Chapter 1

Groups and Rings

Lectured by Someone
Typed by Yu Coughlin
Autumn 2024

Introduction

The following are complementary reading for the course.

- G. Grimmett and D. J. A. Welsh, Probability: An Introduction, 1986
- J. K. Blitzstein and J. Hwang, Introduction to Probability, 2019
- D. F. Anderson et al, Introduction to Probability, 2018
- S. M. Ross, Introduction to Pro ability Models, 2014
- G. Grimmett and D. Stirzaker, Probability and Random Processes, 2001
- G. Grimmett and D. Stirzaker, One Thousand Exercises in Probability, 2009

Contents

1 Quotient groups

1.1 Group homomorphisms

Definition 1.1.1 (Group isomorphism)**.** Given groups G, H, a function $f : G \to H$ is a **group isomorphism** if it is a bijective group homomorphism. If there exists an isomorphism between groups, G is **isomorphic** to H written $G \cong H$.

Definition 1.1.2 (Group automorphism)**.** Given G a group, an isomorphism $f : G \xrightarrow{\sim} G$ is a **group automorphism**.

Theorem 1.1.3. $\operatorname{Aut} G$ (the set of automorphisms of a group G) is a group under function composition.

Proof. By examining the defintion of $\operatorname{Aut} G$, taking $e = \mathrm{id}$ and showing association elementwise. □

Theorem 1.1.4. Given groups G, H, if $f : G \xrightarrow{\sim} H$ then $f^{-1} : H \xrightarrow{\sim} G$.

Proof. $f^{-1}(f(g_1))f^{-1}(f(g_2)) = g_1g_2 = f^{-1}(f(g_1g_2)) = f^{-1}(f(g_1)g(g_2))$ is sufficient as f is surjective. □

1.2 Normal subgroups

Definition 1.2.1 (Normal subgroup)**.** A sugroup N of G is **normal**, written $N \trianglelefteq G$, if it satisfies any of these equal properties:

(N1) N is the kernel of some group homomorphism ϕ,

(N2) N is stable under conjugations ($\forall n \in N$ and $g \in G$, $gng^{-1} \in N$),

(N3) for all $g \in G$ $gN = Ng$.

Proof of equivalence. (N1 $\implies$ N2): $\phi(gng^{-1}) = \phi(g)\phi(n)\phi(g^{-1}) = \phi(g)\phi(g)^{-1} = e_H$.

(N2 $\implies$ N3): $gng^{-1} \in N \implies gn \in Ng$ by g^{-1} so $gN \subseteq Ng$, similarly for $Ng \subseteq gN$ with g^{-1} replacing g.

(N3 $\implies$ N2): The set of left and right cosets of G by N are isomorphic with N as the kernel. □

1.3 Quotient groups

Definition 1.3.1 (Quotient groups)**.** Let $N \trianglelefteq G$, the **quotient group** of G modulo N, written G/N, is the group with elements as left cosets of N in G with $(g_1N) \cdot (g_2N) = (g_1g_2N)$.

Proof. One can easily check this satisfies all of the group axioms. □

Remark 1.3.2. By Lagrange's theorem $|G/N| = |G|/|N|$.

Definition 1.3.3 (Simple group)**.** A group G is **simple** if it has no normal subgroups except $\{e_G\}$ and G.

1.4 Isomorphism theorems

Theorem 1.4.1 (First isomorphism theorem)**.** If $f : G \to H$ is a group homomorphism, $G/\ker f \cong \operatorname{im} f$.

