# Mathematical Tools For Cryptography

Written by HADIOUCHE Azouaou.

## Disclaimer

This document contains the lectures given by Dr.ZAIMI.

> Some contents were added as remainders and extras for the students.
> To seperate the contents of the course to actual additions or out of context information, a black band will be added by its side like the one englobing this comment.

## Contents

Chapter 0

# Remainders

This part will just be a remainder of the important definitions, propositions and theorems of the field extension course that are needed for this course. We assume that rings in this case are commutative rings with unity.

## 0.1. Rings & Homomorphisms

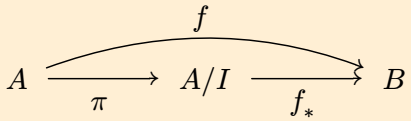
**Definition 0.1.1 (Ring Homomorphism/Kernel/Image)**: *Let $R, R'$ be two rings and $f : R \to R'$ a map. We say that $f$ is a ring homomorphism if*

$$f(a+b) = f(a) + f(b). \qquad f(ab) = f(a)f(b).$$

*define* $\operatorname{Ker} f = f^{-1}(\{0\})$ *and* $\operatorname{Im} f = f(R)$.

**Proposition 0.1.2**: *Let $f : R \to R'$ be a ring homomorphism*
- $\operatorname{Ker} f$ *is an ideal of* $R$ *and* $\operatorname{Im} f$ *is a subring of* $R'$.
- $\operatorname{Ker} f = \{0\} \Leftrightarrow f$ *injective and* $\operatorname{Im} f = R' \Leftrightarrow f$ *surjective.*
- *If* $R, R'$ *are fields then* $f \equiv 0$ *or* $f(1) = 1$.

**Theorem 0.1.3 (First Isomophism Theorem)**: *Let $f : A \to B$ be a ring homomorphism, then* $\operatorname{Im} f \cong A/\operatorname{Ker} f$ *and for* $I \subseteq \operatorname{Ker} f$ *is an ideal then there exists a unique isomorphism* $f_* : A/I \to B$, $f_*(x+I) = f(x)$ *with* $f = f_* \circ \pi$ *and* $\pi(x) = x + I$ *the cannonical surjection.*




## 0.2. Ideals, UFDs, PIDs & EDs

**Definition 0.2.4 (Elements)**: *Let $R$ be a ring, we have the following:*
- ***Unit:*** $x \in R$ *is a unit if* $\exists y \in R, xy = 1$, *denoted* $R^*$.
- ***Zero Divisor:*** $x \in R \setminus \{0\}$ *is a zero divisor if* $\exists y \in R, xy = 0$.
- ***Irreducible:*** $x \in R$ *is irreducible if* $x = x_1 x_2 \Rightarrow x_1 \in R^* \vee x_2 \in R^*$.

**Definition 0.2.5 (Ideals)**: *Let $R$ be a ring, $I \subseteq R$ ideal, we have:*
- ***Prime Ideal:*** $I$ *is prime if* $\forall a, b \in R, ab \in I \Rightarrow a \in I \vee b \in I$.
- ***Principal Ideal:*** $I$ *is principal if* $\exists x \in R, I = (x) = xR$.
- ***Maximal Ideal:*** $I$ *is maximal if* $\forall M$ *ideal*, $I \subseteq M \subseteq R \Rightarrow M = I$ *or* $R$.

**Proposition 0.2.6**: *Let $f : R \to R'$ be a ring homomorphism and let $I'$ be an ideal of $R'$ then $I = f^{-1}(I')$ is an ideal of $R$, if $I'$ is prime then $I$ is prime.*

**Theorem 0.2.7**: *Let $R$ be a ring and $I, J$ ideals of $R$*
- $I$ *is a prime ideal* $\Leftrightarrow R/I$ *is an integral domain.*
- $I$ *is a maximal ideal* $\Leftrightarrow R/I$ *is a field.*
- *if* $I \subseteq J$ *then* $(A/I)/(J/I) \cong A/J$.

**Definition 0.2.8 (Domains)**: *Let $R$ be a ring, we have the following:*
- ***Integral Domain:*** $R$ *is an integral domain if* $xy = 0 \Rightarrow x = 0$ *or* $y = 0$.
- ***Principle Ideal Domain:*** $R$ *is a PID if for any ideal $I$ in $R$, $I$ is principle.*
- ***Euclidean Domain:*** $R$ *is said to be an ED if* $\exists \nu : R/\{0\} \to \mathbb{N}$ *a valuation function,* $\forall a, b \in R, \exists q, r \in R, a = bq + r, r = 0$ *or* $\nu(r) < \nu(b)$.
- ***Unique Factoriation Domain:*** $R$ *is a UFD if any element can be decomposed into a unique product of irreducible elements.*

**Theorem 0.2.9**:
- *If $R$ is a UFD and $x \in R$ is irreducible, then $(x)$ is prime.*
- *If $R$ is an integral domain and a PID, every prime ideal is maximal.*
- *ED $\Rightarrow$ PID $\Rightarrow$ UFD.*

## 0.3. Ring Of Polynomials

**Definition 0.3.10 (Ring Of Polynomials)**: *Let $R$ be a ring, we define*

$$R[X] = \left\{ \sum_{i \in I} a_i X^i \mid I \text{ finite}, \{a_i\}_{i \in I} \subseteq R \right\}.$$

*to be the ring of polynomials on $R$, and for any $P \in R[X]$ we set*

$$\deg P = \max\{i \in \mathbb{N} \mid X^i \text{ has a non-zero coefficent in } P\}.$$

**Definition 0.3.11 (Polynomials)**: *Let $L/K$ be a field extension and $P \in K[X]$*
- ***Minimal:*** *$P$ is the minimal polynomial of $\alpha \in L$ if it is the unique monic polynomial with the smallest degree which vanishes at $\alpha$ denoted $\mathrm{Irr}(\alpha, K, x)$.*

