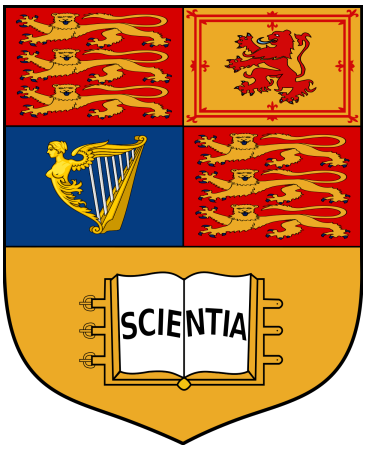
# Groups & Rings - Concise Notes

MATH50005

**Arnav Singh**




**Colour Code** - **Definitions** are **green** in these notes, **Consequences** are **red** and **Causes** are **blue**

*Content from MATH40003 assumed to be known.*

Mathematics
Imperial College London
United Kingdom
January 14, 2022

*"Three Rings for the Elven-kings under the sky,*
*Seven for the Dwarf-lords in their halls of stone,*
*Nine for Mortal Men doomed to die,*
*One for the Dark Lord on his dark throne*
*In the Land of Mordor where the Shadows lie.*
*One Ring to rule them all, One Ring to find them,*
*One Ring to bring them all and in the darkness bind them*
*In the Land of Mordor where the Shadows lie."*

– J.R.R Tolkien, *Rings of Power*

# Contents

# Part I
# Groups

## 1 Homomorphisms + Normal Subgroups

### 1.1 Homomorphisms, Isomorphisms and Automorphisms

**Group Axioms**
**G is a group** w.r.t a binary operation $\iff \forall g, h, i \in G$

- **G1** - $gh \in G$ **(Closure Axiom)**
- **G2** - $(gh)i = g(hi)$ **(Associativity Axiom)**
- **G3** - $\exists e \in G$ **s.t** $\forall g \in G, ge = e = eg$ **(Existence of identity)**
- **G4** - $\forall g \in G, \exists g^{-1}$ **s.t** $gg^{-1} = e = g^{-1}g$ **(Existence of inverses)**

**Definition 1.1** A function $f : G \to H$ is a **Homomorphism** if $\forall a, b \in G$ we have $f(ab) = f(a)f(b)$.
Note $ab$ operation of G, $f(a)f(b)$ operation of H

corollary: $f(e_G) = e_H \implies f(g^{-1}) = f(g)^{-1}$

**Definition 1.4** A function $f : G \to H$ an **Isomorphism** if $f$ **a bijective homomorphism.**
We write $f : G \xrightarrow{\sim} H$ or $G \cong H$

**Definition 1.6** A function $f$ an isomorphism, $f : G \xrightarrow{\sim} G$ is called an **Automorphism**

Extend this to define $Aut(G)$ as the group of automorphisms of G under composition. Conjugation by an element in G is an automorphism.

**Definition**, for a homomorphism $f : G \to H$ assosciate:

1. $Im(f) = f(G) = \{f(x) | x \in G\}$
2. $Ker(f) = \{x \in G | f(x) = e_H\}$

### 1.2 Normal subgroups, quotient groups and the isomorphism theorem

**Definition 1.11 Normal Subgroups**,

$$N \subset G \text{ normal in G} \iff gng^{-1} \in N, \forall g \in G \text{ and } n \in N$$

We say that N is stable under the conjugation by any element in G.

**Definition 1.12 Simple Groups - group** $G$ **simple** if $G$ **has no normal subgroups aside from** $\{e\}$ **and** $G$

**Define**

- $gS := \{gs | s \in S\}$ - **Left cosets** of S
- $Sg := \{sg | s \in S\}$ -**Right cosets** of S

