Introduction aux corps finis

Grigaliūnaitė Deimantė* Enzo Malescot† Théotime Sabathié‡

Encadrant: Stéphane Fischler§

17 janvier 2025

Résumé

We explore the possible cardinalities of finite fields. Starting with groups, we gradually build the theory necessary to define and construct finite fields, particularly those of the form $\mathbb{F}_{g(x)}$ of cardinality p^m. Through the study of polynomials and their properties, we demonstrate that all finite fields are isomorphic to fields of this form. Along the way, we present key theorems, lemmas and examples to support our conclusions.

1 Introduction

Dans cet article, nous allons aborder les définitions des structures algébriques usuelles, telles que les groupes et les corps finis, et en déduire des théorèmes généraux sur ces structures.

Nous commencerons par définir les (sous-)groupes, en particulier les sous-groupes cycliques, ce qui sera très utile pour le corps principal de notre étude : les corps finis. Nous étudierons d'abord les corps premiers $\mathbb{F}_p$, puis nous présenterons les sous-corps. Nous passerons ensuite aux polynômes, que nous utiliserons pour construire les corps de la forme $\mathbb{F}_{g(x)} \sim \mathbb{F}_{p^m}$ pour tout $p \in \mathscr{P}$ l'ensemble des nombres premiers, pour tout $m \in \mathbb{N}^*$. Nous montrerons que tous les corps finis sont isomorphes aux corps de ce type, atteignant ainsi notre objectif principal.

Nous nous intéresserons particulièrement à ces structures en raison de leurs nombreuses applications dans divers domaines des mathématiques et bien au-delà. En effet, ces structures sont utilisées en cryptographie ainsi que dans les langages informatiques de vérification d'erreurs.

De plus, l'intérêt d'étudier ces structures de manière théorique se révèlera pleinement lorsque nous démontrerons le théorème d'isomorphisme qui établit que tous les corps finis sont isomorphes à ceux que nous construisons, ayant p^m éléments.

Enfin, nous tenons particulièrement à remercier Monsieur Stéphane Fischler, professeur et chercheur à l'Institut Mathématique d'Orsay. Ce professeur a eu la charge de nous encadrer, de nous accompagner et de corriger notre travail d'Immersion Recherche effectué durant notre troisième semestre de Licence Mathématiques-Physique à l'Université Paris-Saclay.

*Étudiante à l'université Paris Saclay

†Étudiant à l'université Paris Saclay

‡Étudiant à l'université Paris Saclay

§Enseignant chercheur à l'institut mathématique d'Orsay, Université Paris-Saclay

Table des matières

2 Ensembles

En mathématiques, un ensemble est une collection d'objets distincts, appelés *éléments*, considérés comme une unité. Ces objets peuvent être de nature variée (nombres, lettres, fonctions, etc.), et l'ensemble est caractérisé par le fait que chaque élément y appartient ou n'y appartient pas. L'appartenance d'un élément à un ensemble est exprimée par la relation "$\in$" (par exemple, si a est un élément de l'ensemble A, on écrit $a \in A$).

Explication des ensembles numériques

- $\mathbb{N}$: L'ensemble des **nombres naturels**, qui comprend les nombres : $0, 1, 2, 3, \ldots$ Cet ensemble est utilisé pour compter et ordonner des objets.

- $\mathbb{Z}$: L'ensemble des **entiers relatifs**, comprenant tous les entiers positifs, négatifs ainsi que zéro : $\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots$

- $\mathbb{Q}$: L'ensemble des **nombres rationnels**, qui inclut tous les nombres pouvant s'écrire sous forme de fraction $\frac{p}{q}$, où $p, q \in \mathbb{Z},\ q \neq 0$. On peut ajouter : $p \wedge q = 1$.

- $\mathbb{R}$: L'ensemble des **nombres réels**, qui inclut tous les nombres rationnels ainsi que les nombres irrationnels. Les réels peuvent être représentés sur la droite numérique.

- $\mathbb{C}$: L'ensemble des **nombres complexes**, qui comprend tous les nombres sous la forme $a + bi$, où a et b sont des réels et $i^2 = -1$ est l'unité imaginaire.

On obtient donc la suite d'inclusion suivante : $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$

3 Les groupes

3.1 Définitions

Nous avons tous rencontré des groupes dans notre vie quotidienne, même si nous ne savions pas nécessairement ce que c'était. Par exemple, les nombres entiers $\mathbb{Z}$ munis de l'opération d'addition, que chaque enfant apprend à l'école, constituent l'exemple le plus simple d'un groupe infini. Pour notre étude, il est nécessaire de définir plus précisément les groupes et de se concentrer sur les groupes finis.

Les groupes sont notés $(G, \oplus)$, où G est un ensemble et $\oplus$ est l'opération du groupe. Ils respectent des axiomes élémentaires qui les définissent :

1. *Clôture :* $\forall a, b \in G,\ a \oplus b \in G$.
2. *Associativité :* $\forall a, b, c \in G,\ a \oplus (b \oplus c) = (a \oplus b) \oplus c$.
3. *Élément neutre : il existe un élément neutre* $e \in G$ *tel que pour tout* $a \in G$, $a \oplus e = a = e \oplus a$.
4. *Inverse : pour tout* $a \in G$, *il existe un inverse* $-a \in G$ *tel que* $a \oplus (-a) = e = (-a) \oplus a$.

On pourrait remplacer les axiomes 1 et 4 par :

Propriété de permutation : pour tout $a \in G$, $a \oplus G = \{a \oplus b : b \in G\} = G$.

On montre cette propriété de la manière suivante : On voit qu'il existe $b \in G$ tel que $a \oplus b = 0$, car $0 \in a \oplus G$. De plus, avec $a \oplus G$, on obtient toutes les opérations possibles $a \oplus b$ pour $b \in G$. Ainsi, les deux propriétés sont couvertes par celle-ci.

3.2 Exemple

Calcul d'horloge

On définit l'ensemble $\mathbb{Z}/12\mathbb{Z} := \{0, 1, 2, \ldots, 11\} = \{k \mod 12 : k \in \mathbb{Z}\}$, muni de l'addition $+$. Autrement dit, on prend tous les restes obtenus en divisant les entiers par 12. Vérifions que c'est un groupe :

1. *Clôture :* Pour tous $a, b \in \mathbb{Z}/12\mathbb{Z}$, la somme $a+b \in \mathbb{Z}/12\mathbb{Z}$ par définition de l'arithmétique modulaire. Si $a + b \geq 12$, alors $a + b \equiv (a + b - 12) \pmod{12}$. Ainsi, $a + b \in \mathbb{Z}/12\mathbb{Z}$.
2. *Associativité :* L'addition est associative sur $\mathbb{Z}$, et cette propriété reste valide modulo 12. En effet, pour tous $a, b, c \in \mathbb{Z}/12\mathbb{Z}$, nous avons $(a + b) + c \equiv a + (b + c) \pmod{12}$.
3. *Élément neutre :* L'élément $0 \in \mathbb{Z}/12\mathbb{Z}$ est l'élément neutre car, pour tout $a \in \mathbb{Z}/12\mathbb{Z}$, $a + 0 = a = 0 + a$.
4. *Inverse :* Pour tout $a \in \mathbb{Z}/12\mathbb{Z}$, l'inverse est $-a \equiv 12 - a \pmod{12}$. En effet, $a + (-a) = (-a) + a = a + 12 - a = 12 \equiv 0 \pmod{12}$. □

On peut comparer ce groupe au comptage sur une horloge : par exemple, $8 + 5 = 13$, mais comme une horloge revient à 1 après 12, on obtient $13 \equiv 1 \pmod{12}$. Cela reflète le fonctionnement de l'arithmétique modulaire.

