Y3 Revision - Rings!

Apiros3

First Version : Mar 11, 2025
Last Update : Jan 29, 2025

Contents

1 Introduction

1.1 Basic Definitions

In this note we assume rings are associative, commutative, and unitary. Ring homomorphisms are also unitary (sending 0_R to 0_S).

Definition 1.1.1. *Let R be a ring. Let $I \subseteq R$ is an ideal in R. I is **proper** if $I \neq R$ and I is **principal** if it can be generated by a single element.*

Definition 1.1.2. *An element $r \in R$ is **nilpotent** if there exists an integer $n \geq 1$ such that $r^n = 0$.*

Definition 1.1.3. *A ring R is **local** if it has a single maximal ideal $\mathfrak{m}$. In this case, every element in $R \backslash \mathfrak{m}$ is a unit.*

Definition 1.1.4. *The **prime ring** of a ring R is the image of the unique (unitary) homomorphism $\mathbb{Z} \to R$.*

Definition 1.1.5. *The **zero divisor** of a ring R is an element $r \in R$ such that there exists a $r' \in R \backslash \{0\}$ with $r \cdot r' = 0$. If R is not the zero-ring, 0 is always a zero divisor of R.*

Definition 1.1.6. *A **domain** is a ring R with the property that the set of zero divisors consists only of 0. (In the case it is commutative, we call it an **integral domain**).*

Definition 1.1.7. *A **Unique Factorization Domain** (UFD) or a factorial ring is a domain R which has a unique factorization of non-zero elements with irreducible elements up to permutation and multiplication by units.*

Definition 1.1.8. *Given rings R and T, T is said to be an R-algebra if there is a homomorphism of rings $R \to T$.*

Note that an R-algebra T carries the structure of an R-module using the map provided by the homomorphism.

Definition 1.1.9. *Given $\phi_1 : R \to T_1$ and $\phi_2 : R \to T_2$ to be two R-algebras, a homomorphism of R-algebras is a homomorphism of rings $\lambda : T_1 \to T_2$ such that $\lambda \circ \phi_1 = \phi_2$.*

Definition 1.1.10. *An R-algebra $\phi : R \to T$ is said to be **finitely generated** if there exists an integer $k \geq 0$ and a surjective homomorphism of R-algebras $R[x_1, \ldots, x_k] \to T$ (evaluation of variables) where the polynomial is R if $k = 0$.*

Proposition 1.1.11. *Given that $R \to T$ is a finitely generated R-algebra and $T \to W$ is also a finitely generated T-algebra, the composed map from $R \to W$ is a finitely generated R-algebra.*

Proof. TODO!! □

Definition 1.1.12. *Let M be a R-module and $S \subseteq M$. Then,*

$$\mathrm{Ann}_M(S) = \{r \in R \mid rm = 0 \forall m \in S\}$$

*The set $\mathrm{Ann}_M(S)$ is an ideal of R and is called the **annihilator** of S.*

Definition 1.1.13. *A **poset (partially ordered set)** is a set equipped with an operator $\leq$ which is reflexive, transitive and antisymmetric. It is called a **total order** if it is also connex. We call the operator a **partial order**.*

Definition 1.1.14. *Let $T \subseteq S$. An element $s \in S$ is an* ***upper bound*** *of T if for any $t \in T$, $t \leq s$. An element $s \in S$ is a* ***maximal element*** *of S if for any $t \in S$, $s \leq t$ if and only if $s = t$. Similarly, $s \in S$ is a* ***minimal element*** *if $t \leq s$ if and only if $t = s$.*

Remark 1.1.15. Given a poset S and $T \subseteq S$, the relation $\leq$ on S restricted to elements of T gives a poset on T.

Proposition 1.1.16 (Zorn's Lemma (Equivalently, AC))**.** *Let S be a poset. If every $T \subseteq S$ that is totally ordered (with restriction of $\leq$ on T) has an upper bound in S, then there exists a maximal element in S.*

Proof. TODO!! (set theory stuff, ask cs phil) □

Proposition 1.1.17. *Let R be a ring and $I \subsetneq R$ be a proper ideal. Then, at least one of the maximal ideals of R contains I.*

Proof. Let S be the set of all proper ideals containing I. Give a partial order on S by inclusion. For any $T \subseteq S$ with T totally ordered, then T has an upper bound $\bigcup_{J \in T} J$ is a proper ideal containing I. It is proper as otherwise we have $1 \in J$ for some $J \in T$. Thus, by Zorn's Lemma, there exists a maximal element $\mathfrak{m}$ in S.

By definition, whenever $\mathfrak{m} \subseteq J$ and J is a proper ideal containing I, we have $\mathfrak{m} = J$. If J does not contain I, as $\mathfrak{m}$ contains I, $\mathfrak{m} \nsubseteq J$. Hence, $\mathfrak{m}$ is maximal and contains I. □

2 Localisation

2.1 Localisation of Rings

Definition 2.1.1. *A subset S of R is said to be **multiplicative** or a **multiplicative set** if $1 \in S$ and $xy \in S$ whenever $x \in S$ and $y \in S$.*

Equivalently, it is a submonoid of the multiplicative monoid $(R, \times)$. For instance, the set $\{1, f, f^2, \dots\}$ for a fixed $f \in R$ is a multiplicative set.