**Proposition 0.3.12**: *Let $K$ be a field, $P(X) \in K[X]$ with $\deg P \in \{2, 3\}$ then we have that $P$ is reducible over $K \Leftrightarrow P$ has a zero in $K$.*

**Theorem 0.3.13**: *Let $R$ be a ring*
- *$R$ is an integral domain $\Rightarrow R[X]$ is an integral domain.*
- *$P = \sum a_i X^i$ is a unit in $R[X] \Leftrightarrow a_0 \in R^*$ and $\forall i \geq 1, a_i$ nilpotent.*
- *$P \in R[X]$ irreducible $\Rightarrow R[X]/(P) = \left\{ \sum_{i=0}^{\deg P - 1} a_i \alpha^i \mid a_i \in R \right\}$.*
- *Let $\alpha$ a root of $P \in R[X]$ then $\mathrm{Irr}(\alpha, K, X)$ divides $P$.*
- *if $R$ is a field, $R[X]$ is a Euclidean domain with the valuation $\nu(P) = \deg P$.*

**Proposition 0.3.14 (Eisenstein's Criterions)**:
- *Let $P(x) = a_0 + a_1 x + ... + a_n x^n \in \mathbb{Z}[X]$, if there is a prime $p$ such that $p \mid a_0, ..., p \mid a_{n-1}, p^2 \nmid a_0$ and $p \nmid a_n$ then $P$ is irreducible over $\mathbb{Q}[X]$.*
- *Let $P(X) \in \mathbb{Z}[X]$ and $\varphi : \mathbb{Z}[X] \to \mathbb{Z}_{n[X]}$ the extension of $k \mapsto k \bmod n$, if $\deg \varphi(P) = \deg P$ and $\varphi(P)$ is irreducible in $\mathbb{Z}_{n[X]}$ then $P$ is irreducible in $\mathbb{Q}[X]$.*

## 0.4. Field Extensions

**Definition 0.4.15 (Extension/Degree Of Extension)**: *Let $L, K$ be two fields such that $K \subseteq L$, we call $L$ a field extension of $K$ and we denote it $L/K$, we define the degree of extension of $L$ on $K$ as $\dim_K L$ if it is finite and $+\infty$ if it is infinite, and we denote it $[L : K] = \dim_K L$*

**Definition 0.4.16 (Characteristic)**: *we define the characteristic of $K$ to be the smallest $n$ such that $1 + 1 + ... + 1 = 0$ $n$ times, denoted $\mathrm{Char}\, K = n$, if $n$ does not exist then we say that $\mathrm{Char}\, K = 0$.*

**Definition 0.4.17 (Elements)**: *Let $K$ be a field and $x \in K$.*
- ***Algebraic:*** *$x$ is said to be algebraic if $\exists P \in K[X], \deg P > 0, P(x) = 0$.*
- ***Transcendental:*** *$x$ is said to be transcendental if it is not algebraic.*
- ***Conjugate:*** *$\alpha$ is said to be the conjugate of $\beta$ if $\beta$ is a root of $\mathrm{Irr}(\alpha, K, x)$.*

**Proposition 0.4.18**:
- *If $\alpha, \beta$ are conjugates then $\mathrm{Irr}(\alpha, K, X) = \mathrm{Irr}(\beta, K, X)$.*
- *If $L/K$ then $\mathrm{Char}\, L = \mathrm{Char}\, K$.*
- *if $K$ is a field then $\mathrm{Char}\, K$ is prime.*

**Definition 0.4.19 (Fields)**: *Let $K$ be a field*

- ***Algebraically Closed:*** *$K$ is said to be algebraically closed if any algebraic extension of $K$ is $K$.*

**Definition 0.4.20 (Extensions)**:

- ***$L/K$ Algebraic Extension:*** *$\forall x \in L$, $x$ is algebraic over $K$.*
- ***$L/K$ Transcendental Extension:*** *if it is not an algebraic extension.*
- ***Algebraic Closure:*** *$\overline{K}$ is an algebraic closure of $K$ if $\overline{K}/K$ is an algebraic extension and $\overline{K}$ is algebraically closed.*

**Theorem 0.4.21**: *Let $L/K$ be a field extension and $\alpha_1, ..., \alpha_n \in L$ and set $\alpha = (\alpha_1, ..., \alpha_n)$ then*

- *$K[\alpha_1][\alpha_2]...[\alpha_n] = K[\alpha_1, ..., \alpha_n] = \{P(\alpha) \mid P \in K[X_1, ..., X_n]\}$ is the smallest ring containing $K$ and $\alpha_1, ..., \alpha_n$.*
- *$K(\alpha_1)(\alpha_2)...(\alpha_n) = K(\alpha_1, ..., \alpha_n) = \{P(\alpha)/Q(\alpha) \mid P, Q \in K[X_1, ..., X_n], Q(\alpha) \neq 0\}$ is the smallest field containing $K$ and $\alpha_1, ..., \alpha_n$.*
- *any extension of finite degree is algebraic.*

**Theorem 0.4.22 (Steinitz)**:

1. *Any field is contained inside of an algebraically closed field.*
2. *Any two algebraic closures of a field are isomorphic.*

Chapter 1

# Embeddings

Consider in this chapter, $K, L, E, \Omega$ denote fields, the lower-case elements are used for elements of fields.