Proof. Have $\phi : G/\ker f \to \operatorname{im} f$ with $\phi : g \ker f \mapsto f(g)$.

well defined: if $g \ker f = h \ker f$, $gh^{-1} \ker f = \ker f \implies f(g) = f(gh^{-1}h) = f(gh^{-1})f(h) = f(h)$.

homomorphism: $\phi((g \ker f)(h \ker f)) = \phi(gh \ker f) = f(gh) = f(g)f(h) = \phi(g \ker f)\phi(h \ker f)$.

surjective: any $h = f(g) \in \operatorname{im} f$ is clearly $\phi(g \ker f)$ for any $g \in G$.

injective: if $\phi(g \ker f) = e_H$, $f(g) = e_H \implies g \in \ker f$ so $\ker f = \{\ker \phi\} = \{e_{G/\ker \phi}\}$. By a lemma from *Linear algebra and groups*, we now have ϕ injective. □

Theorem 1.4.2 (Universal property of quotients)**.** Let $N \trianglelefteq G$ and $f : G \to H$ be a group homomorphism such that $N \subseteq \ker f$. There exists a *unique* homomorphism $\tilde{f} : G/N \to H$ such that the diagram

$$\begin{tikzcd} G \arrow[d, "\pi"'] \arrow[dr, "f"] & \\ G/N \arrow[r, dashed, "\tilde{f}"'] & H \end{tikzcd}$$

commutes, (here $\pi : G \to G/N$ is the projection map with $\pi : g \to gN$).

Proof. The proof is essentially that of Theorem 1.4.1 with $H = \operatorname{im} f$. □

Lemma 1.4.3. If $N \trianglelefteq G$ and $N \leq H \leq G$ then $N \trianglelefteq H$.

Proof. $gN = Ng$ for all $g \in G$ so also for all $g \in H$. □

Theorem 1.4.4 (Second isomorphism theorem)**.** Let $K, L \trianglelefteq G$ with $K \leq L$, $G/L \cong (G/K)/(L/K)$

Proof. Have $f : G/K \to G/L$, via same arguments in Theorem 1.4.1, f is a surjective group homomorphism, $gK \in \ker f \implies f(gK) = gL = L$ so $g \in L$ and $\ker f = L/K$. By Theorem 1.4.1, $(G/K)/(\ker f) = (G/K)/(L/K) \cong (G/L)$. □

Definition 1.4.5 (Frobenius product)**.** Given $A, B \subseteq G$ a group, the **(Frobenius) product** of A and B is

$$AB := \{ab \in G : a \in A, b \in B\}.$$

Lemma 1.4.6. Given $H, N \leq G$ a group, N is normal $\implies HN \leq G$ and N, H normal $\implies HN \trianglelefteq G$.

Proof.

1. HN is nonempty with $(h_1n_1)(h_2n_2) = (n_1n_3)(h_1h_2) \in NH$ for some $n_3 \in N$ and $(hn)^{-1} = n^{-1}h^{-1} \in Nh^{-1} = h^{-1}N \subseteq HN$.
2. $gHNg^{-1} = gHg^{-1} \cdot gNg^{-1} = HN$. □

Theorem 1.4.7 (Third isomorphism theorem)**.** If $H \leq G$ and $N \trianglelefteq G$, $H/(H \cap N) \cong (HN)/N$. This is ometimes called the *diamond theorem* due to the shape of the subgroup lattice it produces:

$$\begin{tikzcd} & G \arrow[d] & \\ & HN \arrow[dl] \arrow[dr] & \\ H \arrow[dr] & & N \arrow[dl] \\ & H \cap N \arrow[d] & \\ & \{e_G\} & \end{tikzcd}$$

where arrows point to subgroups.

Proof. Have $\phi : H \to G/N$ be the canonical map, $\ker \phi = H \cap N$ as $hN = N$ iff $h \in N$, $\operatorname{im} \phi = \{hN : h \in H\} = HN/N$, Theorem 1.4.1 on ϕ gives the result. □

Note 1.4.8. The naming of the group isomorphism theorems throughout literatue is very inconsistent.

1.5 Centres

Definition 1.5.1 (Inner automorphisms). Given the group G the conjugations by elements of G form the group $\operatorname{Inn} G \trianglelefteq \operatorname{Aut} G$.

Proof. Have $\phi : G \to \operatorname{Aut}(G)$ assigning to each element in $g \in G$ the conjugation map by G, $\operatorname{Inn}(G) = \operatorname{im} \phi \subseteq \operatorname{Aut}(G)$. □

Definition 1.5.2 (Centre of group). Given the group G the elements of G that commute with all other elements form the **centre** of G, $Z(G) \trianglelefteq G$.

