# 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 separate the contents of the course to actual additions or out of context information, a black band will be added by its side like the globing 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 Isomorphism 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 canonical surjective map.*

$$A \xrightarrow{\pi} A/I \xrightarrow{f_*} B, \qquad A \xrightarrow{f} B$$

## 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 Factorization Domain:*** $R$ *is an UFD if any element can be decomposed into a unique product of irreducible elements.*

**Theorem 0.2.9:**
- *If $R$ is an 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 Criteria):**
- *Let $P(x) = a_0 + a_1 x + \ldots + a_n x^n \in \mathbb{Z}[X]$, if there is a prime $p$ such that $p \mid a_0, \ldots, p \mid a_{n-1}, p^2 \nmid a_0$ 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 $1 + 1 + \ldots + 1 = 0$ $n$ 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 isomorphisms $(\nu_\alpha)_\star : K[X]/I \to K[\alpha]$ and $(\nu_\beta)_\star : K[X]/I \to K[\beta]$ such that $\nu_\alpha = (\nu_\alpha)_\star \circ \pi$ and $\nu_\beta = (\nu_\beta)_\star \circ \pi$. We also have that $K[\alpha] = K(\alpha)$ and $K[\beta] = K(\beta)$ since $\alpha, \beta$ are algebraic.

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

**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 coefficient 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 an 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 $k \in K \setminus \left\{(\alpha - \alpha_i)/(\beta_j - \beta) \mid (i,j) \in [\![1,n]\!] \times [\![2,m]\!]\right\}$.
4. Consider $\theta = \alpha + k\beta$ and $R(X) = P(\theta - kX)$.
5. Prove that $\beta$ is the only common zero 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 sufficient.

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 $R$, 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 fundamental theorem of arithmetic. 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 $q = 7$

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

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

It is 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 Lagrange'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 $\alpha^{p^m} = \alpha$, we will prove by induction that $\alpha^{p^{m \cdot i}} = \alpha$. Its trivial $i = 0$, Suppose its true for $i$, we have that $\alpha^{p^{m \cdot i}} = \alpha \Rightarrow \left(\alpha^{p^{m \cdot i}}\right)^{p^m} = \alpha^{p^m} = \alpha \Rightarrow \alpha^{p^{m \cdot (i+1)}} = \alpha$ thus we get by induction that $\alpha^{p^{mk}} = \alpha \Rightarrow \alpha^{p^n} = \alpha$ so $\alpha \in \mathbb{F}_{p^n}$ thus $\mathbb{F}_{p^m}$ is 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 it is 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 $\overline{\mathbb{F}_p}$. □

Chapter 3

# Normal Extensions

In what follows $K$ denotes a field, $\overline{K}$ an algebraic closure of $K$ and $P(X)$ a non-constant polynomial.

**Definition 3.1 (Splitting Field):** *Let $\alpha_1, ..., \alpha_n$ be the zeros of the polynomial $P \in K[X]$ in $\overline{K}$, then the field $K(\alpha_1, ..., \alpha_n)$ is called splitting field of $P$ over $K$. In other words, $K(\alpha_1, ..., \alpha_n)$ is the smallest subfield of $\overline{K}$, in which, we can write $P(X) = (X - \alpha_1)\cdots(X - \alpha_n)$.*

**Example:**

- The splitting field of $X^2 - 2$ over $\mathbb{Q}$ in $\mathbb{C}$ is $\mathbb{Q}\left(\sqrt{2}\right)$.
- The splitting field of $X^3 - 2$ over $\mathbb{Q}$ in $\mathbb{C}$ is $\mathbb{Q}\left(\sqrt[3]{2}, j\sqrt[3]{2}, j^2\sqrt[3]{2}\right) = \mathbb{Q}\left(\sqrt[3]{2}, j\right)$.
- $\mathbb{C}$ is the splitting field of $X^2 + 1$ in $\mathbb{R}$ because $\mathbb{R}(i, -i) = \mathbb{R}(i) = \mathbb{C}$.
- Any finite field $\mathbb{F}_{p^n}$ is the splitting field some polynomial in $\mathbb{F}_p[X]$, since $\forall \alpha \in \mathbb{F}_{p^n}$, $\alpha$ is a zero of $X^{p^n} - X \in \mathbb{F}_p[X]$ so if we set $\mathcal{Z}(X^{p^n} - X)$ the set of zeros of $X^{p^n} - X$ then $\mathbb{F}_{p^n} = \mathbb{F}_p(\mathcal{Z}(X^{p^n} - X))$.
- The splitting field of $(X^2 - 2)(X^2 - 3)(X^2 - 1) \in \mathbb{Q}[X]$ is the field containing all the roots which is $\mathbb{Q}\left(\pm\sqrt{3}, \pm\sqrt{2}, \pm 1\right) = \mathbb{Q}\left(\sqrt{2} + \sqrt{3}\right)$.

**Definition 3.2 (Splitting Field Of A Family Of Polynomials):** *Let $(P_i)_{i\in I} \subseteq K[X]$ and $\mathcal{Z} = \cup_{i\in I} \mathcal{Z}(P_i)$ then the field $K(\mathcal{Z})$ is the intersection of all subfields of $\overline{K}$ containing $K$ and $\mathcal{Z}$ which is called the splitting field of the family $(P_i)_{i\in I}$ over $K$.*

**Example 3.3:**

- $\overline{K}$ is a splitting field of the family of non-constant polynomials in $K[X]$.
- The splitting field of $\{X^2 - 2, X^2 - X - 1, X^3 - 2, X^3 - 1\}$ over $\mathbb{Q}$ is $\mathbb{Q}\left(\pm\sqrt{2}, \left(1 \pm \sqrt{5}\right)/2, \sqrt[3]{2}, j\sqrt[3]{2}, j^2\sqrt[3]{2}\right) = \mathbb{Q}\left(\sqrt[3]{2}, \sqrt{2}, \sqrt{5}, j\right)$.