## 1.1. Embedding

**Definition 1.1.1 (Embedding)**: *Let $\sigma : K \to L$ a homomorphism, if $\sigma \not\equiv 0$ then $\sigma$ is an embedding from $K$ to $L$.*

**Definition 1.1.2 (Extension/Restriction)**: *Suppose $E$ is an extension of $K$, $\tau$ is an embedding of $E$ into $L$ such that $\forall k \in K, \tau(k) = \sigma(k)$, then $\tau$ is called an extension $\sigma$ and $\sigma$ is called a restriction of $\tau$ to $K$. Moreover if $\sigma = \mathrm{Id}_K$ then $\tau$ is called a $K$-embedding of $E$ into $L$.*

**Example:**

- The unique embedding $\sigma : \mathbb{Q} \to \mathbb{C}$ is the identity, we prove $\sigma(1) = 1$, $\sigma(n) = n$, $\sigma(-n) = -n$, $\sigma(a/b) = \sigma(a)/\sigma(b)$ by induction, then $\sigma = \mathrm{Id}$.
- The embeddings $\tau : \mathbb{Q}\left(\sqrt{2}\right) \to \mathbb{C}$ has only two forms, given that $\tau|_{\mathbb{Q}} = \mathrm{Id}_{\mathbb{Q}}$ then $\tau\left(a + b\sqrt{2}\right) = a + b\tau\left(\sqrt{2}\right)$ and since $\tau\left(\sqrt{2}\right)^2 = \tau\left(\sqrt{2}^2\right) = \tau(2) = 2 \Rightarrow \tau(\alpha) = \sqrt{2}$ or $\tau(\alpha) = -\sqrt{2}$.

**Proposition 1.1.3**: *Let $\tau$ be a $K$-embedding of $L$ into $E$ where $K \subseteq L$ and let $\alpha \in L$ be algebraic over $K$, then $\tau(\alpha)$ is a conjugate of $\alpha$ over $K$.*

*Proof.* Suppose $\alpha$ algebraic of degree $d$ over $K$ and let $P = \mathrm{Irr}(\alpha, K, x)$, we have $P(\alpha) = 0$ and $\tau(P(\alpha)) = \tau(\sum k_i \alpha^i) = \sum \tau(k_i)\tau(\alpha)^i = \sum k_i \tau(\alpha)^i = P(\tau(\alpha)) = 0$ then $\tau(\alpha)$ is a conjugate of $\alpha$. □

We used the fact that $\tau$ is a $K$-embedding in the evaluation $\tau(k_i) = k_i$.

**Proposition 1.1.4**: *Let $K$ be a field, $\overline{K}$ an algebraic closure of $K$, $\alpha \in \overline{K}$ and let $\beta \in \overline{K}$ be a conjugate of $\alpha$ over $K$, then there is a $K$-embedding $\tau : K(\alpha) \to \overline{K}$ which is a $K$-isomorphism of $K(\alpha)$ into $K(\beta)$ sending $\alpha$ to $\beta$.*

> ***Proof Outline:***
> 1. $P(X) = \mathrm{Irr}(\alpha, K, X) = \mathrm{Irr}(\beta, K, X)$ since they are conjugates.
> 2. $K[\alpha] = K(\alpha), K[\beta] = K(\beta)$ since they are algebraic.
> 3. $K(\alpha) \cong K[X]/(P(X)) \cong K(\beta)$.
> 4. Construct using those isomorphisms a map that keeps $K$ invariant.

*Proof.* Let $\alpha, \beta$ conjugates over $K$, then we have that $\mathrm{Irr}(\alpha, K, X) = \mathrm{Irr}(\beta, K, X)$. Define $I = (\mathrm{Irr}(\alpha, K, X))$, $\nu_\alpha : K[X] \to K[\alpha]$ and $\nu_\beta : K[X] \to K[\beta]$ such that $\nu_\alpha(P(X)) = P(\alpha)$ and $\nu_\beta(P(X)) = P(\beta)$ which are surjective by definition. We have that $\mathrm{Ker}(\nu_\alpha) = \mathrm{Ker}(\nu_\beta) = (\mathrm{Irr}(\alpha, K, X))$. From the first isomorphism theorem we have that there exists two isomophisms $(\nu_\alpha)_\star : K[X]/I \to K[\alpha]$ and $(\nu_\beta)_\star : K[X]/I \to K[\beta]$ such that $v_\alpha = (v_\alpha)_\star \circ \pi$ and $v_\beta = (v_\beta)_\star \circ \pi$. We also have that $K[\alpha] = K(\alpha)$ and $K[\beta] = K(\beta)$ since $\alpha, \beta$ are algebraic.

Set $\varphi : K(\alpha) \to K(\beta), x \mapsto \left((v_\beta)_* \circ (v_\alpha)_*^{-1}\right)(x)$, $\varphi$ is the composition of isomophisms then it is an isomorphism, let $x \in K, \varphi(x) = (v_\beta)_*\left((v_\alpha)_*^{-1}(x)\right) = (v_\beta)_*(x + I) = x$ so $\varphi$ is a $K$-isomorphism and $\varphi(\alpha) = (v_\beta)_*\left((v_\alpha)_*^{-1}(\alpha)\right) = (v_\beta)_*(I) = \beta$. □

**Example:** Let $\alpha = \sqrt[3]{2}$ we have $\mathrm{Irr}(\alpha, \mathbb{Q}, X) = X^3 - 2$, the conjugates of $\alpha$ over $\mathbb{Q}$ are $\alpha, j\alpha, j^2\alpha$, there are the following embeddings:

- $\tau_1 : \mathbb{Q}\left(\sqrt[3]{2}\right) \to \mathbb{Q}\left(\sqrt[3]{2}\right)$ which is the identity.
- $\tau_2 : \mathbb{Q}\left(\sqrt[3]{2}\right) \to \mathbb{Q}\left(j\sqrt[3]{2}\right)$ with $\tau_2\left(\sqrt[3]{2}\right) = j\sqrt[3]{2}$ an isomorphism.
- $\tau_3 : \mathbb{Q}\left(\sqrt[3]{2}\right) \to \mathbb{Q}\left(j^2\sqrt[3]{2}\right)$ with $\tau_3\left(\sqrt[3]{2}\right) = j^2\sqrt[3]{2}$ an isomorphism.

so there are exactly three embeddings.