Proof of normality. Have $\phi : G \to \operatorname{Aut} G$ with $\phi : g \mapsto$ conjugation by g, $\ker \phi = Z(G)$. □

Proposition 1.5.3. If $G/Z(G)$ is cyclic, G is Abelian.

Proof. $G/Z(G) = \langle aZ(G) \rangle$ for some $a \in G$, for all $g \in G$ $gZ(G) = [aZ(G)]^m = a^m Z(G)$ for some $m \in \mathbb{N}$ therefore $a^{-m}g = z \in Z(G)$ so $g = a^m z$ and for all $g, h \in G$ we have $gh = a^n z_g a^m z_h = a^{n+m} z_g z_h = a^m z_h a^n z_g = hg$. □

1.6 Commutators

Definition 1.6.1 (Commutator). For $a, b \in G$ a group, we have $[a, b] := aba^{-1}b^{-1}$ the **commutator** of a and b. $[G, G]$ is the smallest subgroup of G containing all commutators of elements of G, called the **commutator** of G.

Remark 1.6.2. A group G is Abelian iff $[G, G] = e_G$.

Theorem 1.6.3. Given G a group, $[G, G] \trianglelefteq G$ with its quotient in G Abelian.

Theorem 1.6.4. Let $N \trianglelefteq G$, G/N is Abelian iff $[G, G] \subseteq N$.

Theorem 1.6.5. Given a group G with $A, B \trianglelefteq G$, $A \cap B = \{e_G\}$ and $AB = G$; $A \times B \cong G$.

1.7 Torsion and p-primary subgroups

Definition 1.7.1 (Torsion subgroup). Given an abelian group G, the set of elemnts of G with finite order form the **torsion subgroup** of G, denoted G_{tors}. When $G = G_{\text{tors}}$, we call G a **torsion Abelian group**.

Definition 1.7.2 (p-primary subgroups). Given an abelian group G, the set of elements of g with order p (a prime) is the **p-primary subgroup** of G, written $G\{p\}$. When $G = G_G\{p\}$, we call G a **p-primary torsion Abelian group**.

Theorem 1.7.3. Let the prime factorisation of $n \in \mathbb{N}$ be $p_1^{a_1} p_2^{a_2} \dots p_m^{a_m}$ with C_n the cyclic group of order n.

$$C_n \cong C_{p_1^{a_1}} \times C_{p_2^{a_2}} \times \cdots \times C_{p_m^{a_m}}.$$

Proof. □

1.8 Generators

Lemma 1.8.1. Given an indexing set $\mathcal{I}$, and a sequence of subgroups $(H_i)_{i \in \mathcal{I}} \leq H$, $\bigcap_{i \in \mathcal{I}} H_i \leq G$.

Definition 1.8.2 (Subgroup generated by a set). Given $S \subseteq G$ a group,

$$\langle S \rangle := \left(\bigcap_{S \subseteq H \leq G} H \right) \leq G$$

is the **subgroup of G generated by S**. If $\langle S \rangle = G$ then we say S **generates** G and G is **finitely generated** is S is finite.

1.9 Classification of finitely generated Abelian groups

Definition 1.9.1 (Free Abelian group of rank n)**.** The **Free Abelian group of rank** n is the group $\mathbb{Z}^n$ under addition. The free abelian group of rank 0 is the trivial group.

Lemma 1.9.2. If $\mathbb{Z}^m \cong \mathbb{Z}^n$ then $n = m$, so the rank of a free abelian group is well defined.

Lemma 1.9.3. Any subgroup of $\mathbb{Z}^n$ is isomorphic to some $\mathbb{Z}^m$ for some $m \leq m$.

Theorem 1.9.4. Every finitely generated Abelian group is isomorphic to a product of finitely many cyclic groups.

Theorem 1.9.5. Every finitely generated Abelian group is isomorphic to a product of finitely many infinite cyclic groups and finitely many cyclic groups of prime order. The number of ininfite cyclic factors and the number of cclic factors of order p^r, where p is primse and $r \in \mathbb{N}$ is determined solely by the group.