Remarque : Ce groupe, comme beaucoup d'autres, est *commutatif*, c'est-à-dire que $a+b = b+a$ pour tous $a, b \in \mathbb{Z}/12\mathbb{Z}$. Cependant, il existe des groupes non commutatifs, comme le groupe des permutations sur un ensemble ayant au moins 2 éléments. Les axiomes élémentaires des groupes ne mentionnent pas cette propriété, donc, en général, les groupes ne sont pas commutatifs.

3.3 Propriétés

Unicité de l'élément neutre

Soit $(G, *)$ un groupe. Nous allons prouver que l'élément neutre est unique dans G.

Soient e_1 et e_2 deux éléments neutres dans G, c'est-à-dire que :

$$\forall g \in G, \quad e_1 * g = g * e_1 = g \quad \text{et} \quad e_2 * g = g * e_2 = g.$$

En utilisant la propriété de e_1 comme élément neutre, on a :

$$e_1 * e_2 = e_2$$

De même, en utilisant e_2 comme élément neutre, on a :

$$e_1 * e_2 = e_1$$

Ainsi, $e_1 = e_2$, ce qui prouve que l'élément neutre est unique. □

Unicité de l'inverse

Soit $g \in G$. Nous devons prouver que l'inverse de g est unique.

Soient h_1 et $h_2 \in G$ deux inverses de g, c'est-à-dire que :

$$g * h_1 = h_1 * g = e \quad \text{et} \quad g * h_2 = h_2 * g = e,$$

où e est l'élément neutre de G.

En utilisant h_1 puis h_2 comme inverses de g, on a par associativé :

$$h_1 = h_1 * e = h_1 * (g * h_2) = (h_1 * g) * h_2 = e * h_2 = h_2.$$

Ainsi, $h_1 = h_2$, ce qui prouve que l'inverse de g est unique. □

3.4 Sous-groupes

En pratique pour montrer qu'un objet possède une structure de groupe nous nous rapportons à un groupe déjà connu. En effet, pour montrer qu'un objet est un groupe nous montrons la plupart du temps que celui-ci est en fait un sous-groupe H d'un groupe déjà connu $(G, *)$.

Pour cela il nous suffit de vérifier 2 propriétés :

— $H \neq \varnothing$

— $\forall\ g, h \in H$ on a $gh^{-1} \in H$

Attention : pour rappel h^{-1} est l'inverse de h. Donc par exemple si on est dans $(G, +)$ alors $h^{-1} = -h$ et si on est dans $(G, \times)$ alors $h^{-1} = \frac{1}{h}$.

Exemple :

Soit $(G, \times)$ un groupe (pas forcément commutatif). On appelle *centre* de G, noté $\mathcal{Z}(G)$, l'ensemble des éléments de G commutant avec tous les éléments de G. Montrons que c'est un sous-groupe de G.

Notons, e le neutre de G et soient $z \in G$, $x, y \in \mathcal{Z}(G)$.

$$e \times x = x \times e \quad \text{On a } \mathcal{Z}(G) \neq \varnothing.$$

Voyons si $xy^{-1} \in \mathcal{Z}(G)$ c'est à dire si $x \times y^{-1} \times z = z \times x \times y^{-1}$:

$$x \times y^{-1} \times z = x \times y^{-1} \times z \times e = x \times y^{-1} \times z \times y \times y^{-1} \quad \text{propriété de } e$$

$$= x \times y^{-1} \times y \times z \times y^{-1} = x \times e \times z \times y^{-1} = x \times z \times y^{-1} = z \times x \times y^{-1} \quad \text{par propriété de } \mathcal{Z}(G) \quad \square$$

Donc $\mathcal{Z}(G)$ est bien un sous-groupe de G.

3.5 Groupes et sous-groupes cycliques

Définition

Un **groupe cyclique** est un groupe dont tous les éléments peuvent être obtenus comme puissances successives (en notation multiplicative : g^k) ou comme multiples (en notation additive : $k\,g$) d'un élément particulier appelé **générateur** du groupe. De plus il faut que ce groupe soit fini.

Exemples

Pour illustrer prenons 3 exemples de groupes cycliques que vous connaissez probablement déjà :

— $(\mathbb{Z}/n\mathbb{Z}, +)$ Le groupe des restes des entiers dans la division euclidienne par n. Il est fini, de cardinal n évidemment 1 l'engendre toujours.

— $(\mathbb{Z}/n\mathbb{Z}, \times)^*$ Le groupe des inversibles modulo n. C'est le groupe des entiers a pour lesquels il existe k tel que $k\,a \equiv 1 \mod n$. Grâce au théorème de Bezout on s'aperçoit également que cette définition est équivalente à $a \wedge n = 1$.

Pour illustrer prenons $(\mathbb{Z}/5\mathbb{Z}, \times)^*$, 5 est premier donc les nombres entre 1 et 4 sont tous premiers avec lui. Il est donc composé de 4 éléments, on dit qu'il est d'ordre 4 et on note $|(\mathbb{Z}/5\mathbb{Z}, \times)^*| = 4$. Nous verrons dans la prochaine partie comment calculer le cardinal de n'importe quel $(\mathbb{Z}/n\mathbb{Z}, \times)^*$.

Après avoir eu de la chance au brouillon vous pouvez voir que les puissances de 2 sont les suivantes :

Exposant	**Puissance de 2**	**Résultat Modulo 5**
1	2^1	2
2	2^2	4
3	2^3	$8 \equiv 3 \pmod 5$
4	2^4	$2 \times 3 = 6 \equiv 1 \pmod 5$

On voit donc que 2 engendre tous les éléments de $(\mathbb{Z}/5\mathbb{Z}, \times)^*$, il est donc générateur et $(\mathbb{Z}/5\mathbb{Z}, \times)^*$ est un groupe cyclique.

— Les **racines n-ièmes de l'unité** sont les solutions de l'équation $x^n = 1$ dans $\mathbb{C}$. Elles forment un groupe cyclique d'ordre n, où chaque racine est une puissance de $e^{2\pi i/n}$, un générateur de ce groupe.

— Les racines carrées de l'unité : 1 et -1.
— Les racines cubiques de l'unité : 1, $e^{2\pi i/3}$ et $e^{4\pi i/3}$.
— Les racines quatrièmes de l'unité : 1, i, -1 et $-i$, où $i = e^{2\pi i/4}$.

Pour illustrer ces exemples, voici une représentation graphique des racines n-ièmes de l'unité sur le cercle unité :

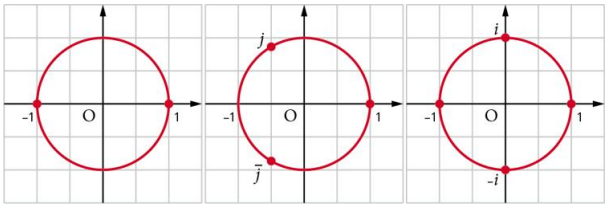

FIGURE 1 – Illustration des racines carrées, cubiques et quatrièmes de l'unité

— En contre exemple on peut voir $(\mathbb{Z}, +)$ en effet 1 l'engendre mais il n'est pas fini donc pas cyclique.