**Lemma** - $H \subset G$ a subgroup. If $gH = Hg \ \forall g \in G \implies H$ **a normal subgroup**
**Lemma** - $N \subset G$ **a normal subgroup.** Then $(g_1N)(g_2N) = (g_1g_2N)$
**Quotient Group** - $N$ a normal subgroup of $G$. $G/N$ the quotient group of $G$ modulo $N$ is the set of all left cosets of N in G. $G/N = \{aN | a \in G\}$
**Lemma** - $N$ a normal subgroup of $G$. The set $G/N$ of left cosets of $G$ modulo $N$ **is a group** under group law $(g_1N, g_2N) \mapsto (g_1g_2N)$**.**

**Theorem 1.19 - Isomorphism Theorem** - Let $f : G \to H$ a homomorphism of groups. Consider the map $gKer(f) \mapsto f(g)$, this map is an **isomorphism** of groups.

$$G/Ker(f) \xrightarrow{\sim} f(G)$$

## 1.3 Group-Theoretic Constructions

- **Centre of a Group** $Z(G)$= $\{a \in G \mid ax = xa, \forall x \in G\}$. It is the set of elements in G that commute with all elements in G.
  $Z(G) = G \iff G$ abelian.
- **Inner Automorphisms** $Inn(G)$ - The set of automorphisms formed by the conjugations of elements in G, forming a subgroup of $Aut(G)$
- **Commutator** - Write $[a, b] = aba^{-1}b^{-1}$ this is the commutator of $a$ and $b$.
- **Commutator of a Group** - $[G, G]$ is the smallest subgroup in $G$ containing the commutators $[a, b] \forall a, b \in G$. It is the subgroup generated by all the commutators.
  $G$ abelian $\iff [G, G] = \{e_G\}$

Sending an element $g \in G$ to the conjugation by $g$ is a homomorphism $G \to Aut(G)$ with image $Inn(G)$ and kernel $Z(G)$. Giving isomorphism $G/Z(G) \xrightarrow{\sim} Inn(G)$. using **Theorem 1.19**

**Lemma 1.21** - $G$ **a group** .Then $[G, G]$ **a normal subgroup** of $G$ and $G/[G, G]$ **is abelian.**
**Proposition 1.22** - $N$ **a normal subgroup of** $G$. Then $G/N$ **is abelian if and only if** $N$ **contains** $[G, G]$
**Lemma 1.23** - Any **subgroup of** $G$ **containing** $[G, G]$ is **normal**

*Behaviour of products of groups in the abelian case:*

**Lemma 1.25** - $G$ an abelian group. **If orders of** $a, b \in G$ **finite**, then **order of** $ab$ **is finite and divides** $lcm(ord(a), ord(b))$**.**

**Torsion subgroups** - The set of elements of $G$ that have finite order is a subgroup of $G$, denoted $G_{\text{tors}}$. If $G = G_{\text{tors}}$ we say G is a **torsion abelian group.**

**$p$-subgroups of G** - $G$ an abelian group, $p$ a prime number.
The subgroup $G\{p\} = \{g | g \in G \text{ s.t } ord(g) = p^n\}$ is the **$p$-primary subgroup of G**
If $G = G\{p\}$ then $G$ is called a **$p$-primary torsion abelian group**

*Generators.*
**Lemma 1.29** - $I$ a set s.t $\forall i \in I$, we **have subgroups** $H_i \subset G$. Then $H = \cap_{i \in I} H_i$ **a subgroup of G.**

**1.30 - Generated Groups** - $G$ a group, $S \subset G$ a set. Intersection of all subgroups of G that contain S is the **subgroup of $G$ generated by** $S$ denoted $< S >$.
If $G =< S >$ then we say $S$ generates G.

**1.32 Finitely generated group** - $G$ finitely generated if $\exists$ pos. integer $n$ s.t $G$ generated by $n$ elements.

# 2 Groups Acting on Sets

## 2.1 Actions, Orbits and Stabilisers

**Definition 2.1** **Action** - $G$ a group, $X$ a set. Let $S(X)$ be the group of bijections $X \to X$ with composition as the group law. An **action of $G$ on $X$ is a homomorphism $G \to S(X)$**
Associates each $g \in G$ to a bijective map $X \to X$, thought of as permutation of elements of X.