**Corollary 1.1.5**: *Let $\alpha$ be algebraic over $K$ of degree $n$, $\alpha \in \overline{K}$ an algebraic closure of $K$ and let $s$ be the number of distinct conjugates of $\alpha$ over $K$, then there are exactly $s$ embeddings of $K(\alpha)$ into $\overline{K}$ sending $\alpha$ to its distinct conjugates.*

**Proposition 1.1.6**: *Let $L/K$ be an algebraic extension and $\sigma$ a $K$-endomorphism of $L$, then $\sigma$ is surjective.*

> ***Proof Outline:***
> 1. $\sigma$ transforms a conjugate to another.
> 2. the conjugates of an element are finite so $\sigma$ is a bijection.
> 3. $\sigma$ is a permutation thus there is a preimage for any element.

*Proof.* Let $\sigma : L \to L$ a $K$-embedding and $\alpha \in L$. Take $P = \mathrm{Irr}(\alpha, K, X)$ and set $C = \{\beta \in L \mid P(\beta) = 0\}$ so $C$ is the set of conjugates of $\alpha$ over $K$, $\alpha \in C \neq \emptyset$ and $C$ is finite since $P$ has finite roots. For any $\beta \in C, \sigma(\beta) \in C$ since $P(\sigma(\beta)) = \sigma(P(\beta)) = 0$, $\sigma$ is an injection from a finite set to itself so $\sigma(C) = C$ thus $\exists \beta \in C, \sigma(\beta) = \alpha$ so $\sigma$ is surjective. □

# 1.2. Primitive Element Theorem

Let $K$ be a field and $\overline{K}$ an algebraic closure of $K$, and let $\alpha \in \overline{K}$ and $\alpha$ is a zero of $P(X) \in K[X] \setminus \{0\}$, recall that $\alpha$ is said to be a zero of $P$ is $P(X) = (X - \alpha)^m Q(X)$ with $Q \in K[X]$, if $m \geq 2$ we say that $\alpha$ is a repeated zero of $P$, if $m = 1$ we say that $\alpha$ is a simple zero.

**Definition 1.2.7 (Derivative/Repeated Factor)**:
- *Let $P \in K[X]$ such that $P(X) = \sum_{i=0}^{n} k_i X^i$, the formal derivative of $P(X)$ is defined by $P'(X) = \sum_{i=1}^{n} i k_i X^{i-1}$.*
- *Let $Q \in K[X]$ of degree $\geq 1$, then $Q$ is said to be a repeated factor of $P \in K[X]$ if $P(X) = Q(X)^m R(X)$ for some $m \geq 2$ and $R \in K[X]$.*

**Proposition 1.2.8**: *Let $K$ be a field with $\mathrm{Char}\, K = 0$, then we have that $\deg P' = \deg P - 1$, thus $P$ does not divide $P'$.*

*Proof.* Let $P(X) = \sum_{i=0}^{n} a_i X^i$, with $a_n \neq 0$, its derivative is defined as $P'(X) = \sum_{i=1}^{n} i a_i X^{i-1}$, the coefficent of the highest degree is $n a_n$, which is not zero since $\mathrm{Char}\, K = 0$. Thus $\deg P' = n - 1 = \deg P - 1$. □

**Proposition 1.2.9**: *Let $K$ be a field with $\mathrm{Char}\, K = 0$ and $P \in K[X]$, then $P$ has a repeated factor in $K[X] \Leftrightarrow P, P'$ have a common factor.*

> *More precisely, if $Q \in K[X]$ a repeated factor of $P$ then it divides both $P$ and $P'$. Conversely if $Q$ is irreducible and is a common divisor of $P$ and $P'$ then it is a repeated factor of $P$.*

*Proof.*
- $\Rightarrow$ suppose that $P(X) = Q^m(X)R(X)$, $P'(X) = mQ^{m-1}(X)Q'(X)R(X) + Q^m(X)R'(X)$ then $Q$ divides both $P$ and $P'$.
- $\Leftarrow$ suppose now that $P, P'$ have a common factor $Q$ irreducible which exists by the fact that $K[X]$ is a UFD, then $P(X) = Q(X)R(X)$ we get then that $P'(X) = Q'(X)R(X) + Q(X)R'(X)$ since $Q$ divides $P$ and $P'$ we have that it divides $Q'(X)R(X) = P'(X) - Q(X)R'(X)$ so $Q$ divides either $Q'$ or $R$, since $\mathrm{Char}\, K = 0$ then $Q$ does not divide $Q'$ so it necessarily divides $R$ then $R(X) = Q(X)R_1(X)$, thus $P(X) = Q(X)R(X) = Q(X)Q(X)R_1(X) = Q^2(X)R_1(X)$ so $Q$ is a repeated factor of $P$.

□

**Corollary 1.2.10**: *Let $P \in K[X]$ irreducible and $\mathrm{Char}\, K = 0$ then $P(X)$ has no repeated zeros in any algebraic closure $\overline{K}$.*

> ***Proof Outline:***
> 1. Consider the Bezout identity $P(X)U(X) + P'(X)V(X) = 1$.
> 2. Replace with the roots of $P(X)$ and deduce it doesn't nullify $P'$.
> 3. Deduce that the factor $(X - \alpha)$ is not present in $P'$.
> 4. Deduce that $(X - \alpha)$ is simple factor of $P$.