3.6 Théorème de Lagrange

Le théorème de Lagrange est essentiel car il relie l'ordre d'un groupe fini à celui de ses sous-groupes, permettant de classifier les sous-groupes et de comprendre la structure du groupe. Le **théorème de Lagrange** affirme que dans un groupe fini G, l'ordre d'un sous-groupe H divise l'ordre de G : $|H| \mid |G|$.

Exemple 1 : Dans $G = (\mathbb{Z}/12\mathbb{Z}, +)$, d'ordre $|G| = 12$, le sous-groupe $H = \langle 4 \rangle = \{0, 4, 8\}$ a un ordre $|H| = 3$, et $3 \mid 12$.

3.7 Décomposition d'un groupe selon les ordres de ses éléments

Comme dit précédemment, nous allons montrer comment calculer l'ordre de n'importe quel $(\mathbb{Z}/n\mathbb{Z}, \times)^*$

Pour cela nous devons introduire "l'indicatrice d'Euler φ"

$$\begin{aligned}\varphi : \mathbb{N}^* &\longrightarrow \mathbb{N}^* \\ n &\longmapsto \text{card}\left(\{m \in \mathbb{N}^* \mid m \leqslant n \text{ et } m \text{ premier avec } n\}\right)\end{aligned}$$

Calcul de $\varphi(n)$ à partir de la décomposition en facteurs premiers

Soit n décomposé en facteurs premiers sous la forme :

$$n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \cdots \times p_k^{\alpha_k}$$

où $p_1, p_2, \ldots, p_k$ sont des nombres premiers distincts et $\alpha_1, \alpha_2, \ldots, \alpha_{k\geq 1}$ sont les puissances associées.

L'indicatrice d'Euler $\varphi(n)$ peut être exprimée de manière équivalente grâce à la formule suivante :

$$\varphi(n) = (p_1^{\alpha_1} - p_1^{\alpha_1 - 1}) \times (p_2^{\alpha_2} - p_2^{\alpha_2 - 1}) \times \cdots \times (p_k^{\alpha_k} - p_k^{\alpha_k - 1}).$$

Explication :

Cette formule est une forme alternative de la définition de $\varphi(n)$. Elle utilise la décomposition de n en facteurs premiers et ajuste chaque facteur pour exclure les multiples de p_i parmi les entiers inférieurs ou égaux à n. En d'autres termes, chaque facteur $p_i^{\alpha_i} - p_i^{\alpha_i - 1}$ exclut les multiples de p_i.

— **Exemple 1 :** Soit $n = 12$. La décomposition de 12 est $12 = 2^2 \times 3$. En appliquant la formule de $\varphi(n)$:

$$\varphi(12) = (2^2 - 2^1) \times (3^1 - 3^0) = 2 \times (3 - 1) = 2 \times 2 = 4$$

Ainsi, $\varphi(12) = 4$. Il y a donc 4 entiers premiers avec 12 entre 1 et 12.

— **Exemple 2 :** Soit $n = 30$. La décomposition de 30 est $30 = 2^1 \times 3^1 \times 5^1$. En appliquant la formule de $\varphi(n)$:

$$\varphi(30) = (2^1 - 2^0) \times (3^1 - 3^0) \times (5^1 - 5^0) = 1 \times 2 \times 4 = 8$$

Ainsi, $\varphi(30) = 8$. Il y a donc 8 entiers premiers avec 30.

Lemme : Si $d \mid n$, le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$ possède exactement $\varphi(d)$ éléments d'ordre d.

Un élément x d'ordre d de $\mathbb{Z}/n\mathbb{Z}$ est générateur d'un sous-groupe à d éléments, noté $\langle x \rangle$. Inversement, tout générateur d'un tel sous-groupe est un élément d'ordre d de $\mathbb{Z}/n\mathbb{Z}$. Or, $\langle x \rangle$ est isomorphe à $\mathbb{Z}/d\mathbb{Z}$. Ainsi, $\langle x \rangle$ contient donc $\varphi(d)$ générateurs. De plus $\mathbb{Z}/n\mathbb{Z}$ possède un seul et unique sous-groupe d'odre d. En conséquence, $\mathbb{Z}/n\mathbb{Z}$ possède exactement $\varphi(d)$ éléments d'ordre d.

D'après le *théorème de Lagrange* l'ordre d'un élément de $\mathbb{Z}/n\mathbb{Z}$ divise n. De plus, d'après ce même lemme, il existe $\varphi(d)$ éléments d'ordre d pour chaque diviseur d de n. En parcourant tous les ordres possibles, on obtient l'égalité suivante :

$$n = \sum_{d=1}^{n} Card(\{x \in \mathbb{Z}/n\mathbb{Z},\ o(x) = d\}) = \sum_{d|n} \varphi(d),$$

où $o(x)$ désigne l'ordre de l'élément x.

4 Les corps

4.1 Définitions

Un **corps** est un ensemble $\mathbb{K}$ muni de deux opérations, l'addition $+$ et la multiplication $\times$, qui satisfont aux axiomes suivants :

1. **Axiomes de l'addition** :
   — $(\mathbb{K}, +)$ est un groupe *commutatif*.
2. **Axiomes de la multiplication** :
   — *Clôture* : $\forall\ a, b \in \mathbb{K}\ \ a \times b \in \mathbb{K}$.
   — La multiplication est *associative* : $(a \times b) \times c = a \times (b \times c)$ pour tous $a, b, c \in \mathbb{K}$.
   — Il existe un *élément neutre* pour la multiplication, noté $1_{\mathbb{K}}$, tel que $a \times 1_{\mathbb{K}} = a$ pour tout $a \in \mathbb{K}$.
   — Chaque élément $a \in \mathbb{K}^* = \mathbb{K} \setminus \{0_{\mathbb{K}}\}$, a un *inverse* multiplicatif, noté a^{-1}, tel que $a \times a^{-1} = 1_{\mathbb{K}}$.
   — La multplication est *commutative*.
3. **Distributivité** : La multiplication est *distributive* par rapport à l'addition, c'est-à-dire que pour tous $a, b, c \in \mathbb{K}$, on a :

$$a \times (b + c) = a \times b + a \times c.$$

Exemple : $\mathbb{Z}/p\mathbb{Z}$ comme un corps

Soit p un nombre premier. Nous allons vérifier que $\mathbb{Z}/p\mathbb{Z}$ satisfait les axiomes d'un corps :

1. **Axiomes de l'addition** : Les axiomes d'addition sont triviaux, car $\mathbb{Z}/p\mathbb{Z}$ hérite des propriétés de $\mathbb{Z}$ (associativité, existence de l'élément neutre 0, et existence d'opposés).
2. **Axiomes de la multiplication** :
   — La multiplication est associative, car elle est définie comme une multiplication habituelle modulo p, et la multiplication dans $\mathbb{Z}$ est associative.
   — L'élément neutre pour la multiplication est 1, car pour tout $a \in \mathbb{Z}/p\mathbb{Z}$, $a \times 1 = a$ modulo p.
3. **Existence d'inverses multiplicatifs** : L'élément $a \in \mathbb{Z}/p\mathbb{Z}$ est inversible si et seulement si $a \neq 0$. En effet, puisque p est premier, a et p sont premiers entre eux pour tout $a \neq 0$, et donc il existe un entier b tel que $a \times b \equiv 1 \pmod{p}$ (ceci découle du théorème de Bézout).
4. **Distributivité** : La distributivité de la multiplication par rapport à l'addition est vérifiée, car la multiplication et l'addition dans $\mathbb{Z}/p\mathbb{Z}$ respectent les mêmes lois que dans $\mathbb{Z}$, et l'opération est simplement effectuée modulo p.