Theorem 1.9.6. A finitely generated Abelian group, G, is not cyclic iff there exists a prime p such that $G \cong C_p \times C_p$.

2 Group actions

2.1 Actions

Definition 2.1.1 (Actions)**.** Given a group G and a set X, a **group action** is: a binary operation

$$\begin{array}{rccc} \cdot & : & G \times X & \longrightarrow & X \\ & & (g, x) & \longmapsto & g \cdot x \end{array}$$

with $e_G \cdot x = x$ for all $x \in X$ and $(g_1 g_2) \cdot x = g_1 \cdot (g_2 x)$ for all $g_1, g_2 \in G$ and $x \in X$; or, equivalently, a homomorphism $\rho : G \to \operatorname{Sym}(X)$.

Definition 2.1.2 (Faithful set)**.** An action of a group G on a set X is **faithful** if the map $\rho : G \to \operatorname{Sym}(X)$ is injective.

2.2 Orbit-stabiliser theorem

Definition 2.2.1 (Orbit)**.** Given a group G acting on a set X, the G**-orbit** of $x \in X$ is

$$G(x) := \{g \cdot x : g \in G\} \subseteq X.$$

Orbits partition X into X/G.

Definition 2.2.2 (Stabiliser)**.** Given a group G acting on a set X, the **stabiliser** of $x \in X$ is

$$\operatorname{Stab}_G(x) := \{g \in G : g \cdot x = x\} \subseteq G.$$

Stabilisers also partition G.

Remark 2.2.3 (Conjugacy classes)**.** When G acts on itself by conjugations, orbits of G are the **conjugacy classes**, x^G of G and the stabilisers of G are the centralisers of G.

Lemma 2.2.4. Given a group G acting on a set X, $\operatorname{Stab}_G(g \cdot x) = g \operatorname{Stab}_G(x) g^{-1}$

Theorem 2.2.5 (Orbit-stabiliser theorem)**.** Given a group G acting on a set X. For all $x \in X$, we have $\phi_x : G/\operatorname{Stab}(x) \xrightarrow{\sim} G(x)$ by $\phi_x : g \operatorname{Stab}(x) \mapsto g \cdot x$, giving $|G(x)| = [G : \operatorname{Stab}(x)] = |G|/|\operatorname{Stab}(x)|$.

Proof. asdfsd □

Corollary 2.2.6. $|X| = \sum_{i=1}^{n} |G(x_i)| = \sum_{i=1}^{n} [G : \operatorname{Stab}(x_i)]$.

Corollary 2.2.7 (Cayley's theorem)**.** Let G be a finite group of order n. Then S_n contains a finite subgroup isomorphic to G.

Corollary 2.2.8 (Cauchy's theorem)**.** Let G be a finite group of order n and let p be a prime factor of n. Then G contains an element of order p.

Definition 2.2.9 (p-group)**.** A finite group G is a p**-group** is the order of G is a power of prime p.

Theorem 2.2.10. Let G be a p-group, $Z(G) \neq \{e_G\}$.

Proof. □

2.3 Jordan's theorem

Definition 2.3.1 (Transitive action)**.** Given a group G acting on a set X, if X is a G-orbit then we say G acts **transitively** on X.

Definition 2.3.2 (Fixed points)**.** Given a group G acting on a set X, an element $x \in X$ is a fixed point of $g \in G$ iff $g \cdot x = x$. We have $\mathrm{Fix}(g) \subseteq X$ the set of fixed points of $g \in G$ satisying:

$$\mathrm{Stab}(x) \xleftarrow[\pi_G]{} \{(x, g) \in X \times G;\ g \cdot x = x\} \xrightarrow[\pi_X]{} \mathrm{Fix}(g)\ .$$

Theorem 2.3.3 (Jordan's theorem)**.** Let G act transitively on a finite set X, we have

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

with there being some element $g \in G$ such that $\mathrm{Fix}(g) = \emptyset$.