**Definition 3.4 (Normal Extension):** *Let $L/K$ be an algebraic extension, then $L/K$ is said to be a* normal extension *if for any $P \in K[X]$ irreducible in $K$, if $P$ has a root in $L$, then all its roots are in $L$.*

**Proposition 3.5:** *Let $L/K$ be an algebraic extension, the following statements are equivalent*

1. *$L/K$ is a normal extension.*
2. *$\forall \alpha \in L$, all conjugates of $\alpha$ over $K$ are in $L$.*

*Proof.*

- 1. $\Rightarrow$ 2. is clear given that the conjugates of $\alpha$ are the roots of $\mathrm{Irr}(\alpha, K, X)$, which exists by the fact that $L/K$ is algebraic and has $\alpha$ as a root in $L$, are contained in $L$ thus all the conjugates of $\alpha$ over $K$ are contained in $L$.
- 2. $\Rightarrow$ 1. Let $P \in K[X]$ be irreducible over $K$, and suppose $P$ has a zero $\alpha \in L$, since $\mathrm{Irr}(\alpha, K, X)$ divides $P(X)$ in $K[X]$ and $P$ is irreducible then $P(X) = \lambda\,\mathrm{Irr}(\alpha, K, X)$, any root of $P$ is a root of $\mathrm{Irr}(\alpha, K, X)$ and thus a conjugate of $\alpha$, so the roots of $P$ are contained in $L$.

□

**Example 3.6:**

- $\overline{K}/K$ is normal since $\overline{K}/K$ is algebraic and every polynomial is split on $\overline{K}$.
- $\mathbb{C}/\mathbb{Q}$ is not normal since it is not algebraic, while $\mathbb{C}/\mathbb{R}$ is normal since $\overline{\mathbb{R}} = \mathbb{C}$.
- $K/K$ is normal since $[K : K] = 1$ thus algebraic and $\mathrm{Irr}(\alpha, K, X) = X - \alpha$ thus its only conjugate is $\alpha$ and thus contained in $K$.
- Let $\mathbb{Q}\left(\sqrt[3]{2}\right)/\mathbb{Q}$ is not normal since the conjugates of $\sqrt[3]{2}$ which are $j\sqrt[3]{2}$ and $j^2\sqrt[3]{2}$ are not in $\mathbb{Q}\left(\sqrt[3]{2}\right)$.

**Theorem 3.7:** *Let $L/K$ be an algebraic extension and $L \subseteq \Omega$, then the following statements are equivalent:*

1. *Any $K$-embeddings of $L$ into $\Omega$ is an automorphism of $L$.*
2. *$L/K$ is normal.*
3. *$L$ is a splitting field over $K$ of a family of $K[X]$.*

*Proof.*

- 1. $\Rightarrow$ 2. Let $\alpha \in L$ and $\beta$ a conjugate of $\alpha$ over $K$, by Proposition 1.1.4 there exists a $K$-embedding $\tau$ from $K(\alpha) \subseteq L$ to $K(\beta) \subseteq \Omega$ that sends $\alpha$ to $\beta$ and since $L/K$ then $L/K(\alpha)$ is algebraic. Let $\sigma$ be an extension of $\tau$ to $L$, so $\sigma$ is a $K$-automorphism of $L$ from assumption, and thus $\sigma(\alpha) = \tau(\alpha) = \beta \in L$.
- 2. $\Rightarrow$ 3. Suppose $L/K$ normal, consider the family of polynomials $\mathcal{F}$ defined by $\mathcal{F} = \{P(X) \in K[X] \mid P \text{ irreducible having a zero in } L\}$ and $F$ be the splitting field of $\mathcal{F}$ over $K$. Let $\mathcal{Z}$ be the set of zeros of all elements of $\mathcal{F}$, $F = K(\mathcal{Z})$. Since $\mathcal{Z} \subseteq L$ (because $L/K$ normal), we have $K(\mathcal{Z}) = F \subseteq L$. Now let $\alpha \in L$, $\alpha$ is algebraic and is a zero $\text{Irr}(\alpha, K, X) \in \mathcal{F}$ so $\alpha \in \mathcal{Z} \subseteq F$ thus $L \subseteq F$.
- 3. $\Rightarrow$ 1. Suppose that $L$ is a splitting field over $K$ of a family $\mathcal{F}$ of $K[X]$, $L = K(\mathcal{Z})$ where $\mathcal{Z}$ is the set of zeros of elements of $\mathcal{F}$ in $\Omega$. Let $\sigma$ be a $K$-embedding of $L$ into $\Omega$. To show that $\sigma$ is a $K$-automorphism of $L$, it suffices to prove that $\sigma$ is a $K$-endomorphism using Proposition 1.1.6. Let $\alpha \in \mathcal{Z}$ then $\sigma(\alpha)$ is a conjugate of $\alpha$ over $K$ thus $\sigma(\alpha) \in \mathcal{Z}$.

□

**Example 3.8:**

- $\mathbb{Q}\left(\sqrt{2}\right)/\mathbb{Q}$ is normal. We have that $\text{Irr}\left(\sqrt{2}, K, X\right) = X^2 - 2$ then there are two embeddings of $\mathbb{Q}\left(\sqrt{2}\right) \to \overline{\mathbb{Q}}$ which are $\sigma_1 : \sqrt{2} \mapsto \sqrt{2}$ and $\sigma_2 : \sqrt{2} \mapsto -\sqrt{2}$ which are both automorphisms.

**Example 3.9:**

- $\mathbb{Q}\left(\sqrt[3]{2}\right)/\mathbb{Q}$ is not normal, we have that $j\sqrt[3]{2}$ is a conjugate of $\sqrt[3]{2}$ over $\mathbb{Q}$ but is not in $\mathbb{Q}\left(\sqrt[3]{2}\right)$ thus
- $F$ is a finite field, $E$ a finite extension of $F$ then $E/F$ is normal.