Ainsi, $\mathbb{Z}/p\mathbb{Z}$ est un corps lorsque p est un nombre premier, car tous les axiomes d'un corps sont satisfaits. C'est un exemple de corps fini, parfois noté $\mathbb{F}_p$, qui est utilisé fréquemment en cryptographie et en théorie des codes.

4.2 Sous-Corps

En pratique d'une façon analogue aux groupes, nous nous ramenons le plus souvent à des corps déjà bien connu pour montrer que d'autres ensembles sont des corps.

Preuve : $\mathbb{Q}[\sqrt{2}]$ est un corps

Soit $\mathbb{K} = \mathbb{Q}[\sqrt{2}] \subset \mathbb{R}$, l'ensemble des nombres de la forme $a + b\sqrt{2}$ où $a, b \in \mathbb{Q}$. Nous allons démontrer que $\mathbb{K}$ est un corps.

1. **Fermeture sous l'addition et la multiplication** :
   — La somme et le produit de deux éléments de $\mathbb{Q}[\sqrt{2}]$, disons $(a + b\sqrt{2})$ et $(c + d\sqrt{2})$, sont respectivement $(a+c)+(b+d)\sqrt{2}$ et $(ac+2bd)+(ad+bc)\sqrt{2}$, qui sont également dans $\mathbb{Q}[\sqrt{2}]$, car $a, b, c, d \in \mathbb{Q}$.
2. **Axiomes de l'addition et de la multiplication** : Les axiomes de commutativité, associativité et existence des éléments neutres pour l'addition et la multiplication sont vérifiés dans $\mathbb{Q}[\sqrt{2}]$ car ces propriétés sont héritées de $\mathbb{R}$.
3. **Existence des inverses multiplicatifs** :
   — Soit $x = a + b\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$, avec $x \neq 0$. L'inverse de x dans $\mathbb{Q}[\sqrt{2}]$ est donné par :

$$x^{-1} = \frac{1}{a + b\sqrt{2}} = \frac{1}{a + b\sqrt{2}} \times \frac{a - b\sqrt{2}}{a - b\sqrt{2}} = \frac{a - b\sqrt{2}}{a^2 - 2b^2} = \frac{a}{a^2 - 2b^2} - \frac{b}{a^2 - 2b^2}\sqrt{2}$$

   On a supposé que $x = a + b\sqrt{2} \neq 0$. Comme $\sqrt{2} \notin \mathbb{Q}$ cela implique $a - b\sqrt{2} \neq 0$ donc on a bien le droit de multplier en haut et en bas par le conjugué ainsi on a bien $a^2 - 2b^2 \neq 0$. L'inverse est donc bien dans $\mathbb{Q}[\sqrt{2}]$.
4. **Distributivité** : La distributivité de la multiplication par rapport à l'addition est vérifiée, car elle est héritée de $\mathbb{R}$.

Ainsi, $\mathbb{Q}[\sqrt{2}]$ est un corps car il vérifie tous les axiomes d'un corps.

Exemples :
— $\mathbb{R}, \mathbb{Q}$ sont des corps.
— $\mathbb{Z}/6\mathbb{Z}$ n'est pas un corps car $3 \times 2 = 6 \equiv 0 \bmod 6$. Tous les éléments de $\mathbb{Z}/6\mathbb{Z}$ ne sont pas inversibles pour la multiplication, on dit alors que $\mathbb{Z}/6\mathbb{Z}$ est un **anneau**.

5 Les polynômes

Nous allons maintenant introduire les polynômes sur un corps $\mathbb{K}$ (commutatif). On pourrait introduire les polynômes sur un anneau intègre, mais ce document a pour sujet l'étude des corps finis, donc nous nous limiterons aux polynômes sur un corps.

5.0.1 Définitions

Soit $\mathbb{K}$ un corps. Un **polynôme** à une indéterminée sur $\mathbb{K}$ est une suite infinie $(a_n)_{n\in\mathbb{N}}$ d'éléments de $\mathbb{K}$ telle qu'à partir d'un certain rang, tous les termes a_n soient nuls. Les termes a_n sont appelés les coefficients du polynôme.

Pour comprendre plus concrètement ce qu'est un polynôme, on peut noter un polynôme P à coefficients dans $\mathbb{K}$ en une indéterminée qu'on note X, de la manière suivante :

$$P = \sum_{n=0}^{\infty} a_n X^n$$

avec $a_n \in \mathbb{K}$ pour tout $n \in \mathbb{N}$.

La somme est infinie mais elle a un sens car la suite est nulle à partir d'un certain rang.

On note $\mathbb{K}[X]$ l'ensemble des polynômes à coefficients dans $\mathbb{K}$ en l'indéterminée X.

Exemple : $X^2 + 1$ est un polynôme sur $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{C}$ et $\mathbb{Z}/p\mathbb{Z}$ pour tout p premier, alors que $X^2 + \pi X$ est un polynôme sur $\mathbb{R}$ et $\mathbb{C}$.

On peut maintenant donner la définition du degré d'un polynôme, de la somme et du produit de deux polynômes, ainsi que celle du produit d'un polynôme par un scalaire :
Soient $P = \sum_{n=0}^{\infty} a_n X^n$ et $Q = \sum_{n=0}^{\infty} b_n X^n$ deux polynômes de $\mathbb{K}[X]$ et $h \in \mathbb{K}$.

On note $deg(P) = max\{n \in \mathbb{N} : a_n \neq 0\}$.
Par convention, si $P = 0$, $\deg(P) = -\infty$

On définit le polynôme $P + Q$ de $\mathbb{K}[X]$ par :

$$P + Q = \sum_{n=0}^{\infty} (a_n + b_n) X^n$$

On définit le polynôme hP de $\mathbb{K}[X]$ par :

$$hP = \sum_{n=0}^{\infty} (h a_n) X^n$$

On définit le polynôme $P \times Q$ de $\mathbb{K}[X]$ par :

$$P \times Q = \sum_{n=0}^{\infty} (\sum_{k=0}^{n} a_k b_{n-k}) X^n$$

5.0.2 Quelques propriétés

Tout d'abord, deux polynômes sont différents si et seulement si au moins un des coefficients est différent.

Par ailleurs, on a les propriétés suivantes pour l'addition :

Soient $P, Q, R \in \mathbb{K}[X]$, on a :

1. *Commutativité :* $P + Q = Q + P$.
2. *Associativité :* $P + (Q + R) = (P + Q) + R$.
3. *Élément neutre :* $P + 0 = P$.
4. *Inverse :* $P + (-P) = 0$.
5. *Degré :* $\deg(P + Q) \leq \max\{\deg(P), \deg(Q)\}$ *avec* $\deg(P + Q) = max\{\deg(P), deg(Q)\}$ *si* $\deg(P) \neq \deg(Q)$.

On voit donc $\mathbb{K}[X]$ est un groupe commutatif par la loi $+$.

On a les propriétés suivantes pour la multiplication par un scalaire :

Soient $P, Q \in \mathbb{K}[X]$, soient $h, k \in \mathbb{K}$. On a :

1. *Distributivité par rapport à l'addition de scalaires et de polynômes :* $(h + k)P = hP + kP$ *et* $h(P + Q) = hP + hQ$
2. *"Associativité" :* $h(kP) = (hk)P$.
3. *Élément neutre :* $1P = P$.
4. *Degré :* $\deg(hP) = \deg(P)$ *si* $h \neq 0$

On observe donc que $\mathbb{K}[X]$ muni de l'addition et de la multiplication par un scalaire est un espace vectoriel.