Corollary 2.3.4 (Burnside's lemma)**.** Given a group G acting on a finite set X:

$$|X/G| = \frac{1}{|G|} \sum_{g \in G} |\,\mathrm{Fix}(g)|.$$

3 Rings

3.1 Rings

Definition 3.1.1 (Ring)**.** A ring (with 1) is a set R with elements $0, 1$ and binary operations $+, \times$ such that

1. $(R, +)$ is an abelian group with identity 0,
2. $(R, \times)$ is a semigroup with 1 as the identity,
3. both left and right multiplication are distributive over addition.

Examples 3.1.2. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ are all rings with their normal operations. $\mathbb{R}[x]$ is the set of real-valued polynomials and is also a ring.

Definition 3.1.3 (Subring)**.** A subset of a ring wich is itself a ring under the same operators with the same 1 is a **subring**.

Definition 3.1.4 (Commutative ring)**.** A ring, R, is **commutative** iff $a + b = b + a$ for all $a, b \in \mathbb{R}$.

Definition 3.1.5 (Invertible)**.** An element x of a ring R is invertible if there exists $y, z \in R$ with $yx = zx = 1$.

Definition 3.1.6 (Division ring)**.** A ring R is called a **division ring** if $R \backslash \{0\}$ is a group under multiplication with identity 1.

Remark 3.1.7. A commutative division ring is a field.

Definition 3.1.8 (Integral domain)**.** A commutative ring R is an integral domain iff $0 \neq 1$ and for all $a, b \in R$ $ab = 0 \implies a = 0$ or $b = 0$.

3.2 Ring homomorphisms

Definition 3.2.1 (Ring homomorphism)**.** Let R, S be rings, a function $f : R \to S$ is a **ring homomorphism** iff it satisfies

1. $f : (R, +) \to (S, +)$ is a group homomorphism,
2. $f(xy) = f(x)f(y)$ for all $x, y \in R$,
3. $f(1_R) = 1_S$.

Lemma 3.2.2. Given the ring homomorphism $f : R \to S$ the kernel of f is a subgroup of $(R, +)$ which satisfies $xr, rx \in \ker f$ for all $x \in \ker f$ and $r \in R$.

3.3 Ideals

Definition 3.3.1 (Ideal)**.** For a ring R, a subset $I \subseteq R$ is a **left ideal**, denoted $I \trianglelefteq R$ iff

1. $(I, +)$ is a subgroups of $(R, +)$,
2. if $r \in R$ and $i \in I$, $ri \in R$.

Similarly, for **right ideals**. A subset I is a bi-ideal if it is both a left and right ideal.

Definition 3.3.2 (Quotient ring)**.** Given ring R with proper ideal $I \subset R$, The quotient abelian group R/I, with natural multiplication, forms the **quotient ring** of R by I.

Definition 3.3.3 (Principal ideal)**.** Given a commutative ring R and some $a \in R$, $aR := \{ax : x \in R\}$ is an ideal called a **principal ideal** with **generator** a.

Definition 3.3.4. A bijective ring homomorphism is a **ring isomorphism**, a ring homomorphism $f : R \to R$ is a **ring endomorphism**, an isomorphic ring endomorphism is **ring automorphism**.

Proposition 3.3.5. Given the ring homomorphism $f : R \to S$, $f(R) = \operatorname{im} R$ is a subring of S which is isomorphic to $R/\ker f$.

Proposition 3.3.6. A commutative ring is a field iff its only proper ideal is the trivial / zero ideal.

Proposition 3.3.7. Given $f : R \to S$ a ring homomorphism with J a left (or right or bi) ideal of S, $f^{-1}(J)$ is a left (respectively) ideal of R.

Definition 3.3.8 (Prime ideal)**.** Let R be a commutative ring, a proper ideal $I \subset R$ is a **prime ideal** iff $ab \in I$ for $a, b \in R \implies a \in I$ or $b \in I$.

Theorem 3.3.9. If $I \subset R$ is a prime ideal, R/I is an integral domain

Definition 3.3.10 (Maximal ideal)**.** A proper ideal I in a commutative rign R is **maximal** iff there are no other proper ideals J with $I \subset J$.

Theorem 3.3.11. I is a maximal ideal of R iff R/I is a field.