*Proof.* Let $P \in K[X]$ be irreducible then $P' \neq 0$ and $P$ does not divide $P'$, if $Q$ is a common factor of $P$ and $P'$ then $Q$ divides $P$ and since $P$ is irreducible then $Q(X) = \lambda P(X)$ thus $P$ divides $P'$, so $\gcd(P(X), P'(X)) = 1$. By Bezout's theorem we have that $\exists u, v \in K[X]$ such that $P(X)u(X) + P'(X)v(X) = 1$, viewing this identity in $\overline{K}[X]$, let $\alpha$ be a zero of $P$ in $\overline{K}$, replacing in the previous equation we have that $P(\alpha)u(\alpha) + P'(\alpha)v(\alpha) = P'(\alpha)v(\alpha) = 1$ then $P'(\alpha) \neq$

0 so $(X-\alpha)$ is not a factor of $P'$ so $P$ has no repeated factor $(X-\alpha)$ then $P$ has no repeated zeros in $\overline{K}$. □

**Corollary 1.2.11**: *Let $K$ be a field of* $\operatorname{Char} K = 0$ *and $\alpha$ be algebraic over $K$ of degree $d$ and let* $\operatorname{Irr}(\alpha, K, X) = (X-\alpha_1)...(X-\alpha_d)$ *in $\overline{K}[X]$, then there exists $d$ embeddings of $K(\alpha)$ into $\overline{K}$ of the form $\sigma_i : \alpha \mapsto \alpha_i$.*

*Proof.* Use the previous corollary and the one of the existence of $s$ embeddings in this case to get $s = d$. □

**Theorem 1.2.12 (Primitive Element)**: *Let $L$ be a finite extension of a field $K$ with* $\operatorname{Char} K = 0$ *then there is $\theta \in L$ such that $L = K(\theta)$.*

> ***Proof Outline:***
> 1. Simplify by induction to two elements $L = K(\alpha, \beta)$.
> 2. Take $P(X) = \operatorname{Irr}(\alpha, K, X)$, $Q(X) = \operatorname{Irr}(\beta, K, X)$.
> 3. Take $\theta \in K \setminus \left\{(\alpha - \alpha_i)/(\beta_j - \beta) \mid (i,j) \in [\![1,n]\!] \times [\![2,m]\!]\right\}$.
> 4. Consider $\theta = \alpha + k\beta$ and $R(X) = P(\theta - kX)$.
> 5. Prove that $k$ is the only common factor of $R$ and $Q$.
> 6. Deduce that $(X-\beta) \in K(\theta)[X]$ and thus $\beta \in K(\theta)$.

*Proof.* It is easy to notice that by induction, a proof for the existence of $\theta$ when $L = K(\alpha, \beta)$ is sufficent.

Consider $L = K(\alpha, \beta)$. Consider the minimal polynomials

$$P(X) = \operatorname{Irr}(\alpha, K, X) \underset{\overline{K}[X]}{=} (X-\alpha_1)...(X-\alpha_n)$$

$$Q(X) = \operatorname{Irr}(\beta, K, X) \underset{\overline{K}[X]}{=} (X-\beta_1)...(X-\beta_m)$$

Let $k \in K$ such that $\forall i \in [\![1,n]\!], \forall j \in [\![2,m]\!], k \neq \frac{\alpha-\alpha_i}{\beta_j-\beta}$ which exists since $\operatorname{Char}(K) = 0 \Rightarrow \#K = \infty$ and consider $\theta = \alpha + k\beta$, clearly $K(\theta) \subseteq K(\alpha, \beta)$.

Consider the polynomial $R(X) = P(\theta - kX)$, $\deg R = \deg P = n$ and $R \in K(\theta)[X]$, we have $R(\beta) = P(\theta - k\beta) = P(\alpha) = 0$ so $\beta$ is a zero of $R$ and also a zero of $Q$. We want to prove that the only common zero of $R$ and $Q$ is $\beta$, let $\gamma$ be a zero of $R$ and $Q$ in $\overline{K}$, $R(\gamma) = P(\theta - k\gamma) = 0 \Rightarrow \theta - k\gamma = \alpha_i$ so we get that $\gamma$ satisfies $\gamma = \frac{\theta-\alpha_i}{k} = \frac{\alpha-\alpha_i}{k} + \beta$, since $\gamma$ is a zero of $Q$ then $\gamma = \beta_j$ but this reduces to $k = \frac{\alpha-\alpha_i}{\beta_j-\beta}$ which is not true by choice of $k$ so $\gamma = \beta_1 = \beta$. Thus the unique common zero of $Q$ and $R$ is $\beta$ then $\operatorname{Irr}(\beta, K, X)$ divides both $Q$ and $R$ and is of degree one so $\operatorname{Irr}(\beta, K, X) = X - \beta \in K(\theta)[X]$ thus we have $\beta \in K(\theta)$.

It is clear that $K(\theta) \subseteq K(\alpha, \beta)$ and we have that $\beta \in K(\theta)$ then $\alpha = \theta - k\beta \in K(\theta)$ since $k, \theta, \beta \in K(\theta)$ and thus $K(\alpha, \beta) = K(\theta)$. □

**Example:**

- to find the primitive of $\mathbb{Q}\left(\sqrt{a}, \sqrt{b}\right)$ with $a, b \in \mathbb{Z}$ non-perfect squares, we have that $\operatorname{Irr}(\sqrt{a}, \mathbb{Q}, K) = X^2 - a$ and $\operatorname{Irr}\left(\sqrt{b}, \mathbb{Q}, K\right) = X^2 - b$ thus $\alpha_1 = \sqrt{a}, \alpha_2 = -\sqrt{a}$ and $\beta_1 = \sqrt{b}, \beta_2 = -\sqrt{b}$ and thus we obtain that the set of non-allowed values of $k$ are $\left\{0, \sqrt{a/b}\right\}$, given that $a \neq b$ then $k = 1$ is not in that list so we obtain that

$$\mathbb{Q}\left(\sqrt{a} + \sqrt{b}\right) = \mathbb{Q}\left(\sqrt{a} + \sqrt{b}\right)$$

Chapter 2

# Extensions Of Finite Fields

The aim of this chapter is to study the structure of the finite fields and how to characterize them using their ground fields. Consider the fields $\mathbb{F}_p$ as the fields $\mathbb{Z}_p$ with the modular addition and multiplication.