**Proposition 3.10:** *Let $K \subseteq L \subseteq M$ be a tower of fields, if $M/K$ is normal then $M/L$ is normal.*

*Proof.* Since $M/K$ is normal, then it is algebraic and so are $M/L$ and $L/K$. Also, $M$ is the splitting field of a family $\mathcal{F} \subseteq K[X]$. Let $\mathcal{Z}$ be the zeros of elements of $\mathcal{F}$ in $K$ then $M = K(\mathcal{Z})$ because $K[X] \subseteq L[X]$ we see $\mathcal{F} \subseteq L[X]$ and $M = K(\mathcal{Z}) \subseteq L(\mathcal{Z}) \subseteq M$ and so $M = L(\mathcal{Z})$. □

- If $M/K$ and $M/L$ are normal then $L/K$ is not necessarily normal. Notice that $\mathbb{Q}\left(\sqrt[3]{2}\right)$ is not normal because $j\sqrt[3]{2}$ is a conjugate of $\sqrt[3]{2}$ which is not in $\mathbb{Q}\left(\sqrt[3]{2}\right)$, by taking $K = \mathbb{Q} \subseteq L = \mathbb{Q}\left(\sqrt[3]{2}\right) \subseteq M = \mathbb{Q}\left(\sqrt[3]{2}, j\right)$
- If $L/K$ and $M/L$ are normal then $M/K$ is not necessarily normal. Notice that $K = \mathbb{Q} \subseteq L = \mathbb{Q}\left(\sqrt{2}\right) \subseteq M = \mathbb{Q}\left(\sqrt[4]{2}\right)$ are both normal but the overall extension is not normal.

**Proposition 3.11:** *Let $M/K$ be an algebraic extension and let $(F_i)_{i\in I}$ be a family of intermediate fields $\forall i \in I, K \subseteq F_i \subseteq M$ such that $F_i/K$ is normal, then $\left(\bigcap_{i\in I} F_i\right)/K$ is normal.*

*Proof.* Since $M/K$ is algebraic then $F_i/K$ is algebraic for any $i \in I$, consider $\alpha \in \cap_{i\in I} F_i$, we have that $\forall i \in I$ the set of conjugates $\mathcal{C}$ of $\alpha$ are in $F_i$ since they are all normal, and thus the set of conjugates $\mathcal{C}$ is contained in $\bigcap_{i\in I} F_i$ thus $\bigcap_{i\in I} F_i/K$ is a normal extension. □

**Definition 3.12 (Normal Closure):** *Let $L/K$ e an algebraic extension where $L \subseteq \overline{K}$, then the intersection of all extensions of $L$ in $\overline{K}$ which are normal over $K$, is called the* normal closure *of $L$ over $K$.*

The extension exists since $\overline{K}/K$ is normal and by the Proposition 3.11 it is normal.

**Example:**

- Suppose $L/K$ is normal, then the normal closure of $L$ over $K$ is $L$.
- $K = \mathbb{Q} \subseteq L = \mathbb{Q}\left(\sqrt[3]{2}\right) \subseteq N = \mathbb{Q}\left(\sqrt[3]{2}, j\right)$, $N/Q$ is normal because $N$ is the splitting field of $X^3 - 2 \in \mathbb{Q}[X]$.

Chapter 4

# Separable Extensions

**Proposition:** *Let $L/K$ be an algebraic extension and let $\tau_1$ and $\tau_2$ be two embeddings of $K$ into an algebraically closed field $\Omega$. Let $E_1$, $E_2$ be the set of extensions of $\tau_1, \tau_2$ into $\Omega$ respectively, then there is a bijection between $E_1$ and $E_2$.*

**Definition (Separable Degree):** *The common number of elements of the extensions of $\tau_1$ from the previous proposition (maybe infinite) is called the separable degree of the extension $L/K$ denoted $[L : K]_s$.*

**Proposition 4.1:**

1. *Let $K \subseteq L \subseteq M$ be a tower of algebraic extensions then the separable degree satisfies $[M : K]_s = [M : L]_s \cdot [L : K]_s$.*
2. *If $L/K$ is a finite extension then $[L : K]_s \leq [L : K]$.*

**Proof Outline:**

1. 1. Consider $\{\sigma_i : L \to \Omega \mid i \in I\}$ the set of extensions of $\tau$ to $L$ and extend each $\sigma_i$ to $M$ which gives $\left\{\sigma_i^j \mid j \in J\right\}$.
   2. Deduce that $[M : K]_s \geq [M : L]_s [L : K]_s$.
   3. Consider an embedding $\varphi : M \to \Omega$.
   4. Restrict to $K, L$ and deduce that $\exists (i, j) \in I \times J, \varphi \equiv \sigma_i^j$.
   5. Deduce that $[M : K]_s \leq [M : L]_s [L : K]_s$.
2. 1. Deduce from Corollary 1.1.5 that $[K(\alpha) : K]_s \leq [K(\alpha) : K]$.
   2. Deduce $[K(\alpha, \beta) : K]_s \leq [K(\alpha, \beta) : K]$ $(K(\alpha, \beta) = K(\alpha)(\beta))$.
   3. By induction $[L : K]_s \leq [L : K]$.