Equivalent to a function $G \times X \to X$, an action $\iff (g_1 g_2(x) = g_1(g_2(x)) \forall g_1, g_2 \in G$ and $x \in X$

**Definition 2.3** **Faithful actions** - an action of $G$ on $X$ is **faithful if $G \to S(X)$ is injective**
Equivalently, kernel of $G \to S(x)$ is trivial. $g(x) = g \forall x \implies g = e_G$

**Definition 2.4.1** **Orbit of elements** - Let $G \times X \to X$ an action of G on a set X. The $G$-orbit of $x \in X$ is $G(x) = \{g(x) | g \in G\} \subset X$

**Definition 2.4.2** **Stabiliser of $x$** - $\mathbf{St}_G(x) = \{g \in G | g(x) = x\} \subset G$

**Theorem 2.6** **Orbit-Stabiliser Theorem**
$G \times X \to X$ an action of $G$ on $X$. $\forall x \in X$ the map $g \mapsto g(x)$, gives bijection from set of left cosets $G/St(x) \to G(x)$, the orbit of $x$.
If $G$ a finite group $\implies |G(x)| = |G|/|St(x)| \forall x \in X$.
If $X$ a finite set and $X = \cup_{i=1}^{n} G(x_i)$ is a disjoint union of $G$-orbits, then

$$|X| = \sum_{i=1}^{n} |G(x_i)| = \sum_{i=1}^{n} [G : St(x_i)],$$

where $[G : St(x_i)]$ **is the index of $St(x_i)$ in G**

## 2.2 Applications of the orbit-stabiliser theorem

**Theorem 2.7** - *(Cayley).*
Let $G$ a finite group of order $n \implies S_n$ has a subgroup isomorphic to $G$

**Theorem 2.8** - *(Cauchy)*
$G$ a finite group of order $n$ with $p$ a prime factor of $n \implies$ G has an element of order $p$.

**Definition 2.9 - $p$-groups** - $p$ a prime, finite group $G$ is a $p$-group if order of $G$ is a power of $p$.
*Corollary 2.10* - $G$ a $p$-group $\iff$ order of every element of G is a power of $p$.

**Theorem 2.11.**
$G$ a $p$-group, $p$-prime. Then $Z(G) \neq \{e_G\}$

**Definition 2.13** - $G \times X \to X$ an action of $G$ on $X$. If $X = G(x)$ ($X$ a $G$-orbit) for some $x \in X$, then we say **$G$ acts transitively on $X$**.
**Definition 2.14** - Let $G \times X \to X$ an action of $G$ on $X$. If $x \in X$ s.t $g(x) = x$. **We say $x$ a fixed point**.
**Fix($g$) $\subset X$ - the set of fixed points of $g \in G$**

**Theorem 2.15** - *(Jordan)*
Let $G \times X \to X$ a transitive action of a finite group $G$ on a finite set $X$. Then:

$$\sum_{g \in G} |Fix(G)| = |G|$$

$\exists g \in G$ s.t $Fix(g) = \varnothing$
*Corollary 2.16* Let $G \times X \to X$ an action of a finite group $G$ on a finite set $X$ Then the number of $G$-orbits in $X$ is $|G|^{-1} \sum_{g \in G} |Fix(g)|$.

# 3 Finitely Generated Abelian Groups

## 3.1 Smith Normal form

**Definition 3.1 - Smith Normal Form**
$A = (a_{ij}) \in \mathbb{Z}$ a $(m \times n)$ matrix in **Smith Normal Form** if:

- $a_{ij} = 0$ if $i \neq j$ (only diagonal terms are non-zero)
- $a_i = a_{ii}$. For $k \geq 0, a_i > 0$ for $i \leq k, a_i = 0$, for $i > k$
- $a_1 | a_2 | \dots | a_k$