Enfin, on a les propriétés suivantes pour la multiplication de deux polynômes :

Soient $P, Q, R \in \mathbb{K}[X]$. On note e le polynôme $e = 1$. On a :

1. *Commutativité :* $PQ = QP$
2. *Associativité :* $P(QR) = (PQ)R$.
3. *Élément neutre :* $Pe = P$.
4. *Distributivité par rapport à l'addition :* $(P + Q)R = PR + QR$.
5. *Degré :* $\deg(PQ) = \deg(P) + \deg(Q)$

On observe donc que $\mathbb{K}[X]$ muni de l'addition et la multiplication de polynômes est un anneau intègre, c'est-à-dire que c'est un anneau pour lequel un produit de deux éléments non nuls est non nuls.

5.0.3 Liens avec $\mathbb{Z}$

Nous allons maintenant voir les liens entre les polynômes $\mathbb{K}[X]$ et les entiers relatifs $\mathbb{Z}$.

On commence par donner quelques définitions :

Soient $A = \sum_{k=0}^{\infty} a_k X^k, B \in \mathbb{K}[X]$.

— B est un **diviseur** de A s'il existe un polynôme $Q \in \mathbb{K}[X]$ tel que $A = QB$.
— A est **constant** si $a_k = 0$ pour tout $k \geq 1$.
— A de degré $n \in \mathbb{N}$ est **unitaire** si $a_n = 1$.
— B est un **facteur** de A si B est un polynôme unitaire qui divise A et si $1 \leq deg(B) \leq deg(A) - 1$.
— A est **irréductible** si $\deg(A) \geq 1$ et A n'a pas de facteurs.

On peut déjà remarquer que le groupe des polynômes inversibles est l'ensemble des polynômes constants non nuls car on travaille sur un corps. Par ailleurs, tout polynôme peut s'écrire comme le produit d'un polynôme unitaire et d'un polynôme constant.

De plus on peut faire une division euclidienne d'un polynôme par un autre, comme on peut faire la division euclidienne entre deux entiers relatifs :

Division euclidienne : Soient $A, B \in \mathbb{K}[X]$ avec B non nul.
Il existe un unique couple $(Q, R) \in \mathbb{K}[X]^2$ tel que :

$$\begin{cases} A = QB + R \\ \deg(R) < \deg(B) \end{cases}$$

On appelle quotient le polynôme Q et reste le polynôme R.

Enfin, un polynôme unitaire peut être factorisé en un unique produit de polynômes irréductibles unitaires, tout comme un entier relatif peut être factorisé en un unique produit de nombres premiers, à l'ordre près :

Soit $P \in \mathbb{K}[X]$ un polynôme unitaire avec $\deg(P) \geq 1$. Alors :

$$P = \prod_{i=1}^{k} A_i$$

où les $A_i \in \mathbb{K}[X]$ sont des polynômes irréductibles unitaires.

On montre l'existence ainsi : si P est irréductible, alors P est bien un produit d'un polynôme irréductible unitaire. Sinon, P est un produit de deux facteurs, qui sont à leur tour irréductibles ou produit de deux facteurs. Puisque $\deg(P)$ est fini et que le degré de chaque facteur baisse d'au moins un, ce processus se termine après un nombre fini d'étapes.
Par ailleurs, on montre l'unicité de cette décomposition par l'absurde :
On prend m le plus petit entier tel qu'il existe un polynôme unitaire de degré m qui se décompose de deux manières différentes :

$$P = \prod_{i=1}^{k} A_i = \prod_{i=1}^{j} B_i$$

avec $j, k \geq 1$ et A_i et B_i des polynômes irréductibles unitaires. Alors A_1 ne peut pas apparaitre dans la factorisation de droite, sinon on pourrait factoriser les produits des deux côtés par A_1, et m ne serait pas le plus petit entier pour lequel il existe un polynôme unitaire de degré m qui se décompose de deux manières différentes. De même, B_1 ne peut pas apparaitre dans la factorisation de gauche. Sans perte de généralité, on suppose $\deg(B_1) \leq \deg(A_1)$. On peut donc faire la division euclidienne de A_1 par B_1 : $A_1 = QB_1 + R$. Puisque A_1 est irréductible, $R \neq 0$ et $0 \leq \deg(R) < \deg(B_1) \leq \deg(A_1)$. Ainsi, R a une décomposition en facteurs irréductibles $R = \beta R_1 ... R_n$ où β est le coefficient dominant de R, et R_i les facteurs irréductibles de la décomposition (il peut ne pas y avoir de R_i dans la décomposition en facteurs irréductibles, si $deg(R) = 0$). Alors B_1 n'est diviseur d'aucun des R_i, car B_1 est de plus grand degré.
On a donc :
$P = (QB_1 + \beta R_1 ... R_n) \prod_{i=2}^{k} A_i = \prod_{i=1}^{j} B_i$
Où, en définissant $P' = \prod_{i=1}^{n} R_i \prod_{i=2}^{k} A_i$ et en réarrangeant les termes,

$$\tilde{P} = \prod_{i=1}^{n} R_i \prod_{i=2}^{k} A_i = \beta^{-1} B_1 (\prod_{i=2}^{j} B_i - Q \prod_{i=2}^{k} A_i)$$

$\tilde{P}$ est unitaire car c'est un produit de polynôme unitaire. Alors, $\deg(P') < \deg(P)$ car $\deg(R) < \deg(A_1)$ et il a deux factorisations différentes, avec B_1 facteur dans l'une des deux, mais B_1 diviseur d'aucun des facteurs dans l'autre. Ainsi m n'est pas le plus petit entier pour lequel il existe un polynôme unitaire qui se décompose de deux manières différentes. Contradiction, donc la décomposition en facteurs irréductibles est unique.

5.1 Construction d'un corps à p^m éléments

On va maintenant voir comment construire un corps à p^m éléments, avec p un nombre premier et $m \geq 1$ un entier. On construira un corps à $3^2 = 9$ éléments pour avoir un exemple de cette construction.

5.1.1 Recherche de polynômes irréductibles unitaires

Pour construire un corps avec p^m éléments, il faut trouver un polynôme unitaire irréductible de degré m dans le corps $\mathbb{Z}/p\mathbb{Z}$. On peut le trouver en faisant la liste des polynômes de degré m dans ce corps, et en éliminant les polynômes qui ont des facteurs.

Exemple : On cherche un polynôme irréductible unitaire $P \in \mathbb{Z}/3\mathbb{Z}$:
Aucun polynôme de degré 1 n'a de facteurs, donc tous les polynômes unitaires de degré 1 sont irréductibles, c'est à dire x , $x + 1$ et $x + 2$.
Ensuite on élimine les polynômes qui ont des facteurs, c'est à dire :

$$x^2 = x \times x$$
$$x^2 + x = x(x + 1)$$
$$x^2 + 2x = x(x + 2)$$
$$x^2 + 2x + 1 = (x + 1) \times (x + 1)$$
$$x^2 + 2 = (x + 1)(x + 2)$$
$$x^2 + x + 1 = (x + 2) \times (x + 2)$$

Ainsi, les trois polynômes unitaires de degré 2 qui restent, c'est-à-dire $x^2 + 2x + 2$, $x^2 + x + 2$ et $x^2 + 1$ sont irréductibles unitaires.