*Proof.*

1. Let $\tau$ be an embedding of $K$ into $\Omega$ an algebraically closed field, let $\{\sigma_i \mid i \in I\}$ be the set of extensions of $\tau$ into $L$. Each extension $\sigma_i$ has extension to $M$, we denote the set of those extensions of $\sigma_i$ as $\left\{\sigma_i^j \mid j \in J\right\}$, so $\tau$ has $\# I \cdot \# J$ extensions into $M$ so we get $[M : K]_s \geq [M : L]_s \cdot [L : K]_s$. Now let $\varphi$ be an embedding of $M$ into $\Omega$, then the restriction of $\varphi$ to $L$ is an embedding of $L$ into $\Omega$ and so $\varphi = \sigma_i^j$ for some $(i, j) \in I \times J$, hence $[M : K]_s \leq [M : L]_s \cdot [L : K]_s$ and we get the result $[M : K]_s = [M : L]_s \cdot [L : K]_s$.
2. - Suppose $L = K(\alpha)$, we have that $[K(\alpha) : K]$ is the number of embeddings of $K(\alpha)$ into $\Omega$ which is the number of distinct conjugates of $\alpha$ over $K$ which is less than the degree of the minimal polynomial of $\alpha$ thus $[K(\alpha) : K]_s \leq \deg(\mathrm{Irr}(\alpha, K, X)) = [K(\alpha) : K]$.
   - Suppose that $L = K(\alpha, \beta)$, we have that $K \subseteq K(\alpha) \subseteq K(\alpha)(\beta) = K(\alpha, \beta)$. By applying the first case we have that $[K(\alpha) : K]_s \leq [K(\alpha) : K]$ and $[K(\alpha)(\beta) : K(\alpha)]_s \leq [K(\alpha)(\beta) : K(\alpha)]$ and by using the 1. we get $[K(\alpha)(\beta) : K(\alpha)]_s \cdot [K(\alpha) : K]_s \leq [K(\alpha)(\beta) : K(\alpha)] \cdot [K(\alpha) : K]$ we obtain directly the result that $[K(\alpha, \beta) : K]_s \leq [K(\alpha, \beta) : K]$.
   - Since $L/K$ is finite then $L = K(\alpha_1, ..., \alpha_n)$ using the multiplicativity property of degree and separable degree we obtain the result.

□

**Definition 4.2 (Separable Finite Extension/Polynomial/Element):**

1. *Let $L/K$ be a finite extension then we say that $L/K$ is separable if $[L : K]_s = [L : K]$.*
2. *A polynomial $P \in K[X]$ with $\deg P \geq 1$ is said to be separable if its zeros in an algebraically closed field $\Omega$ are distinct.*
3. *Let $\alpha \in \overline{K}$, we say that $\alpha$ is separable if $\mathrm{Irr}(\alpha, K, X)$ is separable.*

**Proposition 4.3:** *Let $\alpha \in \overline{K}$, then $\alpha$ is separable over $K \Leftrightarrow \alpha$ is a zero of a separable of a polynomial in $K[X] \Leftrightarrow [K(\alpha) : K]_s = [K(\alpha) : K]$.*

**Proposition 4.4:** *Let $L/K$ be a finite extension such that $K$ is finite or $\mathrm{Char}\, K = 0$, then $L/K$ is separable.*

*Proof.* From Theorem 1.2.12 and Corollary 2.1.5, there is $\theta \in L$ such that $L = K(\theta)$ since $\mathrm{Irr}(\theta, K, X)$ is irreducible it is separable when $\mathrm{Char}\, K = 0$ by Corollary 1.2.10. Also when $K$ is finite $\Rightarrow L$ is finite, say $\# L = p^n$ hence $\theta$ is a zero of $X^{p^n} - X \in \mathbb{F}_p[X] \subseteq K[X]$ which is separable then we can conclude from Proposition 4.3. □

**Example 4.5:**

- Let $p$ be prime $K = \mathbb{F}_p(y^p)$ and $L = \mathbb{F}_p(y)$, we have that $\mathbb{F}_p \subseteq K \subseteq L = K(y)$ since $y$ is a zero of $X^p - y^p \in K[X]$ then $L/K$ is finite with $[L : K] \leq p$, and $\mathrm{Irr}(y, K, X)$ divides $X^p - y^p = (X - y)^p$ then $\mathrm{Irr}(y, K, X) = (X - y)^t$ with $1 \leq t \leq p$. Indeed,, if $t = 1$ then $y \in K$ and so $y = P(y^p)/Q(y^p)$ for some $P, Q \in \mathbb{F}_p[X]$ then $yQ(y^p) = P(y^p)$ but $(yQ(y^p))' = Q(y^p) + ypQ'(y^p) = Q(y^p)$ and $(P(y^p))' = 0$ thus $Q(y^p) = 0$ which is a contradiction.

> **Proposition 4.6:** *Let $L/K$ be a finite extension, $L/K$ separable $\Leftrightarrow \forall \alpha \in L$, $\alpha$ is separable over $K$.*

*Proof.* $\Rightarrow$ Suppose $L/K$ be separable then $[L : K]_s = [L : K]$, let $\alpha \in L$, then $K \subseteq K(\alpha) \subseteq L$, $[L : K] = [L : K(\alpha)] \cdot [K(\alpha) : K]$ and $[L : K]_s = [L : K(\alpha)]_s \cdot [K(\alpha) : K]_s$, by the Proposition 4.1 we have that $[L : K(\alpha)]_s \cdot [K(\alpha) : K]_s = [L : K(\alpha)] \cdot [K(\alpha) : K]$ by the inequalities then necessarily $[K(\alpha) : K]_s = [K(\alpha) : K]$. $\Leftarrow$ Suppose $\forall \alpha \in L$, $\alpha$ is separable over $K$, since $L/K$ is finite we have $L = K(\alpha_1, ..., \alpha_n)$ for some $\alpha_i \in L$

- $\alpha_1$ is separable over $K \Rightarrow [K(\alpha_1) : K]_s = [K(\alpha_1) : K]$.
- $\alpha_2$ is separable over $K \Rightarrow \alpha_2$ is separable over $K(\alpha_1) \Rightarrow [K(\alpha_1, \alpha_2) : K]_s = [K(\alpha_1, \alpha_2) : K]$.

By induction we get that $L/K$ is separable. □

> **Definition 4.7 (Separable Extension):** *Let $L/K$ be an algebraic extension, we say that $L/K$ is* separable *if $\forall \alpha \in L, \alpha$ is separable over $K$.*

> **Proposition 4.8:** *Let $K \subseteq L \subseteq M$ be a tower of fields then $M/K$ separable $\Leftrightarrow M/L$ and $L/K$ separable.*

*Proof.* $\Rightarrow$ suppose $M/K$ is separable, then $\forall \alpha \in M, \alpha$ is separable over $K$, and thus $\forall \alpha \in L \subseteq M, \alpha$ is separable over $K$ thus $L/K$ is separable. Let $\alpha \in M$, $\alpha$ is separable over $K$ then $\mathrm{Irr}(\alpha, K, X)$ is separable, since $\mathrm{Irr}(\alpha, K, X) \in K[X]$ then $\alpha$ is separable over $L$.