**Theorem 3.2**
Any Matrix of integer coefficients made into Smith Normal form via row/col operations.
Row Operations:

$1 \rightarrow$ Swap $i^{\text{th}}$ and $j^{\text{th}}$ row

$2 \rightarrow$ multiply $i^{\text{th}}$ row by $-1$

$3 \rightarrow$ replace $i^{\text{th}}$ row; $r_i$ by $r_i + ar_j,\ i \neq j,\ a \in \mathbb{Z}$

*Notation*

$$d(A) - \text{gcd of } (a_{ij})$$

$$t(A) - \text{smallest non-zero } |a_{ij}|$$

*Corollary*; $d(A) | t(A) \implies d(A) \leq t(A)$
*Lemma*; Any matrix $A$ of integer coefficients transformed via row/col operations to $B$ s.t $t(B) = d(B) = d(A)$

## 3.2 Classification of finitely generated abelian groups

**Definition 3.4 - Free abelian group of rank $n$**

$$\mathbb{Z}^n := \{(a_1, \dots, a_n) | a_i \in \mathbb{Z}\}$$

*Lemma*; $\mathbb{Z}^m \cong \mathbb{Z}^m \implies n = m$, shows rank is well defined
*Lemma*; Any subgroup of $\mathbb{Z}^n$ isomorphic to $\mathbb{Z}^m$ for $m \leq n$

***Corollary 3.7***
$G$ a finitely generated abelian group.
$\implies \exists$ surjective homomorphism $f : \mathbb{Z}^n \rightarrow$ some $n$
$\text{Ker}(f) \cong \mathbb{Z}^m$

**Theorem 3.8**
Every finitely generated abelian group is isomorphic to a product of finitely many cyclic groups
***Corollary - 3.10***; Any finite abelian group isomorphic to a product of its $p$-primary torsion subgroups.

**Theorem 3.11**
Every finitely generated abelian group isomorphic to a product of *finitely many infinite cyclic groups* and *finitely many cyclic groups of prime power order*
The number of infinite cyclic factors and the number of cyclic factos of order $p^r$, for $p \in \mathbb{P}, r \in \mathbb{N}_+$, depends only on the group.

# Part II
# Rings

## 4 Basic Theory of Rings

### 4.1 Motivation

**Definition 4.1 - Ring**
A ring a set $R$ with 2 binary operations, $+$ and $\times$, satisfying:

1. $(R, +)$ an abelian group
   $\hookrightarrow$ written additively; 0 an identity element, with $-x$ the inverse of $x$
2. Multiplication is **assosciative**
   $\hookrightarrow \forall a, b, c \in R \implies (a \cdot b) \cdot c = a \cdot (b \cdot c)$
3. $\exists!$ unit element for multiplication ; 1
   Satisfying: $1x = x1 = x \ \forall x \in R$
4. Distributivity
   $\hookrightarrow \forall a, b, c \in R; a(b + c) = ab + ac \ , (a + b)c = ac + bc$

$R$ is closed under both $+$ and $\times$
Say $R$ commutatitive if $xy = yx, \ \forall x, y \in R$ *Lemma 4.2 - Properties of rings*

- $\forall x \in R, x0 = 0x = 0$
- $\forall x, y \in R \implies (-x)y = x(-y) = -xy$
- $R \neq \{0\} \implies 1 \neq \{0\}$

**Definition 4.3 - Subring**
Subset of a ring which is a ring under the same $+, times$ and same 1 is a **subring**
***Lemma 4.4***
$S$ a non-empty subset of ring $R$ Then;
$S$ a subring of $R \iff 1 \in S$ and $\forall a, b \in S; a + b \in S, \ ab \in S, \ -a \in S$

**Definition 4.6 - Invertible Elements**
$x \in R$ invertible if $y, z \in R$ s.t $xy = 1$ and $zx = 1$
if $y = z$ denote $x^{-1} = y = z$
**Definition 4.6.2 - Multiplicative group of $R$**

$$R^{\times} = \{x \in R \mid x \text{ invertible}\}$$

**Definition 4.8 - Division Ring** A ring where all non-zero elements a **division ring**
**Definition 4.8.2 - Field**
A commutative division ring a **Field**.