## 2.1. Finite Fields

**Proposition 2.1.1**: *Let $F$ be a finite field with $\# F = q$ and $E/F$ a finite extension of degree $n$ then $\# E = q^n$.*

*Proof.* We have that $[E : F] = \dim_F E = n$, thus $E \cong F^n$ as an $F$-vector space, so $\# E = \#(F^n) = (\# F)^n = q^n$. □

**Corollary 2.1.2**: *Let $E$ be a finite field with* Char $E = p$, *then $\# E = p^n$ for some $n \in \mathbb{N}^\star$.*

*Proof.* We have that Char $E = p$, then it has a copy of $\mathbb{Z}/p\mathbb{Z}$ by the isomorphism $\varphi : \mathbb{Z}/p\mathbb{Z} \to E, n \mapsto 1 + 1 + ... + 1$, $n$ times, take $F = \varphi(\mathbb{Z}/p\mathbb{Z})$, it is a subfield of $E$, we get then that $\# E = (\# F)^n = p^n$ where $n = [E : F]$. □

**Theorem 2.1.3**: *Let $E$ be a finite field with $\# E = p^n$, then the elements of $E$ are precisely the zeros of the polynomial $X^{p^n} - X \in \mathbb{F}_p[X]$ in a certain algebraic closure $\overline{\mathbb{F}_p}$.*

*Proof.* Let $P(X) = X^{p^n} - X$ and $\mathcal{Z}(P) = \left\{\alpha \in \overline{\mathbb{F}_p} \mid P(\alpha) = 0\right\}$

- $E \subseteq \mathcal{Z}(P)$: $\# E = p^n$ then $\# E^* = p^n - 1$ thus the multiplicative group $E^*$ is of order $p^n - 1$, by Lagrange's theorem, we have that $\forall a \in E^*, a^{p^n - 1} = 1$ thus we get that $a^{p^n} - a = 0$ so $P(a) = 0$ and notice also that $P(0) = 0$ thus we obtain $E = E^* \cup \{0\} \subseteq \mathcal{Z}(P)$.
- $\mathcal{Z}(P) \subseteq E$: notice that $\# \mathcal{Z}(P) \leq p^n$ since $\deg P = p^n$ and $\# E = p^n$ thus it is clear that $\mathcal{Z}(P) \subseteq E$.

So we conclude that $\mathcal{Z}(P) = E$. □

**Example:**

1. $E = \mathbb{F}_2$ with $n = 1$ and $p = 2$ then $\mathbb{F}_2$ are the zeros of $X^2 - X = X(X - 1)$.
2. $E = \mathbb{F}_2(\alpha)$ with $\alpha^2 + \alpha + 1 = 0$, we have that $E = \{0, 1, \alpha, \alpha^2\}$ and by the theorem the roots of $X^4 - X = X(X - 1)(X^2 + X + 1)$ are the solutions.

**Theorem 2.1.4**: *Let $E$ be a finite field, then the group $E^*$ is cyclic.*

*Proof.* Let $E$ be a finite field and $E^* = E \setminus \{0\}$ the multiplicative group of $E$, then $E^*$ is abelian and $\# E^* = p^n - 1$ where $\# E = p^n$, assume on the contrary that $E^*$ is not cyclic, so the order of any element of $E^*$ is strictly less than $p^n - 1$. Let $\alpha \in E^*$ of maximal order $s < p^n - 1$. Let $G = \langle\alpha\rangle = \{\alpha, \alpha^2, ..., \alpha^s\}$ be the cyclic subgroup of $E^*$ generated by $\alpha$. Any element of $G$ has an order that divides $s$ by Lagrange's theorem, $\forall g \in G, g^s = 1$ thus $g$ is a zero of $X^s - 1 \in E[X]$, and since $\deg(X^s - 1) = s$ then this polynomial has at most $s$ zeros, so $G$ are exactly the roots of $X^s - 1$ in $\overline{\mathbb{F}_p}$, since $\# G = s < p^n - 1 = \# E^*$ then there exists $\beta \in E^*$ with $\beta \notin G$. Let $t$ be the order of $\beta$, $\beta^t = 1$ and $t$ does not divide $s$

$$s = p_1^{l_1} p_2^{l_2} ... p_j^{l_j} ... p_r^{l_r} \qquad t = p_1^{k_1} p_2^{k_2} ... p_j^{k_j} ... p_r^{k_r}$$

with $p_i$ prime numbers and $l_i, k_i \in \mathbb{N}$, $l_1 < k_1, l_j < k_j, l_{j+1} \geq k_{j+1}, ..., l_r \geq k_r$. $j$ exists since $t$ does not divide $s$, set $u = p_1^{l_1} ... p_j^{l_j}$, $u' = s/u$, $v = p_1^{k_1} ... p_j^{k_j}$ and $v' = t/v$. Notice that $u < v$ and $\gcd(u, v') = 1$. Let $\gamma = \alpha^u \beta^{v'}$, $\gamma \in E^*$ since $\alpha, \beta \in E^*$, $\alpha^u$ is of order $u'$ and $\beta^{v'}$ is of order $v$ and since $u$ and $v'$ are coprime then the order of $\alpha^u \beta^v$ is $u'v > u'u = s$, contradiction with the fact that the maximal order is $s$. □

**Constructive Proof:** Let $q = \# E$ and $q - 1 = \prod_{i=1}^{k} p_i^{l_i}$ by the fundemental theorem of artihemtic. Consider for $i \in [\![1, k]\!]$ the polynomials $P_i(X) = X^{\frac{q-1}{p_i}} - 1$, notice that $\# \mathcal{Z}(P_i) \leq \frac{q-1}{q_i} < q - 1 = \# E^*$, thus there exists $y_i \in$