$\Leftarrow$ suppose $M/L$ and $L/K$ are separable, let $\alpha \in M$, $\alpha$ is separable over $L$. Consider $\mathrm{Irr}(\alpha, K, X) = X^d + a_{d-1}X^{d-1} + \cdots + a_1 X + a_0 \in L[X]$, consider $L' = K(a_0, ..., a_{d-1}) \subseteq L$, we have by induction that $\forall i \in [\![0; n]\!], [K(a_0, ..., a_i) : K(a_0, ..., a_{i-1})]_s = [K(a_0, ..., a_i) : K(a_0, ..., a_{i-1})]$ because $a_i$ is separable over $K$ thus over any field containing $K$, by Proposition 4.1 we have that $[L' : K]_s = [L' : K]$. Also $[L'(\alpha) : L']_s = [L'(\alpha) : L']$ because the separable polynomial $\mathrm{Irr}(\alpha, L, X) \in L'[X]$, again by Proposition 4.1 $[L'(\alpha) : K]_s = [L'(\alpha) : K]$ thus $\alpha$ is separable over $K$. □

> **Corollary 4.9:** *Let $K/L$ be a finite separable extension, then $\exists \theta \in L$ such that $L = K(\theta)$.*

*Proof.* If $K$ if finite, then $L$ is finite and thus $L = K(\theta)$ where $\theta$ is the generator of $L^*$. Now if $K$ is infinite, we follow the same steps as Proposition 1.2.12. □

> **Definition 4.10 (Galois Extension):** *A field extension $L/K$ is said to be Galois if it is normal and separable.*

**Example 4.11:**

1. $K/K$ is Galois.
2. $\overline{K}/K$ is Galois.
3. $\mathbb{Q}(\sqrt{m})/\mathbb{Q}$ with $m$ square free integer

> **Definition (Fixed Field):** *Let $L$ be a field and $S \subseteq \mathrm{Aut}(L)$, the set $L^S$ defined as $L^S = \{\alpha \in L \mid \forall \sigma \in S, \sigma(\alpha) = \alpha\}$ is the* fixed field *of $S$ in $L$.*

> **Proposition 4.12:** *Let $L$ be a field and the set of automorphisms of $L$, denoted $\mathrm{Aut}(L)$.*
> *1. $(\mathrm{Aut}(L), \circ)$ is a group.*

2. *Let $S \subseteq \mathrm{Aut}(L)$, then $L^S$ is a subfield of $L$.*

*Proof.* Trivial ? □

**Note 4.13:** *Let $L/K$ be a Galois extension of degree $n$, then $L = K(\theta)$ for some $\theta \in L$ because $L/K$ is separable and there are exactly $n$ $K$-embeddings of $L$ into an algebraically closed field $\Omega$ which are automorphisms, let $G(L/K)$ be the set of such $K$-automorphisms, then $\#\, G(L/K) = n$ and $G(L/K) \subseteq \mathrm{Aut}(L)$.*

**Definition (Galois Group):** *Let $L/K$ be an extension, the set of all $K$-automorphisms of $L$ is called the Galois group of the extension $L/K$ and we denote it $G(L/K)$.*

- *$L/K$ is said to be abelian if $G(L/K)$ is abelian.*
- *$L/K$ is said to be cyclic if $G(L/K)$ is cyclic.*

**Theorem 4.14:** *Let $L/K$ be a Galois field extension of degree $n$, then $G(L/K)$ the set of all $K$-automorphisms of $L$ is a subgroup of $\mathrm{Aut}(L)$. Moreover, if $H$ is a subgroup of $G(L, K)$ then $L^H = K \Rightarrow H = G(L/K)$.*

**Theorem 4.15 (Galois Theorem):** *Let $L/K$ be a Galois extension of degree $n$ and let $\mathcal{F}$ be the set of intermediate fields of $L/K$ and $\mathcal{G}$ be the set of subgroups of $G(L/K)$. Then there is a correspondence between $\mathcal{F}$ and $\mathcal{G}$ with the map defined as*

$$\begin{aligned} \varphi : \mathcal{F} &\to \mathcal{G} & \varphi^{-1} : \mathcal{G} &\to \mathcal{F} \\ F &\mapsto G(L/F) & H &\mapsto L^{(H)} \end{aligned}$$

Chapter 5

# Groups

## 5.1. Remainders

**Definition (Group/Subgroup):** *A non-empty set $G$ and an operation $\cdot : G \times G \to G$ is said to be a* group *if*
- *Closure: $\cdot$ is well defined, that is, $\forall x, y \in G, x \cdot y \in G$.*
- *Associativity: $\forall x, y, z \in G, x \cdot y \cdot z = (x \cdot y) \cdot z = x \cdot (y \cdot z)$.*
- *Neutral Element: $\exists e \in G, \forall x \in G, x \cdot e = e \cdot x = x$.*
- *Inverse Element: $\forall x \in G, \exists x^{-1} \in G, x \cdot x^{-1} = x^{-1} \cdot x = e$.*

*$G$ is said to be abelian if $\forall x, y \in G, x \cdot y = y \cdot x$. $H \subseteq G$ is said to be a subgroup of $G$ if $(H, \cdot)$ is also a group.*

The most import groups include

$$(\mathbb{Z}, +) \quad (\mathbb{Q}, +) \quad (\mathbb{R}, +) \quad (\mathbb{C}, +) \quad (\mathbb{Z}_n, +_{\bmod n})$$
$$(\mathbb{Q}^*, \cdot) \quad (\mathbb{R}^*, \cdot) \quad (\mathbb{C}^*, \cdot) \quad (\{-1, 1\}, \cdot)$$

To simplify notation we denote $x \cdot y = xy$. We also have $S_n$ the set of bijections from $[\![1, n]\!]$ to itself called the symmetric group, we represent the permutation $\sigma : [\![1, n]\!] \to [\![1, n]\!]$ as

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ \sigma_1 & \sigma_2 & \sigma_3 & \cdots & \sigma_n \end{pmatrix}$$