### 4.2 Homomorphisms, ideals and quotient rings

**Definition 4.12 - Homomorphism of Rings**
$R, S$ rings. $f : R \to S$ a homomorphism of rings if

(i) $f : (R, +) \to (S, +)$ a homomorphism of abelian groups

(ii) $f(xy) = f(x)f(y)$

(iii) $f(1_R) = 1_S$

A subset $R'$ of $R$ a subring $\iff$ tautological map $R' \to R$ a homomorphism of rings

**Definition 4.16 - Ideal rings**
$R$ a ring, $I \subset R$ **ideal** if:

1. $I$ a subgroup of $(R, +)$ w.r.t $+$
2. $\forall x \in I,\ \forall r \in R \implies$
   - $I$ left ideal if only $rx \in I$
   - $I$ right ideal if only $xr \in I$
   - $I$ 2-sided ideal if $rx \in I$ and $xr \in I$

   Mostly consider commutative rings so one condition is often enough.

An ideal ring not equal to the whole ring a **proper ideal**

**Defintion 4.17 - Quotient Ring**
$R$ a ring, $I \subset R$ a proper ideal
Quotient abelian group, $R/I$ with multiplication as in $R$ called a **quotient ring** of $R$ by ideal $I$

**Definition 4.18 - Principal ideal**
$R$ a commutative ring.
Take $a \in R$, consider $aR = \{ax | x \in R\}$, this is an ideal in $R$, called the **principal ideal with generator** $a$

**Definition 4.19 - Types of homomorphisms**

1. A bijective homomorphism of rings $f : R \to S$ called an **isomorphism of rings**
2. A homomorphism of rings $R \to R$ an **endomorphism of rings**
3. An isomorphism of rings $R \to \sim R$ an **automorphism of rings**

**Theorem 4.20 - *(Isomorphism Theorem)***
Let $f : R \to S$ a homomorphism of rings.
Then subring $f(S)$ of $S$ is isomorphic to quotient ring $R/\text{Ker}(f)$

## 4.3 Integral domains and fields

**Definition 4.21. Zero-divisors**

$R$ a ring. non-zero elements $a, b \in R$ are called **zero divisors** if $ab = 0$

**Definition 4.21. Integral Domain**

Commutative ring without zero divisors an **integral domain**

**Lemma 4.23.**

$R$ an integral domain. $ab \in R$

$$aR = bR \iff a = br,\ r \in R^\times$$

**Proposition 4.24.**

Every field is an integral domain.

**Theorem 4.25.**

Every finite integral domain a field
***Corollary 4.26.***
$n \in \mathbb{N}_+$, ring $\mathbb{Z}/n\mathbb{Z}$ an integral domain $\iff n \in \mathbb{P}$

**Definition 4.27. Subfield**

subset $K$ of field $\mathbb{F}$ a **subfield of** $\mathbb{F}$ if $K$ a field with the same addition and multiplication as in $\mathbb{F}$.
Say $\mathbb{F}$ a **field extension** of $K$
**Proposition 4.28**
$\forall$ rings $R$, $\exists!$ homemomorphism of rings $\mathbb{Z} \to R$

**Lemma 4.29.**
$R$ an integral domain. kernel of unique homomorphism $\mathbb{Z} \to R$ either $0-$ideal; $\{0\} \subset \mathbb{Z}$ or principal ideal $p\mathbb{Z},\ p \in \mathbb{P}$

**Definition 4.30.** **Characteristic of integral domain**

Characteristic of integral domain $R$ is the unique non-negative generator of the kernel of a homomorphism $\mathbb{Z} \to R$; either 0 or $p \in \mathbb{P}$.
denoted $\text{Char}(R)$

**Definition 4.31.**

$k$ a field, $V$ an abelian group with an action of elements of $k$ (scalars) on elements of $V$ (vectors)
Where for $x \in k,\ v \in V,\ xv \in V$

