ai donc décidé de changer de perspective : définir des problématiques à partir de questions simples que pourrait se poser le lecteur (qu'est-ce qu'une structure algébrique, comment réduire sa taille, ...) et de traiter chacune de ces problématiques pour l'ensemble des structures.
Je me suis inspiré des courtes présentations orales que je faisais de mon TM à mon entourage (famille, camarades, ...) lorsque je devais expliquer sur quoi je travaillais.
J'ai ainsi réorganisé totalement mes chapitres pour parler des corps dès la 3ème page du TM.
Afin de ne pas perdre mes lecteurs, j'ai choisi un fil conducteur à savoir la construction d'un corps fini.

J'ai dû renoncer à quelques démonstrations afin de ne pas me disperser, et d'éviter trop de notions telles que les homomorphismes.
J'ai dû sélectionner les preuves "stars" que je voulais conserver. J'ai gardé le théorème de Lagrange, la cyclicité du groupe des inversibles et le quotient d'un anneau par un idéal maximal.

L'important travail au cours de la première étape m'a été très utile et cette troisième étape fut plutôt rapide par rapport aux deux premières. Je connaissais mon sujet, c'était plus simple.

Dans cette phase, j'ai dû faire un effort de vulgarisation afin que les notions abordées restent à la portée du public visé. En effet, j'ai retenu comme forme pour mon TM un cours de maths pour les gymnasiens.
J'ai modifié quelques preuves et choisi de nouveaux exemples.
Ce qui était difficile car il fallait rendre le rapport accessible, c'était parfois de rajouter des éléments et donc d'allonger le rapport.

Plus que la nature du public visé, le nombre de pages limité à 30 pour le corps du TM (chapitres 2 à 4) (c'est une contrainte imposée par mon gymnase à tous les TM) a été une forte contrainte.

6.3 Bilan personnel

Sur un plan personnel, j'ai beaucoup appris :

— j'ai beaucoup aimé apprendre à utiliser LaTex. Utiliser LaTex m'a aidée à être plus rigoureuse dans le langage mathématique.

— je sens que j'ai fait des progrès en mathématiques, notamment dans la logique des démonstrations, Cela m'a déjà aidée pour le premier cours de 3ème année sur les espaces vectoriels.

— j'ai fait des progrès en synthèse.

— j'ai eu un avant-goût des cours de maths universitaires.

Je remercie M.Devanthéry de m'avoir poussé à aller plus loin dans mes connaissances, à sortir de ma zone de confort.

En conclusion, j'encourage les gymnasiens à choisir des TM de maths.

Chapitre 7

Bibliographie et sitographie

7.1 Bibliographie

1. Assem Ibrahim, Leduc Pierre Yves, *Cours d'algèbre, Groupes, anneaux, modules et corps*, Québec, Presses internationales Polytechnique, 2009, pp.113-124, 153-183, 200-203, 239-262, 265-282, 323-329, 339-344, 353-355, 393-411, 633-636.
2. Bailly-Maitre Gilles, *Arithmétique et cryptologie*, Paris, Ellipses, 2012, pp.39-60, 93-97, 115-122, 194-195.
3. Buchmann Johannes, *Introduction à la cryptographie*, collection Sciences sup, Paris, Dunod, 2016, pp.27-35, 45-53.
4. Dubertret Gilles, *Initiation à la cryptographie*, Paris, Vuibert, 2018, pp.17-20, 35, 95-99.
5. Gred Louis, *Notions fondamentales de la mathématique élémentaire*, Suisse, Editions L.E.P. Loisirs et Pédagogie, 1980.