$E^* \setminus \mathcal{Z}(P_i)$. Now for $i \in [\![1,k]\!]$ $z_i = y_i^{(q-1)/\left(p_i^{l_i}\right)}$, notice that $z_i$ has order $p_i^{l_i}$ since $z_i^{p_i^{l_i}} = y_i^{q-1} = 1$ by Lagrange's theorem and $z_i^{p_i^{l_i-1}} = y_i^{(q-1)/p_i} \neq 1$ by the definition of $y_i$. We chose $z = \prod_{i=1}^n z_i$, since all the orders of $z_i$ are coprime from the fact that they are different primes, then the order of $z$ is $\prod_{i=1}^n p_i^{l_i} = q-1 = \#\, E^*$, thus $E^* = \langle z \rangle$ and $E^*$ is cyclic.

**Example:** Consider $\mathbb{F}_7$ then $p = 7$, $n = 1$ and $q = 7$

$$q-1 = 6 = 2 \cdot 3 \Rightarrow \begin{cases} p_1 = 2 \\ l_1 = 1 \\ p_2 = 3 \\ l_2 = 1 \end{cases} \Rightarrow \begin{cases} P_1(X) = X^3 - 1 \\ P_2(X) = X^2 - 1 \end{cases}$$

$$\Rightarrow \begin{cases} y_1 = 3 \\ y_2 = 4 \end{cases} \Rightarrow \begin{cases} z_1 = 3^3 = 6 \\ z_2 = 4^2 = 2 \end{cases} \Rightarrow z = 6 \cdot 2 = 5$$

its easy to verify that $\langle 5 \rangle = \mathbb{F}_7^\star$.

**Corollary 2.1.5**: *Let $E$ be a finite extension of a finite field $F$, then there exists a primitive element $\theta \in E$, $E = F(\theta)$.*

*Proof.* Consider $\theta$ the generator of $E^*$ from the previous proposition. $F(\theta) \subseteq E$ since $\theta \in E^* \subseteq E$ and $F \subseteq E$. $E \subseteq F(\theta)$ given that $E^* = \langle \theta \rangle \subseteq F(\theta)$ and $0 \in F \subseteq F(\theta)$ thus we obtain $E = \{0\} \cup E^* \subseteq F(\theta)$ hence $E = F(\theta)$. □

**Theorem 2.1.6**: *Let $n \in \mathbb{N}^*$ and $p$ a prime number, there exists a unique field of order $p^n$ up to an isomorphism denoted $\mathbb{F}_{p^n}$.*

*Proof.* Consider $P(X) = X^{p^n} - X$ in $\overline{\mathbb{F}_p}$ and let $K = \left\{\alpha \in \overline{\mathbb{F}_p} \mid P(\alpha) = 0\right\}$. We will prove that $K$ is a subfield of $\overline{\mathbb{F}_p}$ containing $\mathbb{F}_p$.

- $\mathbb{F}_p \subseteq K$: let $\alpha \in \mathbb{F}_p$, we have $\alpha^{p-1} = 1$ by Langrange's theorem, thus $\alpha^p = \alpha$, by induction we have that $\alpha^{p^i} = \alpha$ thus $P(\alpha) = \alpha^{p^n} - \alpha = 0$ so $\alpha \in K$.
- $K$ is a field: Let $\alpha, \beta \in K$, we have that $\left(\alpha^{-1}\right)^{p^n} = \left(\alpha^{p^n}\right)^{-1} = \alpha^{-1}$, $(\alpha\beta)^{p^n} = \alpha^{p^n}\beta^{p^n} = \alpha\beta$ since $\cdot$ is commutative, $(\alpha+\beta)^{p^n} = \sum_{i=0}^{p^n} \binom{p^n}{i} \alpha^i \beta^{p^n - i}$, since $K \subseteq \overline{\mathbb{F}_p}$ and $\operatorname{Char} \overline{\mathbb{F}_p} = \operatorname{Char} \mathbb{F}_p = p$ then $\forall i \in [\![1, p-1]\!], p \mid \binom{p^n}{i}$ thus we get $(\alpha+\beta)^{p^n} = \alpha^{p^n} + \beta^{p^n} = \alpha + \beta$.

Thus $K$ is a subfield of $\overline{\mathbb{F}_p}$ containing $\mathbb{F}_p$ and has $p^n$ elements since $\overline{\mathbb{F}_p}$ is algebraically closed and $\deg P = p^n$. □

**Corollary 2.1.7**: *Let $F$ be a finite field, $F \subseteq \overline{\mathbb{F}_p}$ and $\alpha \in \overline{\mathbb{F}_p}$, then the zeros of $\operatorname{Irr}(\alpha, F, X)$ are distinct, the conjugates of $\alpha$ are all in $F(\alpha)$ and so there are exactly $[F(\alpha) : F]$ embeddings which are all automorphisms.*

*Proof.* we have $\mathbb{F}_p \subseteq F \subseteq F(\alpha)$, $\left[F : \mathbb{F}_p\right] = d$ and $[F(\alpha) : F] = n$ then we get $\mathbb{F}(\alpha) \cong \mathbb{F}_{p^{nd}}$. The elements of $F(\alpha)$ are zeros of $X^{p^{nd}} - X \in \mathbb{F}_p[X]$ so $\operatorname{Irr}\left(\alpha, \mathbb{F}_p, X\right)$ divides $X^{p^{nd}} - X$ whose zeros are distinct so the zeros of $\operatorname{Irr}\left(\alpha, \mathbb{F}_p, X\right)$ are distinct. Let $\sigma$ be an $F$-embedding of $F(\alpha)$ then $\sigma(\alpha)$ is a conjugate of $\alpha$ so $\#\, F(\alpha) = \#\, F(\sigma(\alpha))$ thus $F(\alpha) = F(\sigma(\alpha))$. □

**Example:**

- $\mathbb{F}_2 = \{0, 1\}$, the set of cubic polynomials over $\mathbb{F}_2[X]$ are $P_1(X) = X^3 + X + 1$ and $P_2(X) = X^3 + X^2 + 1$.