(i) $1v = v$ and $x(yv) = (xy)v, \forall\ x, y \in k,\ v \in V$

(ii) $(x + y)v = xv + yv, \forall\ x, y \in k, v \in V$

(iii) $x(v + w) = xv + xw, \forall\ x \in k, \forall\ v, w\ inV$

**Lemma 4.32.**
field extension $\mathbb{F}$ of $k$ is a vector space over $k$

**Theorem 4.33.**

$k$ a field.
if $\text{char}(k) = 0 \implies k$ has unique subfield isomorphic to $\mathbb{Q} \implies k$ a vector space over $\mathbb{Q}$
if $\text{char}(k) = p \in \mathbb{P} \implies k$ contains unique subfield isomorphic to $\mathbb{F}_p \implies k$ a vector space over $\mathbb{F}_p$

***Corollary 4.34.***
Every finite field has $p^n$ elements, $p \in \mathbb{P},\ n \in \mathbb{N}_+$

## 4.4 More on ideals

**Proposition 4.35.**
A commutative ring a field $\iff$ only proper ideal is the zero ideal.

**Proposition 4.36.**
$f : R \to S$ a homomorphism of rings
$J \subset S$ an ideal $\implies f^{-1}(J)$ an ideal of $R$

**Proposition 4.37.**
$f : R \to S$ surjective homomorphism of rings.
$I \subset R$ an ideal $\implies f(I)$ an ideal of $S$
The maps

$$I \mapsto f(I) \qquad J \mapsto f^{-1}(J)$$

give a bijection between ideals of $R$ that contain $\ker(f)$ and ideals of $S$

**Definition 4.38.**

$R$ a commutative ring. We say a proper ideal $I \subset R$ a **prime ideal** if quotient ring $R/I$ an integral domain.
**Proposition 4.39.**

$R$ a commutative ring. Proper ideal $I \subset R$ a **maximal ideal** if quotient ring $R/I$ a field.
Every Maximal ideal a Prime ideal.
**Proposition 4.41.**

$I \subset R$ a maximal ideal $\iff$ there is no proper ideal $J \subset R$ s.t $I \subset J$ and $I \neq J$

# 5 PID and UFD

## 5.1 Polynomial rings

$R$ an integral domain. $R[t]$ the ring of polynomials in $t$ with coefficients in $R$.

$$R[t] = \{a_n t^n + a_{n-1}t^{n-1} + \cdots + a_1 t + a_0 | a_i \in R\} \quad n = deg(p(t))$$

**Proposition 5.1.**

$R$ an integral domain $\implies$

$$deg(p(t)q(t)) = deg(p(t)) + deg(q(t))$$

$R[t]$ an integral domain. $R[t]^\times = R^\times$

**Proposition 5.2.**

$k$ a field
$\forall a(t), b(t) \in k[t],\ b(t) \neq 0$
$\implies \exists! q(t), r(t) \in k[t]$ s.t

$$a(t) = q(t)b(t) + r(t)$$

$r(t) = 0$ or $deg(r(t)) < deg(b(t))$

**Definition 5.3.**

Integral domain $R$ with a function $\phi : R\backslash\{0\} \to \mathbb{Z}_{\geq 0}$ a **Euclidean domain** if

(i) $\phi(xy) \geq \phi(x) \quad \forall$ non-zero $x, y \in R$

(ii) $\forall a, b \in R,\ \exists q, r \in R$ s.t $a = qb + r$ where $r = 0$ or $\phi(r) < \phi(b)$

**Definition 5.4.**

Integral domain $R$ a **principal ideal domain (PID)** if every ideal of $R$ is principal. i.e of form $aR, a \in R$

**Theorem 5.5.**

Any euclidean domain is a PID.