7.2 Sitographie

1. Caruso Xavier, directeur de recherche en mathématiques au CNRS, *Choisissez votre corps !*, exposé à Mathematic Park, 2004, p.36.
   [En ligne] Site Xavier Caruso, consulté le 09.10.2019.
   Disponible à l'adresse : htpp ://xavier.toonywood.org/popularization/mathpark/corps.pdf
2. Kraus Alain, professeur à l'université Pierre et Marie Curie de Paris, polycopié du cours Arithmétique et Algèbre, 2M220, 2016-2017, 126 p.
   [En ligne] Département Informatique de l'Ecole Normale Supérieure, consulté le 09.10.2019.
   Disponible à l'adresse : https ://di.ens.fr/ nitulesc/files/2M220/Cours.pdf
3. Kraus Alain, professeur à l'université Pierre et Marie Curie de Paris, polycopié du cours de cryptographie MM029, 2009-2010, chapitre III - Corps finis, 24 p.
   [En ligne] Département de Mathématiques de l'Université Paris 13, consulté le 09.10.2019.
   Disponible à l'adresse : https ://www.math.univ-paris13.fr/ boyer/enseignement/crypto/Chap3.pdf
4. Kohel David, professeur à l'université d'Aix-Marseille, polycopié du cours de cryptographie symétrique, Rappel sur les corps finis, 9 p.
   [En ligne] Institut de mathématiques de Luminy IML, consulté le 09.10.2019.
   Disponible à l'adresse : http ://iml.univmrs.fr/ kohel/tch/M2CryptoSymetrique/CM/RappelCorps_finis.pdf
5. Evain Laurent, professeur à l'université d'Angers, Polycopié du Cours sur les Anneaux, 2014, 112 p.
   [En ligne] Mathématiques à Angers, consulté le 09.10.2019.
   Disponible à l'adresse : https ://www.math.univ-angers.fr/ evain/_static/anneaux.pdf

6. Geandier Françoise, maître de conférences à l'université Henri Poincaré de Nancy, Polycopié du cours d'algèbre pour Licence 3, 2009, pp.1-15, 38-42.
[En ligne] Institut Elie Cartan de Lorraine IECL, consulté le 09.10.2019.
Disponible à l'adresse : http ://www.iecl.univ-lorraine.fr/ Francoise.Geandier/cours-Alg-L3-2009.pdf

7. Goze Michel, Remm Elizabeth, professeurs à la Faculté des Sciences et Techniques de l'Université de Haute-Alsace FST-UHA, Polycopié du cours de mathématiques pour Licence 3 et Master 1, Théorie des corps, 2014, pp.5-9, 11-12, 27-28.
[En ligne] Livres de mathématiques, consulté le 09.10.2019.
Disponible à l'adresse : http ://livres-mathematiques.fr/onewebmedia/Theorie%20des%20Corps7.pdf

8. Rolland Robert, chercheur à l'institut de mathématiques de Marseille, Aspects cryptographiques des corps finis, 2007 révisé le 18 avril 2015, présentation, 39 p.
[En ligne] Acrypta, consulté le 09.10.2019.
Disponible à l'adresse : http ://www.acrypta.com/telechargements/cfel/crypto_cf.pdf

9. Schön Walter, professeur au Département de Génie informatique de l'Université de Technologie de Compiègne, Présentation cours de Mathématiques pour la cryptographie 2ème partie, Anneaux de polynômes et corps finis, 2001, pp.2-10, 12-14, 16-33.
[En ligne] Université de Compiègne UTC, consulté le 09.10.2019.
Disponible à l'adresse : https ://www.utc.fr/ wschon/sr06/CoursMT10Partie2.pdf

10. Zémor Gilles, professeur à l'Université de Bordeaux, Polycopié du cours de master Cryptologie et Sécurité Informatique, Arithmétique 1, Corps finis et applications, 2006, pp.1-8.
[En ligne] Institut de mathématiques de Bordeaux, consulté le 09.10.2019.
Disponible à l'adresse : https ://www.math.u-bordeaux.fr/ gzemor/arit06.pdf

11. Collectif La minerve, Ecole Normale Supérieure de Rennes, 2013-2014, 3 p.
Preuve du théorème "Le groupe multiplicatif d'un corps fini est cyclique".
(adaptation de la preuve de Perrin Daniel, Cours d'algèbre, Ellipses, 1996, p.74)
[En ligne] La minerve de l'ENS de Rennes (site aide préparation agrégation maths), consulté le 09.10.2019.
Disponible à l'adresse : https ://www.minerve.ens-rennes.fr/images/Groupe_multiplicatif.pdf

12. Collectif, Université de Bordeaux, Polycopié du résumé du cours de Structures Algébriques 1, pp.5-12, 23-24, 31-40, 45-50.
[En ligne] Institut de mathématiques de Bordeaux, page de Renaud Coulangeon, consulté le 09.10.2019.
Disponible à l'adresse : https ://www.math.u-bordeaux.fr/ rcoulang/n1ma4w11/stalg1web.pdf

13. Elèves de l'Ecole Normale Supérieure de Paris, cours d'algèbre 1 d'Ariane Mézard, exposé sur les corps finis, 2016, 11 p.
[En ligne] Institut de mathématiques de Jussieu Paris-Rive Gauche IMJ-PRG, Ariane Mézard, consulté le 09.10.2019.
Disponible à l'adresse : https ://webusers.imj-prg.fr/ ariane.mezard/corps-fini.pdf