**Proposition:** *Let $G$ be a group and $H \subseteq G$, if $H$ is finite then $H$ is a subgroup of $G \Leftrightarrow \forall x, y \in H, x \cdot y \in H$.*

**Definition (Order):** *Let $G$ be a group and $g \in G$.*
- *The order of $g$ is the smallest positive integer such that $g^n = e$.*
- *The order of $G$ is the cardinality of $G$.*

*We denote them as $o(\cdot)$, if the order does not exist then $o(g) = \infty$.*

**Proposition:** *Let $G$ be a group and $g \in G$.*
- *$o(g) = o(g^{-1})$.*
- *Lagrange: $o(g)$ divides $o(G)$.*

**Definition (Cyclic):** *Let $G$ be a group and $g \in G$, we say that $G$ is cyclic $G = \langle g \rangle = \{g^n \mid n \in \mathbb{N}\}$.*

**Proposition:** *A subgroup of a cyclic group is cyclic.*

**Definition (Homomorphism):** *Let $G, G'$ two groups, $f : G \to G'$, $f$ is said to be a homomorphism if $\forall x, y \in G, f(xy) = f(x)f(y)$. $f$ is said to be an isomorphism if $f$ is bijective.*

**Proposition:** *Let $f : G \to G'$ be a group homomorphism.*
- *$\operatorname{Ker} f = \{x \in G \mid f(x) = e'\}$ is a subgroup of $G$.*
- *$\operatorname{Im} f = f(G)$ is a subgroup of $G'$.*
- *$f$ injective $\Leftrightarrow \operatorname{Ker} f = \{e'\}$.*
- *$f$ surjective $\Leftrightarrow \operatorname{Im} f = G'$.*

**Definition (Cosets):** *Let $G$ be a group, $H \subseteq G$ a subgroup and $a \in G$.*
- *Left Coset: $aH = \{ah \mid h \in H\}$.*
- *Right Coset: $Ha = \{ha \mid h \in H\}$.*

**Proposition:** *Let $G$ be a group, $H \subseteq G$ a subgroup and $a, b \in G$.*

- $aH = H \Rightarrow a \in H$.
- $aH = bH \Rightarrow b^{-1}a \in H$.
- *There is a bijection between left cosets and right cosets and we denote the number of cosets as $(G : H)$, if $G$ and $H$ are finite then $(G : H) = \#G/\#H$.*

**Definition (Normal Subgroup/Quotient Group):** *Let $G$ be a group, $H \subseteq G$ a subgroup, $H$ is said to be a normal subgroup if $\forall a \in G, aH = Ha$ or equivalently $\forall a \in G, aHa^{-1} = H$. If $H$ is normal we define the quotient group $G/H = \{aH \mid a \in G\}$ with the operation $aH \cdot bH = abH$.*

**Theorem (First Isomorphism Theorem):** *Let $f : G \to G'$ be a group homomorphism then we have $\operatorname{Ker} f$ is a normal subgroup of $G$ and we have that $G/\operatorname{Ker} f \cong \operatorname{Im} f$.*

## 5.2. Some Prelimining Results

**Lemma 5.2.1:** *Let $G$ such that $G \neq \{e\}$ be a group without non-trivial subgroups, then $G$ is finite and $\#G$ is prime.*

**Proposition 5.2.2 (Cauchy's Lemma):** *Let $G$ be a finite abelian group, if $p$ is prime dividing $\#G$ then there is a subgroup $H$ subset $G$ with $\#H = p$.*

*Proof.* By induction on $\#G$.

- It is trivial for $\#G = 1$.
- Suppose it is true for all $k \leq n$
  - If $G$ has no proper subgroup, then $\#G$ is prime so all its divisors are $p$ and 1 thus the subgroups are $G$ and $\{e\}$.
  - Assume that $G$ has a proper subgroup $K$
    - If $p \mid \#K$ then it satisfies the induction hypothesis and thus there is a subgroup of order $p$ of $K$ and thus a subgroup of $G$.
    - If $p \nmid \#K$ then by considering $G/K$, $\#(G/K) = \#G/\#K$ and since $p \mid \#G$ and $p \nmid \#K$ then $p \mid \#(G/K)$ so by hypothesis there is a subgroup $bK$, then $(bK)^p = K$ and $bK \neq K$, let $m = \#K$ then $b^p \in K \Rightarrow (b^p)^m = e$. Take $a = b^m$, $a^p = e$, assume that $a = e$ then $b^m = e$ so $p$ divides $m$ which is a contradiction.

□

**Proposition 5.2.3 (Sylow's Theorem):** *Let $G$ be a finite abelian group and let $p$ a prime dividing $\#G$ and $v \in \mathbb{N}$ such that $p^v \mid \#G$ and $p^{v+1} \nmid \#G$, then there exists a subgroup of order $p^v$.*

*Proof.* Consider $S = \{g \in G \mid \exists n \in \mathbb{N}, g^{p^n} = e\}$.

1. $e \in S$: $e^p = e$.
2. $S \neq \{e\}$: by Proposition 5.2.2, $\exists a \in G$ with order $p$, $a \neq e$ and $a^p = e$.
3. Let $a, b \in S$ with $a^{p^n} = e$ and $b^{p^m} = e$ then $(ab)^{p^{n+m}} = \left(a^{p^n}\right)^{p^m}\left(b^{p^m}\right)^{p^n} = e$ since $S$ is finite and closed then it is a subgroup.
4. $\#S = p^\beta$ for some $\beta \in \mathbb{N}$: $\forall g \in G$ order of $g$ is a power of $p$. Suppose on the contrary $\forall \beta \in \mathbb{N}, \#S \neq p^\beta$ then there exists a prime $q \neq p$ dividing $\#S$. From Cauchy's theorem $\exists g \in G$ with order $q$ then $\exists t \in \mathbb{N}^*, q = p^t \Rightarrow q = p, t = 1$ contradiction.
5. $v \stackrel{?}{=} \beta$: since $S$ is a subgroup of $G$, $p^\beta = \#S \mid \#G = p^v$ thus $\beta \leq v$. Suppose by contradiction that $\beta < v$, consider the quotient group $G/S$ then $p \mid \#(G/S) = \#G/\#S$ and $G/S$ is abelian. By Proposition 5.2.2, there exists $bS$ of order $p$ ($b^pS = S$) and $bS \neq S$ ($b \notin S$) but $b^p \in S \Rightarrow \exists n \in \mathbb{N}, (b^p)^{p^n} = e \Rightarrow b^{p^{n+1}} = e \Rightarrow b \in S$ which is a contradiction.