4 Integral domains

Throughout this section we will always have R be an integral domain.

4.1 Integral domains

Theorem 4.1.1. $ab = ac \implies b = c$ for all $a, b, c \in R$. (the cancellation law holds for all integral domains)

Proposition 4.1.2. For $a, b \in R$, $aR = bR$ iff $a = br$ for some $r \neq 0 \in R$.

Proof. □

Theorem 4.1.3. All fields are integral domains and all finite integral domains are fields.

Remark 4.1.4. The ring $\mathbb{Z}/n\mathbb{Z}$ is an integral domain iff it is a field $\iff$ n is prime.

Definition 4.1.5 (Unit)**.** $r \in R$ is a **unit** if there exists some $y \in R$ with $x \times y = 1_R$. We write $R^\times$ for the group of units in R under multiplication.

Definition 4.1.6 (Irreducible)**.** $r \in R \setminus R^\times$ is **irreducible** if it cannot be written as the product of two elements of $R \setminus R^\times$.

4.2 Charateristic

Lemma 4.2.1. For any ring S there is a uniqure ring homomorphism $f : \mathbb{Z} \to S$.

Proof. Have $f(0_R) = 0$, $f(1) \to 1_S$ and inductively have $f(n)$ be the sum of 1_S n times. □

Lemma 4.2.2. The kernel of the unique homomorphism $\mathbb{Z} \to R$ is either $\{0\}$ or $p\mathbb{Z}$ for some prime p.

Definition 4.2.3 (Charateristic)**.** The **characteristic** of R is the unique non-negative generator of the kernel of $\mathbb{Z} \to R$, denoted $\text{char } R$.

4.3 Polynomial rings

Definition 4.3.1 (Polynomial ring)**.** $R[t]$ is, formally, the set of infinite sequences of elements of R with finitely many non-zero terms, but more helpfully: the set of polynomials in t with coefficients in R.

Definition 4.3.2 (Polynomial degree)**.** The **degree** of a polynomial, $r_0 + r_1 t + r_2 t^2 + \ldots + r_i t^i + \ldots \in R[t]$, is the unique maximum $i \in \mathbb{N}$ with $r_i \neq 0$ and 0 otherwise.

Lemma 4.3.3. Given $p(t), q(t) \in R$, $\deg(p(t)q(t)) = \deg(p(t)) + \deg(q(t))$, $R[t]$ is an integral domain and $R[t]^* = R^*$.

Theorem 4.3.4. If k is a field with $a(t), b(t) \in k[t]$ with $b(t) \neq 0$, there exists $q(t), r(t) \in k[t]$ such that $a(t) = q(t)b(t) = r(t)$ with $\deg(r(t)) < \deg(b(t))$ and $q(t), r(t)$ unique.

5 PIDs and UFDs

5.1 Euclidian domains

Definition 5.1.1 (Euclidian domain)**.** An integral domain R is a Euclidian domain if there exists some $\phi : R^* \to \mathbb{N}_0$ satsifying:

1. $\phi(ab) \leq \phi(a)$ for all $a, b \neq 0$,
2. for all $a, b \in R$ there exists $q, r \in R$ with $a = qb + r$ with $r = 0$ or $\phi(r) \leq \phi(b)$.

5.2 Principal ideal domains

Definition 5.2.1 (Principal integral domain)**.** An integral domain R is a **principal integral domain** iff every ideal of R is principal.

Theorem 5.2.2. R is a Euclidian domain $\implies$ R is a principal integral domain.

Proof. □

Corollary 5.2.3. F is a field $\implies$ $F[t]$ is a PID.

5.3 Unique factorisation domains

Definition 5.3.1 (Unique factorisation domain)**.** An integral domain R is a **unique factorisation domain** iff every element of $R \setminus R^\times$ can be written as the product of a single unit and finitely many irreducibles in R which is unique up to rearrangement.

Definition 5.3.2 (Division)**.** Given a, b in the integral domain R, we say a **divides** b, written $a|b$ iff $b = ra$ for some $r \in R$ and **properly divides** if $r \notin R^\times$.