**Proposition 2.1.8**: *Let $m, n \in \mathbb{N}^*$ and $p$ prime then*

$$\mathbb{F}_{p^m} \text{ is a subfield of } \mathbb{F}_{p^n} \Leftrightarrow m \text{ divides } n.$$

*Proof.* $\Rightarrow$ suppose that $\mathbb{F}_{p^m}$ is a subfield of $\mathbb{F}_{p^n}$, then $\mathbb{F}_{p^n}$ is an extension of $\mathbb{F}_{p^m}$ and we have that $n = \left[\mathbb{F}_{p^n} : \mathbb{F}_p\right] = \left[\mathbb{F}_{p^n} : \mathbb{F}_{p^m}\right] \cdot \left[\mathbb{F}_{p^m} : \mathbb{F}_p\right] = k \cdot m$ thus $m$ divides $n$. $\Leftarrow$ suppose that $m$ divides $n$ so $n = k \cdot m$, let $\alpha \in \mathbb{F}_{p^m}$, by definition of $\mathbb{F}_{p^m}$ we have $\alpha^{p^m} = 1$ so $\alpha^{p^n} = \alpha^{p^{km}} = \left(\alpha^{p^m}\right)^{p^{(k-1)m}} = 1^{p^{(k-1)m}} = 1$ thus $\alpha \in \mathbb{F}_{p^n}$, and since $\mathbb{F}_{p^m}$ is a field then it is a subfield of $\mathbb{F}_{p^n}$. □

**Corollary 2.1.9**: *The number of subfields of $\mathbb{F}_{p^n}$ is equal to the number of positive divisors of $n$.*

*Proof.* It is clear from the previous statement that the only subfields are divisors of $n$, denote them $d_1, \ldots, d_k$. Then the subfields of $\mathbb{F}_{p^n}$ are $\mathbb{F}_{p^{d_1}}, \mathbb{F}_{p^{d_2}}, \ldots, \mathbb{F}_{p^{d_k}}$. □

**Definition 2.1.10 (Frobenius Automorphisms)**: *Let $f : \mathbb{F}_q \to \mathbb{F}_q$ where $q = p^n$ with $f : \alpha \mapsto \alpha^p$, then $f$ is called the frobenius automorphism of $\mathbb{F}_q$.*

To justify this nomination, we will prove that it is a $\mathbb{F}_p$-automorphism

- $f$ is well defined: since for $\alpha \in \mathbb{F}_q$, $\alpha^p \in \mathbb{F}_q$ thus $f(\alpha) \in \mathbb{F}_q$.
- $f$ is a $\mathbb{F}_p$-embedding: let $\alpha, \beta \in \mathbb{F}_q$, $f(\alpha+\beta) = (\alpha+\beta)^p = \alpha^p + \beta^p = f(\alpha) + f(\beta)$ since $\operatorname{Char} \mathbb{F}_q = p$, $f(\alpha\beta) = (\alpha\beta)^p = \alpha^p\beta^p = f(\alpha)f(\beta)$. $f$ is injective since $\operatorname{Ker} f = \{\alpha \in \mathbb{F}_q \mid f(\alpha) = 0\} = \{\alpha \in \mathbb{F}_q \mid \alpha^p = 0\} = \{0\}$ given its a field. Let $\alpha \in \mathbb{F}_p$, $\alpha$ satisfies $\alpha^p - \alpha = 0$ thus $f(\alpha) = \alpha^p = \alpha$.

Using Proposition 1.1.6, we deduce that $f$ is an automorphism of $\mathbb{F}_q$.

**Proposition 2.1.11**: *Let $\alpha$ be algebraic over $\mathbb{F}_p$ of degree $n$ $\left(\mathbb{F}_p(\alpha) = \mathbb{F}_{p^n}\right)$ then the embeddings of $\mathbb{F}_p(\alpha)$ into $\overline{\mathbb{F}_p}$ are $f^1, f^2, ..., f^n$ where $f$ is the Frobenius automorphism of $\mathbb{F}_{p^n}$.*

*Proof.* Notice that $f$ is an automorphism, thus $\forall i \in [\![1, n]\!]$, $f^i$ is an automorphism from $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^n}$ so is an embedding from $\mathbb{F}_p(\alpha)$ to $\overline{\mathbb{F}_p}$. Since $\alpha$ is of degree $n$ then there are exactly $n$ embeddings, we will prove that all of them are of the form $f^i$.

There $n$ embeddings $f^1, ..., f^n$, now we will prove that they are all not equal, that is $\forall 1 \leq i < j \leq n$, $f^i \not\equiv f^j$. Suppose that there exists $i, j \in [\![1, n]\!]$, $i < j$ such that $f^i \equiv f^j$, $\mathbb{F}_p(\alpha)$ is a finite field then there is a generator $\theta$ for the multiplicative group $\left(\mathbb{F}_p(\alpha)\right)^* = \langle\theta\rangle$, $\theta^{p^i} = f^i(\theta) = f^j(\theta) = \theta^{p^j}$, so $\theta^{p^j - p^i} = 1$ but $p^j - p^i < p^n$ and the order of $\theta$ is $p^n$ which is a contradiction. Thus we conclude that $\{f^i\}_{i \in [\![1,n]\!]}$ are the only embeddings of $\mathbb{F}_p(\alpha)$ into $\overline{\mathbb{F}_p}$. □