□

**Lemma 5.2.4:** *Let $H$ and $K$ be subgroups of a group of $G$ then $HK$ is a subgroup of $G$ if and only if $HK = KH$.*

*Proof.*

- $\Leftarrow$ suppose $HK = KH$, then $H \cup K \subseteq HK$. Let $h_1k_1, h_2k_2 \in HK$ with $h_i \in H$ and $k_i \in K$ then $h_1(k_1h_2)k_2 = h_1(h_3k_3)k_2 = (h_1h_3)(k_3k_2) \in HK$ and $(hk)^{-1} = k^{-1}h^{-1} \in KH = HK$.

- $\Rightarrow$ suppose that $HK$ is a subgroup, let $h \in H$ and $k \in K$ then $(hk)^{-1} = k^{-1}h^{-1}$, since $(h^{-1}k^{-1})^{-1} \in HK$ and thus $kH \in KH$ so $HK \subseteq KH$.

□

**Lemma 5.2.5:** *Let $H, K$ be two finite subgroups of a group $G$, then $\#HK = (\#H \#K)/(\#(H \cap K))$.*

*Proof.* Consider the map $\varphi : H \times K \to HK, \varphi(h,k) \mapsto hk$ $\varphi$ is well defined and surjective by definition. We prove that $\forall x \in HK$, $\#\varphi^{-1}(\{x\}) = |H \cap K|$. Let $(h_1,k_1),(h_2,k_2) \in HK, \varphi(h_1,k_1) = \varphi(h_2,k_2) \Rightarrow h_1k_1 = h_2k_2 \Rightarrow h_2^{-1}h_1 = k_2k_1^{-1}$, since $h_1,h_2 \in H$ and $k_1k_2 \in K$ then we have that $h_2^{-1}h_1 \in H \cap K$ then there exists $x \in H \cap K$ such that $h_1 = h_2x$ and $k_1 = x^{-1}k_2$, conversely if $x \in H \cap K$ then $\varphi(h_2x, x^{-1}k_2) = h_2xx^{-1}k_2 = h_2k_2 = \varphi(h_2,k_2)$. Thus we can deduce that $\varphi^{-1}(\{h_1k_1\}) = \{((h_1x, x^{-1}h_2)) \mid x \in H \cap K\}$ thus $\#(H \times K) = \#HK \cdot \#(H \cap K)$ and since $\#(H \times K) = \#H \#K$ then we get $\#HK = (\#H \#K)/(\#(H \cap K))$. □

**Corollary 5.2.6:** *If $H$ and $K$ are finite subgroups of $G$, $\#H \#K > \#G$ then $\#(H \cap K) \geq 2$.*

*Proof.* $HK$ is a subgroup of $G$ then $\#HK \leq \#G$ and since $\#H \#K > \#G$ then $\#HK = (\#H \#K)/\#(H \cap K)$ is satisfied only if $\#(H \cap K) > 1$. □

**Definition (Commutator Of An Element):** *Let $G$ be a group and $x, y \in G$. The commutator of $x, y$ is the element $xyx^{-1}y^{-1}$ denoted as $[x,y]$.*

**Proposition:** *Let $G$ be a group and $x, y \in G$.*
1. *$[x,y] = e \Leftrightarrow xy = yx$.*
2. *$[x,y]^{-1} = [y,x]$.*
3. *$[y,x]xy = yx$.*
4. *$\forall g \in G, g[x,y]g^{-1} = [gxg^{-1}, gyg^{-1}]$.*

*Proof.*
1. $[x,y] = e \Leftrightarrow xyx^{-1}y^{-1} = e \Leftrightarrow xyx^{-1} = y \Leftrightarrow xy = yx$.
2. $[x,y]^{-1} = (xyx^{-1}y^{-1})^{-1} = yxy^{-1}x^{-1} = [y,x]$.
3. $[y,x]xy = yxy^{-1}x^{-1}xy = yx$.
4. $$\begin{aligned} g[x,y]g^{-1} &= gxyx^{-1}y^{-1}g^{-1} \\ &= gxg^{-1}gyg^{-1}gx^{-1}g^{-1}gy^{-1}g^{-1} \\ &= (gxg^{-1})(gyg^{-1})(gxg^{-1})^{-1}(gyg^{-1})^{-1} \\ &= [gxg^{-1}, gyg^{-1}] \end{aligned}$$

□

**Definition (Commutator Of A Group):** *Let $G$ be a group. The commutator or derived set of $G$ is the smallest subgroup containing $\{[x,y] \mid x,y \in G\}$ denoted $G'$, $G' = \left\{\prod_{i=1}^{n}[x_i,y_i] \mid n \in \mathbb{N}, (x_i)_{i=1}^{n}, (y_i)_{i=1}^{n} \subseteq G\right\}$.*

**Proposition 5.2.7:** *Let $G$ be a group and $G'$ the commutator of $G$.*
1. *$G'$ is normal in $G$.*
2. *$G/G'$ is an abelian group.*
3. *Let $N$ a normal subgroup of $G$, $G/N$ abelian $\Rightarrow G' \subseteq N$.*

*Proof.*
1. Let $z \in G'$ and $g \in G$, we have that $z = \prod_{i=1}^{n}[x_i,y_i]$ with $n \in \mathbb{N}, x_i, y_i \in G$, then $gxg^{-1} = g\prod_{i=1}^{n}[x_i,y_i]g^{-1} = \prod_{i=1}^{n} g[x_i,y_i]g^{-1} = \prod_{i=1}^{n}[gx_ig^{-1}, gy_ig^{-1}] \in G'$, thus $G'$ is normal.
2. Let $x,y \in G$, $xG'yG' = xyG' = (y^{-1}x^{-1}G')^{-1} = (x^{-1}y^{-1}[y,x]G')^{-1} = (x^{-1}y^{-1}G')^{-1} = yxG' = yG'xG'$, thus $G/G'$ is abelian.
3. Let $N$ be a normal subgroup with $G/N$ abelian. Let $x,y \in G, xNyN = yNxN$ then $xyN = yxN \Rightarrow xy(yx)^{-1} \in N \Rightarrow [x,y] = xyx^{-1}y^{-1} \in N$ so $G' \subseteq N$.