Lemma 5.3.3. Given $p, a, b \in R$ a UFD, if p is irreducible then $p|ab \implies p|a$ or $p|b$.

Lemma 5.3.4. There is no infinite sequence of non-zero $r_1, r_2, \ldots \in R$ a UFD such that r_{n+1} properly divides r for all $n \geq 1$.

Theorem 5.3.5. The integral domain R is a UFD iff the properties in Lemma 5.3.3 and Lemma 5.3.4 hold.

Theorem 5.3.6. Every principal ideal domain is a unique factorisation domain.

6 Fields

6.1 Vector spaces

Throughout this section let k be a field.

Definition 6.1.1 (Vector space)**.** A k-vector space V is an abelian group with an action of k on the elements of V satisfying

1. $1_k v = v$ for all $v \in V$,
2. $(x + y)V = xv + yv$ for all $x, y \in k$ and $v \in V$,

3. $x(v+w) = xv + xw$ for all $x \in k$ and $v, w \in V$.

Proposition 6.1.2. If $\operatorname{ch} k = 0$ then k contains a unique subfield isomorphic to $\mathbb{Q}$. Otherwise, if $\operatorname{ch} k = p$ then k contains a unique subfield isomorphic to $\mathbb{F}_p$.

Theorem 6.1.3. Every finite field has p^n elements for some prime p and $n \in \mathbb{N}$.

6.2 Field extensions

Definition 6.2.1 (Field extension)**.** A **field extension** F of k is a k-vector space.

Proposition 6.2.2. All homomorphisms between fields and rings are injective.

Proof. The only possible maps between fields are field extensions, the only proper ideal of a field is the zero ideal. □

Definition 6.2.3 (Finite field extension)**.** An extension of the fields $k \subset K$ is **finite** iff K is a finite dimensional vector space over k with $\dim K$ the **degree** of the extension

Theorem 6.2.4. If $k \subset F \subset K$ are field extensions, K is a finite extension of k iff K is a finite extension of F and F is a finite extension of k. We then have $[K : k] = [K : F][F : k]$.

Remark 6.2.5. Degree 2 and 3 field extensions are called quadratics and cubics respectively.

6.3 Constructing fields

Lemma 6.3.1. Given R a PID with $a \neq 0 \in R$, aR is maximal iff a is irreducible.

Proof. □

Corollary 6.3.2. Given R a PID with reducible $a \in R$, R/aR is a field.

Theorem 6.3.3. A polynomial $f(t) \in k[t]$ of degree 2 or 3 is irreducible iff it has no root in k.

Definition 6.3.4 (Non-Square)**.** $a \in k$ is non-square if there is no element $b \in k$ with $b^2 = a$.

Lemma 6.3.5. Let p be an odd prime. The field $\mathbb{F}_p$ contins $(p-1)/2$ non-squares. For all non-square $a \in \mathbb{F}_p$, $t^2 - a$ is irreducible in $\mathbb{F}_p[t]$.

Theorem 6.3.6. For all $p(t) \in k[t]$, there exists a finite field extension $k \subset K$ such that:

$$p(t) = c\prod_{i=1}^{n}(t - a_i),$$

for some $c \in k^\times$ and $a_i \in K$ for all $i \in [1, n]$.

6.4 Existence of finite fields

Theorem 6.4.1. Let k have characteristic $p \neq 0$, for all $x, y \in k$ and $m \in \mathbb{Z}^{\geq 0}$,

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

Definition 6.4.2 (Derivative)**.** Let $p(t) = a_0 + a_1 t + \ldots + a_n t^n \in k[t]$, the **derivative** of $p(t)$ is

$$p'(t) := a_1 + 2a_2 t + \ldots + n a_n t^{n-1}.$$

Lemma 6.4.3. Let $p(t) = (x - a_1)(x - a_2)\ldots(x - a_n) \in k[t]$, $a_i \neq a_j$ for all $i \neq j$ iff $p(t)$ and $p'(t)$ have no common roots.

Theorem 6.4.4. For all prime p and natural n, there exists a field with p^n elements.