$\times$	0	1	2	X	$X+1$	$X+2$	$2X$	$2X+1$	$2X+2$
0	0	0	0	0	0	0	0	0	0
1	0	1	2	X	$X+1$	$X+2$	$2X$	$2X+1$	$2X+2$
2	0	2	1	$2X$	$2X+2$	$2X+1$	X	$X+2$	$X+1$
X	0	X	$2X$	2	$X+2$	$2X+2$	1	$X+1$	$2X+1$
$X+1$	0	$X+1$	$2X+2$	$X+2$	$2X$	1	$2X+1$	2	X
$X+2$	0	$X+2$	$2X+1$	$2X2$	1	X	$X+1$	$2X$	2
$2X$	0	$2X$	X	1	$2X+1$	$X+1$	2	$2X+2$	$X+2$
$2X+1$	0	$2X+1$	$X+2$	$X+1$	2	$2X$	$2X+2$	X	1
$2X+2$	0	$2X+2$	$X+1$	$2X+1$	X	2	$X+2$	1	$2X$

TABLE 1 – Table de multiplication de $\mathbb{K}_{X^2+1}$

5.1.2 Construction du corps

Pour construire un corps à p^m éléments, on prend le reste de la division euclidienne $R_{\mathbb{Z}/p\mathbb{Z},m}$ d'un polynôme $A \in \mathbb{Z}/p\mathbb{Z}[X]$ par un polynôme irréductible unitaire $P \in \mathbb{Z}/p\mathbb{Z}[X]$ de degré m, en supposant qu'il en existe un. On prend l'addition et la multiplication de deux polynômes mod(P). Alors, $R_{\mathbb{Z}/p\mathbb{Z},m}$ est effectivement de cardinal p^m.
Nous allons maintenant montrer que c'est bien un corps, qu'on va noter $\mathbb{K}_P$.
L'associativité, la commutativité, la distributivité et l'inversibilité de l'addition sont vérifiées mod(P) car elles sont vérifiées pour $\mathbb{Z}/p\mathbb{Z}[X]$. L'élément neutre pour l'addition est évidemment $E_+ = 0$ et l'élément neutre pour la multiplication est $E_\times = 1$. Enfin, on va montrer la propriété de permutation pour montrer que $(R^*_{\mathbb{Z}/p\mathbb{Z},m}, \times)$ est un groupe. Soit trois polynômes $R, S, T \in R_{\mathbb{Z}/p\mathbb{Z},m}$ avec $S \neq T$ et $R \neq 0$.

$$S \neq T \Leftrightarrow S - T \neq 0$$

Comme P est irréductible, il n'a pas de facteur, donc $R(S-T) \neq P = 0 \bmod(P)$ et comme $R \neq 0$, $R(S-T) \neq 0$. On obtient donc :

$$R(S-T) \neq 0 \Leftrightarrow RS - RT \neq 0 \Leftrightarrow RS \neq RT$$

par distributivité de l'addition.
Ainsi, comme $RS \neq RT$ pour $S \neq T$ et $R \neq 0$, $R \times R^*_{\mathbb{Z}/p\mathbb{Z},m} = \{R \times S : S \in R^*_{\mathbb{Z}/p\mathbb{Z},m}\} = R^*_{\mathbb{Z}/p\mathbb{Z},m}$, donc on a la propriété de permutation donc $(R^*_{\mathbb{Z}/p\mathbb{Z},m}, \times)$ est un groupe et $\mathbb{K}_P$ est effectivement un corps.

Exemple : On va construire le corps $\mathbb{K}_9$ de cardinal 9 : On choisit le polynôme irréductible unitaire de degré 2, $P = x^2 + 1 \in \mathbb{Z}/3\mathbb{Z}[X]$
On peut ainsi déterminer les tables d'addition et de multiplication $mod(P)$, et comme la table d'addition est facile à obtenir, on a la table 1 de multiplication $mod(P)$ suivant :

5.2 Le groupe multiplicatif $\mathbb{F}_q^*$

Dans cette section, nous étudierons le groupe multiplicatif $\mathbb{F}_q^*$, sa nature cyclique, ainsi que la décomposition de ses éléments pour mieux comprendre la structure des corps finis.

5.2.1 Les élements primitifs de $\mathbb{F}_q$

Un élément primitif d'un corps fini $\mathbb{F}_q$ est un élément β qui engendre tout le groupe multiplicatif $\mathbb{F}_q^*$. Alors il engendre le sous-groupe cyclique $\{\beta^k : k \in \{0, 1, 2, \cdots, q-2\}\} \subset \mathbb{F}_q$. On peut aussi engendrer des autres sous-groupes, plus petits, engendrés par des éléments nonprimitifs. Comme on a déjà vu, le théorème de Lagrange nous montre que l'ordre de chacun de ces sous-groupes cycliques divise $q-1 = |\mathbb{F}_q^*|$, et on a la relation :

$$\sum_{d:d|(q-1)} \varphi(d) = q-1$$

De plus, il y a au moins $\varphi(q-1) \geq 1$ éléments d'ordre $q-1$, alors l'élément primitif existe. Alors $\mathbb{F}_q^*$ est un groupe cyclique.

Maintenant vérifions que la structure de $\mathbb{F}_q^*$ est bien cyclique en montrant que chaque élément non nul du corps est une racine du polynôme $x^q - x$, ce qui permet de conclure que le groupe multiplicatif est entièrement décrit par les *racines n-ièmes de l'unité*. Pour cela, analysons la décomposition de $x^q - x$ en facteurs irréductibles.

5.2.2 Les racines des polynômes

Soit $\mathbb{F}[x]$ l'ensemble des polynômes sur un corps arbitraire $\mathbb{F}$. Si $f(x) \in \mathbb{F}[x]$ possède un facteur $x - \alpha$ avec $\alpha \in \mathbb{F}$, alors α est une racine de $f(x)$. D'un autre côté, si $f(\alpha) = 0$ pour un $\alpha \in \mathbb{F}$, alors α est une racine de $f(x)$.

Comme la décomposition en polynômes irréductibles d'un polynôme est unique, et le degré d'un polynôme est égal à la somme des degrés de ses facteurs, on a le théorème suivant :

Le théorème sur les racines

Sur tout corps $\mathbb{F}$, un polynôme unitaire $f(x) \in \mathbb{F}[x]$ quelconque de degré m ne peut avoir plus de m racines dans $\mathbb{F}$. Si $f(x)$ a m racines $\{\beta_0, \beta_1, \ldots, \beta_{m-1}\}$, alors sa factorisation unique est donnée par :

$$f(x) = (x - \beta_0)(x - \beta_1) \cdots (x - \beta_{m-1}).$$

De plus, si le corps a un sous-groupe cyclique d'ordre n, les racines sont de la forme $\{1, \beta, \beta^2, \cdots, \beta^{n-1}\}$ avec $\beta^n = 1$, alors :

$$(\beta^k)^n = (\beta^n)^k = 1^k = 1$$

pour tout $k \in \{0, 1, ..., n-1\}$, alors le polynôme $x^n - 1$ dans cette groupe s'écrit comme :

$$x^n - 1 = (x-1)(x-\beta) \cdots (x - \beta^{n-1}).$$

Le dernier est une généralisation des **racines n-ièmes de l'unité**. Pour améliorer l'intuition en plus, prenons le produit et le développons :

$$\prod_{0 \leq k \leq n-1} (x - \beta^k)$$

Comme on a n facteurs avec l'indéterminée x et une puissance de la racine primitive β, le produit sera de la forme :

$$x^n + \sum_{0 \leq k \leq n-1} (-1)^{n-k} \sigma_{n-k} x^k$$

Notre but maintenant est de trouver l'expression de σ_i et montrer que $\sigma_n = (-1)^{n+1}$ et $\sigma_i = 0$ pour tout $1 \leq i < n$ qui nous permetra de déduire que le produit est, en fait, égal à $x^n - 1$.