□

**Definition (Center Of A Group):** *Let $G$ be a group, we define the center of $G$ as $\mathcal{Z}(G) = \{x \in G \mid \forall y \in G, xy = yx\}$.*

**Proposition 5.2.8:** *Let $G$ be a group and $\mathcal{Z}(G)$ the center of $G$.*
1. *$\mathcal{Z}(G)$ is a normal subgroup of $G$.*
2. *$G$ is abelian $\Leftrightarrow \mathcal{Z}(G) = G$.*

*Proof.*
1. Let $g \in G$ and $x \in \mathcal{Z}(G)$ then $gxg^{-1} = xgg^{-1} = x$ thus $\mathcal{Z}(G)$ is normal in $G$.
2. $G$ is abelian $\Leftrightarrow \forall x \in G, \forall y \in G, xy = yx \Leftrightarrow G = \mathcal{Z}(G)$.

□

**Proposition 5.2.9:**

$$G/\mathcal{Z}(G) \text{ is cyclic} \Leftrightarrow G \text{ is abelian.}$$

*Proof.* $\Leftarrow$ trivial since $\mathcal{Z}(G) = G$ thus $G/\mathcal{Z}(G) = \{e\}$. $\Rightarrow$ Suppose that $G/Z(G)$ is cyclic, set $Z = \mathcal{Z}(G)$, then $\exists g \in G, G/Z = \langle gZ \rangle$, let $x, y \in G$, we have $xZ = g^n Z$ and $yZ = g^m Z$ and thus $x = g^n z_1$ and $y = g^m z_2$, $xy = (g^n z_1)(g^m z_2)$ since $z_1, z_2 \in Z$ then $xy = g^{n+m} z_1 z_2 = g^{m+n} z_2 z_1 = (g^m z_2)(g^n z_1) = yx$. □

**Lemma 5.2.10:** *Let $G$ and $G'$ be two groups and $\varphi : G \to G'$ a surjective homomorphism.*
1. *Let $H'$ be a subgroup of $G'$ then $\varphi^{-1}(H')$ is a subgroup of $G$, if $H'$ is normal then so is $G$ containing $\operatorname{Ker}\varphi$.*
2. *Let $\Phi$ be the (resp. normal) subgroups of $G$ containing $\ker\varphi$ and $\Phi'$ be the (resp. normal) subgroups of $G'$ then the map*

$$f : \Phi' \to \Phi$$
$$H' \mapsto f(H') = \varphi^{-1}(H')$$

*is bijective with inverse $H \mapsto \varphi(H)$.*

*Proof.* You can do it! □

**Proposition 5.2.11:** *Let $\varphi : G \to G'$ be a group surjective homomorphism, and let $N'$ be a subgroup of $G'$, then $\varphi^{-1}(N')$ is a normal subgroup of $G$ containing $\operatorname{Ker}\varphi$, then we have that $G/N \cong G'/N'$.*

*Proof.* Consider the map $G \xrightarrow{\varphi} G' \xrightarrow{\pi'} G'/N$, then $\psi = \pi' \circ \varphi$ is a surjective homomorphism with $\operatorname{Ker}\psi = N$, by the first isomorphism theorem $G/N \cong G'/N'$ □

**Proposition:** *Let $K \subseteq N \subseteq G$, then $G/N \cong (G/K)/(N/K)$.*

*Proof.* Suppose $K$ is normal in $G$, then $K$ is normal in $N$, we have that $N/K$ is a normal subgroup of $G/K$, by setting $G' = G/K$, $N' = N/K$ and $\varphi = \pi$ we get from the previous proposition that $G/N \cong (G/K)/(N/K)$. □

### 5.2.1. Dihedral Group

### 5.2.2. Cayley's Theorem & Premutation Group

**Lemma:** *Let $G$ be a group, $g \in G$, the map $\varphi_g : G \to G, x \mapsto gx$ is a bijection.*

**Theorem 5.2.2.12 (Cayley's Theorem):** *Any group $G$ is isomorphic to a subgroup of a symmetric group $\mathcal{S}(X)$, more specifically, by taking $X = G$ we get that $G$ is isomorphic to a subgroup of $\mathcal{S}(X)$, if $G$ is finite and of order $n$ then $G$ is isomorphic to a subgroup $S_n$.*

*Proof.* Consider $\varphi : G \to \mathcal{S}(G), g \mapsto \varphi_g$. It is enough to prove that $\varphi$ is an injective homomorphism thus $G$ would be isomorphic to $\varphi(G) \subseteq \mathcal{S}(G)$ which would be a subgroup since $\varphi$ is a homomorphism.

- $\varphi$ is a homomorphism: let $g, g' \in G$, $\forall x \in G, \varphi(gg')(x) = \varphi_{gg'}(x) = (gg')(x) = g(g'x) = (\varphi_g \circ \varphi_{g'})(x)$ thus $\varphi(gg') = \varphi(g) \circ \varphi(g')$ thus we have that $\varphi$ is a homomorphism.
- $\varphi$ is injective: let $g \in \operatorname{Ker}\varphi$ then $g \equiv \mathrm{id}$, so $\forall x \in G, \varphi(g)(x) = \varphi_g(x) = gx = x$, by taking $x = e$ we get that $g = e$ thus $\operatorname{Ker}\varphi = \{\mathrm{id}\}$.

□