## 5.2 Factorisation in Integral Domains

**Definition 5.5.**

$R$ an integral domain.
non-zero $x \in R\backslash R^\times$ an **irreducible element** if $x$ not a product of 2 elements of $R\backslash R^\times$
**Lemma 5.7.**
$R$ an integral domain.
if $x$ irreducible, $a \in R^\times \implies ax$ also irreducible

**Definition 5.8.**

An integral domain $R$ a **unique factorisation domain (UFD)** if every element of $R\backslash R^\times$ a product of finitely many irreducibles.
This decomposition is unique up to changing order of factors and multiplication of factors by elements in $R^\times$.
Also called **factorial rings**

**Definition 5.9.**

$R$ an integral domain. $a, b \in R$
Say $a \in R$ **divides** $b \in R$; $a|b$ if $b = ra,\ r \in R$
$a$ **properly divides** $b$ if $b = ra$ and $r \notin R^\times$
if $b = ra, r \in R^\times \implies a$ and $b$ **associates**
**Proposition 5.10.**
$R$ a UFD $\implies \nexists$ infinite sequence of non-zero elements $r_1, r_2, \ldots$ of $R$ s.t $r_{n+1}$ properly divides $r_n\ \forall n \geq 1$
**Proposition 5.11.**
Let $R$ be a UFD. If $p$ is irreducible and $p|ab \implies p|a$ or $p|b$

**Theorem 5.12.**

$R$ an integral domain. $R$ a UFD $\iff$

(i) There is no infinite sequence $r_1, r_2, \ldots$ of elements of $R$ such that $r_{n+1}$ properly divides $r_n$ $\forall n \geq 1$

(ii) For every irreducible elements $p \in R$ if $p|ab \implies p|a$ or $p|b$

**Proposition 5.14.**
Suppose $R$ a PID and $I_1 \subset I_2 \subset \ldots$ are ideals in $R$ Then for some $n$ we have $I_n = I_n + 1 = \ldots$.
We say that an ascending chain of ideals **stabilises**
**Proposition 5.16.**
Suppose $R$ a PID. $p \in R$ an irreducible element such that $p|ab \implies p|a$ or $p|b$

**Theorem 5.17.**

Every PID is a UFD.

# 6 Fields

## 6.1 Field extensions

**Definition 6.1.**

An extension of fiels $k \subset K$ is called **finite** if $K$ a finite-dimensional vector space over $k$
$dim_k(K) =$ **degree** of the extension. We write $[K : k] = dim_k(K)$

**Theorem 6.2.**

$k \subset F$ and $F \subset K$ field extensions. Then $K$ a finite extension of $k \iff F$ a finite extension of $k$ and $K$ a finite extension of $F$
i.e we have $[K : k] = [K : F][F : k]$

## 6.2 Constructing fields from irreducible polynomials

**Proposition 6.3.**

Let $R$ a PID and let $a \in R, a \neq 0$.
$aR$ maximal $\iff$ $a$ irreducible.

**Corollary 6.4.**
$R$ a PID and $a \in R$ irreducible then $R/ar$ a field.

**Proposition 6.6.**
Let $k$ a field. A polynomial $f(t) \in k[t]$ of degree 2 or 3 irreducible $\iff$ has no roots in $k$

**Proposition 6.8.**
$p \neq 2$ prime. Field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ contains $(p-1)/2 \geq 1$ non-squares.
$\forall a \in \mathbb{F}_p$ non-square we have $t^2 - a$ irreducible in $F_p[t]$ with $F_p[t]/(t^2 - a)\mathbb{F}_p[t]$ a quadratic extension of $\mathbb{F}_p$

## 6.3 Existence of finite fields

**Lemma 6.10**

$k$ a field s.t $char(k) = p$, $p$ a prime. $\forall x, y \in k$

$$(x + y)^{p^m} = x^{p^m} + y^{p^m}$$

$\forall x, y \in k,\ m \in \mathbb{Z}$
**Lemma 6.11**
$k$ a field $p(t) = (t - \alpha_1) \ldots (t - \alpha_n)$ for $\alpha_i \in k, i \in \{1, \ldots, n\}$
Then $\alpha_i \neq \alpha_j$ for $i \neq j \iff p(t), q(t)$ have no common root.

**Theorem 6.12.**

Let $p$ prime, $n \in \mathbb{Z}_+$

$$\exists \text{ field of } p^n \text{ elements.}$$