Pour déterminer σ_{n-k}, on considère le coefficient de x^k dans le développement du produit. Cela revient à sélectionner k termes x parmi les n facteurs et les $n-k$ termes restants sous forme des racines β^i. La somme σ_{n-k} regroupe donc tous les produits possibles de $n-k$ racines, soit :

$$\sigma_{n-k} = \sum_{0 \leq j_1 < j_2 < \cdots < j_{n-k} \leq n-1} \beta^{j_1}\beta^{j_2}\cdots\beta^{j_{n-k}}.$$

Cependant, en utilisant la propriété fondamentale $\beta^n = 1$, chaque produit de racines $\beta^{j_1}, \beta^{j_2}, \ldots, \beta^{j_{n-k}}$ se trouve annulé par un produit symétrique opposé dans la somme totale. Cela provient du fait que pour tout produit $\beta^{j_1}\beta^{j_2}\cdots\beta^{j_{n-k}}$, il existe un autre produit $\beta^{n-j_1}\beta^{n-j_2}\cdots\beta^{n-j_{n-k}}$ tel que leur somme est nulle. La seule exception se produit lorsque $j_i = 0$, car dans ce cas, $n - 0 = n$ et $\beta^n = 1 = \beta^0$. Toutefois, nous ne prenons qu'une seule occurrence de ce cas dans la somme, car j_i varie de 0 à $n-1$, excluant ainsi n. Par conséquent, bien qu'il n'existe pas d'élément opposé pour β^0 dans ce contexte, la simplification par annulation reste valide. Cela s'explique par le fait que multiplier un produit par 1 (lorsque β^0 est présent) ne modifie pas la valeur du produit, et donc l'annulation générale des termes dans la somme reste inchangée. Par conséquent, on a :

$$\sigma_{n-k} = 0, \quad \text{pour tout } 1 \leq k \leq n-1.$$

Le cas spécifique est $k = n$.

Pour n impair, les racines distinctes forment des paires (β^i, β^{n-i}), avec $\beta^i \cdot \beta^{n-i} = \beta^n = 1$. Ainsi, le produit total est :

$$\prod_{i=0}^{n-1} \beta^i = 1,$$

ce qui correspond à $(-1)^{n+1} = 1$, car $n+1$ est pair.

Pour n pair, les racines forment des paires similaires, sauf $\beta^{n/2}$, qui reste seule. Puisque $(\beta^{n/2})^2 = \beta^n = 1$, on a $\beta^{n/2} = -1$ (les racines étant distinctes et $\beta^0 = 1$). Le produit total devient donc :

$$\prod_{i=0}^{n-1} \beta^i = (-1),$$

ce qui correspond à $(-1)^{n+1} = -1$, car $n+1$ est impair.

En conclusion, pour tout n, le produit des racines est donné par :

$$\prod_{i=0}^{n-1} \beta^i = (-1)^{n+1}.$$

Donc, on obtient bien ce qui est attendu. □

Mainenant reprenons le cas où $n = q-1$. Alors pour touS $\beta \in \mathbb{F}_q^*$, $\beta^{q-1} = 1$ et $|\langle\beta\rangle| \mid (q-1)$. Alors :

$$x^q - x = x(x^{q-1} - 1) = x \prod_{\beta \in \mathbb{F}_q^*} (x - \beta) = \prod_{\beta \in \mathbb{F}_q} (x - \beta)$$

Exemple : Considérons le corps $\mathbb{F}_4$, mod.2 (on verra prochainement que dans ce cas, 2 est la *caractéristique* de $\mathbb{F}_4$). Ses éléments sont $0, 1, \alpha, \alpha+1$, où $\alpha^2 = \alpha + 1$. Vérifions que $x^{4-1} - 1 = (x-1)(x-\alpha)(x-(\alpha+1))$:

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

Alors, $\alpha+(\alpha+1)+1 = 2\alpha+2 = 0$, $\alpha(\alpha+1)+\alpha+(\alpha+1) = \alpha^2+\alpha+\alpha+\alpha+1 = (\alpha+1)+3\alpha+1 = 4\alpha+2 = 0$, et $-\alpha(\alpha+1) = -(\alpha^2+\alpha) = -1 = 1$.

Donc, $(x-1)(x-\alpha)(x-(\alpha+1)) = x^3-1$. Ainsi, on a vérifié la décomposition et les formules de σ aussi. □

Pour conclure, la décomposition de $x^{q-1}-1$ en facteurs linéaires met en évidence la structure cyclique du groupe multiplicatif $\mathbb{F}_q^*$. Cela illustre également le rôle fondamental des éléments primitifs dans la compréhension des propriétés algébriques des corps finis.

5.3 Isomorpismes entre les corps

Dans cette partie on montrera que chaque corps $\mathbb{F}_q$ est isomorphique au corps $\mathbb{F}_{g(x)}$ polynomial qu'on a construit dans la partie précédente, particulièrement de cardinal p^m.

La *caractéristique* d'un corps $\mathbb{F}$ est le plus petit entier positif p tel que la somme de p fois l'unité multiplicative 1 soit égale à 0. Si un tel entier n'existe pas, le corps est de caractéristique 0. Par exemple, $\mathbb{F}_p$ est de caractéristique p, tandis que $\mathbb{Q}$ est de caractéristique 0.

5.3.1 Décomposition de $x^q - x$ dans $\mathbb{F}_p$

On a montré dans la partie précédente la décomposition du polynôme $x^q - x$ en facteurs irréductibles, et comme $\mathbb{F}_q^*$ est cyclique, tous ses facteurs sont de degré 1. Maintenant prenons le sous-groupe $\mathbb{F}_p \subset \mathbb{F}_q$ où p est la *caractéristique* de q. Cette fois, comme $|\mathbb{F}_q| \geq |\mathbb{F}_p|$, pas tous les éléments de $\mathbb{F}_q$ seront aussi de $\mathbb{F}_p$, mais ceux qui sont, seront aussi les éléments de $\mathbb{F}_q$. Alors, comme le polynôme $x^q - x$ peut être décomposé aux facteurs irréductibles dans $\mathbb{F}_p$, certaines facteurs seront de degré supérieur à un. Alors la décomposition est :

$$x^q - x = \prod_{\beta \in \mathbb{F}_q} (x-\beta) = \prod_i g_i(x).$$

où $g_i(x)$ est un polynôme irréductible dans $\mathbb{F}_p$ pour tout i. Ici,

$$g_i(x) = \prod_{k=1}^{deg(g_i(x))} (x - \beta_{i_k})$$

où β_{i_k} sont quelques éléments de $\mathbb{F}_q$. De tels polynômes $g_i(x)$ irréductibles en $\mathbb{F}_p$ sont appelés les *polynômes minimaux* de $\mathbb{F}_q$. Puisque cette décomposition polynomiale est en facteurs tels que, si $i \neq i'$, alors les zéros de g_i sont disjoints de ceux de $g_{i'}$, chaque β est associé à exactement un unique polynôme minimal de $\mathbb{F}_q$. En fait, on peut montrer facilement que $g(x)$ est un unique polynôme minimal de β, élément de $\mathbb{F}_q$ donnée, car si on suppose qu'il est le plus petit, on trouve que tout autre polynôme n'est pas irréductible ce qui est contraire à notre hypothèse.

Exemple : Le corps $\mathbb{F}_4$ est de cardinal $4 = 2^2$ et donc de caractéristique 2. Le polynôme $x^4 - x$ est décomposé comme suit :

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

dans $\mathbb{F}_4$. Dans $\mathbb{F}_2$, il se décompose comme :

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

Le polynôme $x^2+x+1 = (x-\alpha)(x-\alpha^2)$ (la dernière décomposition dans $\mathbb{F}_4$) est un polynôme minimal et irréductible dans $\mathbb{F}_2$, mais réductible dans $\mathbb{F}_4$.

5.3.2 Construction d'isomorphismes entre corps finis

Changeons maintenant de point de vue et regardons les choses sous l'angle où β est fixé, et où nous considérons une application définie comme suit :

$$\mathbb{F}_p[x] \to \mathbb{F}_q$$

$$f(x) \mapsto f(\beta).$$

et montrons qu'elle est un isomorphisme des corps :

Théorème : Soit $\beta \in \mathbb{F}_q$ et $g(x)$ le polynôme minimal de β sur $\mathbb{F}_p$. L'application

$$m_\beta : \mathbb{F}_p[x] \to \mathbb{F}_q, \quad f(x) \mapsto f(\beta),$$

induit un isomorphisme entre $R_{\mathbb{F}_p,m} = \mathbb{F}_p[x]/(g(x))$ et $\mathbb{G}_\beta = \{f(\beta) \mid f(x) \in \mathbb{F}_p[x]\}$, qui est le sous-corps de $\mathbb{F}_q$ engendré par β.

Preuve : Par la division euclidienne, tout $f(x) \in \mathbb{F}_p[x]$ peut s'écrire sous la forme :

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

En évaluant en β, on obtient $m_\beta(f(x)) = f(\beta) = r(\beta)$, ce qui montre que $m_\beta(\mathbb{F}_p[x]) = \mathbb{G}_\beta$, et que chaque élément de $\mathbb{G}_\beta$ correspond à un polynôme résidu $r(x)$ modulo $g(x)$.

L'injectivité découle du fait que si $m_\beta(f(x)) = m_\beta(h(x))$, alors $f(\beta) = h(\beta)$, et donc $f(x) - h(x)$ est divisible par $g(x)$, ce qui implique $f(x) \equiv h(x) \pmod{g(x)}$.

Enfin, m_β préserve l'addition et la multiplication :

$$m_\beta(r(x) + s(x)) = m_\beta(r(x)) + m_\beta(s(x)) \quad \text{et} \quad m_\beta(r(x)s(x)) = m_\beta(r(x))m_\beta(s(x)).$$

Ainsi, m_β est un isomorphisme entre $R_{\mathbb{F}_p,m}$ et $\mathbb{G}_\beta$, prouvant que $\mathbb{G}_\beta$ est un sous-corps isomorphe à $\mathbb{F}_{g(x)}$, où $g(x)$ est le polynôme minimal de β. □

Finalement on établit le théorème qu'on a attendu :

Théorème (Tout corps fini est isomorphe à un corps $\mathbb{F}_{g(x)}$)
Tout corps fini $\mathbb{F}_q$ de caractéristique p avec q éléments est isomorphe à un corps de restes polynomiaux $\mathbb{F}_{g(x)}$, où $g(x)$ est un polynôme irréductible de degré m dans $\mathbb{F}_p[x]$. Par conséquent, $q = p^m$ pour un entier positif m.

Preuve : Si $g(x)$ est un polynôme irréductible dans $\mathbb{F}_p[x]$ de degré m, alors l'arithmétique modulo $g(x)$ forme un corps $\mathbb{F}_{g(x)}$ avec p^m éléments. Dans ce corps, le polynôme résidu x est un élément de $\mathbb{F}_{g(x)}$. Clairement, $g(x)$ s'annule en β (c'est-à-dire $g(\beta) = 0$), mais $r(\beta) \neq 0$ si $\deg(r(x)) < m$. Ainsi, $g(x)$ est le polynôme minimal de β.

De plus, comme $\beta^{p^m-1} = 1$, β est une racine de $x^{p^m-1} - 1$. Cela implique que $g(x)$ divise $x^{p^m-1} - 1$, et donc $g(x)$ divise également $x^{p^m} - x$.

Donc, par le théorème précédent, chaque polynôme irréductible dans $\mathbb{F}_p[x]$ correspond à une unique valeur de $f(\beta) \in \mathbb{G}_\beta$. De plus, comme $g(\beta) = 0$ et que $\mathbb{F}_q$ est un corps des polynômes modulo $g(x)$ dans $\mathbb{F}_p[x]$, chaque racine de $g(x)$ correspond à un unique polynôme minimal dans $\mathbb{F}_q$, et chaque polynôme minimal dans $\mathbb{F}_q$ correspond à au moins une racine de $g(x)$. Enfin, puisque $g(x)$ est de degré m et que le groupe multiplicatif $\mathbb{F}_q^*$ est cyclique, $g(x)$ possède exactement m racines, qui correspondent à m polynômes minimaux.

Cela montre que tout corps de taille p^m inclut m éléments dont les polynômes minimaux divisent $x^{p^m} - x$. Par conséquent, cette propriété est en accord avec le théorème au-dessus, qui affirme que tous les corps finis de taille p^m sont isomorphes. □

Ces théorème établit que tout corps fini $\mathbb{F}_q$, où $q = p^m$, est isomorphe à un corps $\mathbb{F}_{g(x)}$ construit à partir d'un polynôme irréductible $g(x)$ de degré m sur $\mathbb{F}_p$. De plus, il montre que tous les corps finis de même taille p^m sont isomorphes entre eux, ce qui complète la classification des corps finis.

6 Conclusion

Dans ce document, nous avons vu comment créer des corps finis à p^m éléments, grâce à la modulation par un nombre premier et à un polynôme unitaire irréductible de degré m. Cependant, la question se pose de démontrer l'existence d'un tel polynôme. La preuve peut être trouvée dans le premier document de la bibliographie, chapitre 7.9.

De plus, nous avons posé des questions sur la méthode permettant de trouver les polynômes irréductibles. Bien qu'il n'existe pas de méthodes universelles pour tous les cas, il y a quelques techniques décrites dans le livre *Finite Fields* de Rudolf Lidl et Harald Niederreiter, pages 96 à 98.

Enfin, il reste à explorer les applications concrètes de cette théorie en théorie des codes.

7 Bibliographie

— https://tinyurl.com/mr4aurj7
— https://fr.wikipedia.org/wiki/Ensemble
— https://fr.wikipedia.org/wiki/Racine_de_l'unit%C3%A9
— https://tinyurl.com/5b9te7xa
— https://fr.wikipedia.org/wiki/Indicatrice_d'Euler
— https://progresser-en-maths.com/theoreme-de-lagrange-enonce-et-demonstration/
— https://progresser-en-maths.com/cours-indicatrice-d-euler/
— Cours de MPSI de Monsieur Poiret sur les "Polynômes en une indéterminée"
— Algèbre et probabilité de Xavier Gourdon