Definition 2.1.2. *Let $S \subseteq R$. Consider the set $R \times S$ and define a relation $\sim$ on it, where $(a,s) \sim (b,t)$ if and only if there exists a $u \in S$ such that $u(ta - sb) = 0$. One can check this is an equivalence relation.*

*Define the **localisation** of R at S, denoted R_S or RS^{-1} to be $(R \times S)/\sim$. Given $a \in R$ and $s \in S$, write a/s for the image of (a,s) in RS^{-1}.*

Define

$$+ : RS^{-1} \times RS^{-1} \to RS^{-1}, (a/s, b/t) \mapsto (at + bs)/(st)$$

and

$$\cdot : RS^{-1} \times RS^{-1} \to RS^{-1}, (a/s, b/t) \mapsto (ab)/(st)$$

These are both well defined with any choice of representative.

The set RS^{-1} with the operations above give a structure of a ring with identity element $1/1$, 0-element $0/1$ and a natural map from R to RS^{-1} via $r \mapsto r/1$. By construction, for any $r \in S$, $r/1$ is invertible with $1/r$.

Note the fact that if R is a domain, the fraction field of R is the ring $R(R\backslash 0)^{-1}$.

Proposition 2.1.3. *If R is a domain, for any $S \subseteq R$, RS^{-1} is also a domain.*

Proof. Suppose $0 \notin S$ and $(a/s)(b/t) = 0$ where $a, b \in R$ and $s, t \in S$. Then, we have $u(ab) = 0$ for some $u \in S$. As R is a domain, $ab = 0$, giving $a = 0$ or $b = 0$. Specifically, $a/s = 0/1$ or $b/t = 0/1$.

If $0 \in S$, the equivalence relation equates all elements, making the localisation a zero-ring. This is a domain. □

Definition 2.1.4. *Let M be a R-module. Let $S \subseteq R$ be multiplicative. Define a relation $\sim$ on $M \times S$ by $(a,s) \sim (b,t)$ if and only if there exists a $u \in S$ such that $u(ta - sb) = 0$. We define **localised module** MS^{-1} or M_S to be $(M \times S)/\sim$ with*

$$+ : MS^{-1} \times MS^{-1} \to MS^{-1}, (a/s, b/t) \mapsto (ta + sb)/(st)$$

and

$$\cdot : RS^{-1} \times MS^{-1} \to MS^{-1}, (a/s, b/t) \mapsto (ab)/(st)$$

which give MS^{-1} the structure of a RS^{-1} module. The 0 element is $0/1$ and carries the structure of a natural map $R \to RS^{-1}$ and a natural map of R-modules $M \to MS^{-1}$ given by $m \mapsto m/1$

Lemma 2.1.5. *Let $\phi : R \to R'$ be a ring homomorphism and $S \subseteq R$ be a multiplicative set. Suppose $\phi(S)$ consists of units in R'. Then, there is a unique ring homomorphism ϕ_S such that $\phi_S(r/1) = \phi(r)$ for all $r \in R$*

$$\begin{tikzcd}
R \arrow[r, "\phi"] \arrow[d] & R' \\
RS^{-1} \arrow[ur, dashed, "\phi_S"'] &
\end{tikzcd}$$

Proof. Define the map $\phi_S : R_S \to R'$ by $\phi_S(a/s) = \phi(a)(\phi(s))^{-1}$ for all $a \in R$ and $s \in S$. We first show it is well defined. Suppose $(a, s) \sim (b, t)$. Then,

$$\phi_S(b/t) = \phi(b)(\phi(t))^{-1}$$

and noting that $u(ta - sb) = 0$ for some $u \in S$,

$$\phi(u)(\phi(t)\phi(a) - \phi(s)\phi(b)) = 0$$

As $\phi(u)$ is a unit, multiplying it away we have $\phi(t)\phi(a) - \phi(s)\phi(b) = 0$, or $\phi(t)\phi(a) = \phi(s)\phi(b)$. Consequently, $\phi_S(a/s) = \phi(a)(\phi(s)^{-1}) = \phi(b)(\phi(t)^{-1}) = \phi_S(b/t)$. Noting that ϕ_S is also a homomorphism, we also confirm $\phi_S(r/1) = \phi(r)$ for all $r \in R$.

For uniqueness, if $\phi'_S : R_S \to R'$ is another such map, for every $r \in R$ and $t \in S$,

$$\begin{aligned}\phi'_S(r/t) &= \phi'_S((r/1)(t/1)^{-1}) \\ &= \phi'_S(r/1)\phi'_S(t/1)^{-1} \\ &= \phi_S(r)\phi_S(t)^{-1} \\ &= \phi_S(r/t)\end{aligned}$$

□

Lemma 2.1.6. *Let R be a ring and $S \subseteq R$ be a multiplicative set. Let M be an R-module, and for all $s \in S$ suppose the map*

$$[s]_M : M \to M, m \mapsto sm$$

is an isomorphism. Then there is a unique structure of an R_S module on M such that $(r/1)m = rm$ for all $m \in M$ and $r \in R$.

Proof. Follows a similar structure to above. The left-multiplication operator being an isomorphism lets us define suitable inverses for elements of S. Specifically, we define $(r/s)m$ to be $[s]_M^{-1}(r/m)$ and extend from here. □

Lemma 2.1.7. *Let R be a ring and $f \in R$. Define $S = \{1, f, f^2, \dots\}$. Then R_S is finitely generated as an R-algebra.*

Proof. Consider the R-algebra $T = R[x]/(fx - 1)$. Note that T is generated as an R-algebra by $1 + (fx - 1)$ and $x + (fx - 1)$. Define $\phi : R[x] \to R_S$ by the homomorphism of R-algebras extneded from $\phi(x) = 1/f$. Then $\phi(fx - 1) = 0$ and thus ϕ induces a homomorphism of R-algebras $\psi : T \to R_S$ by $g + (fx - 1) \mapsto \phi(g)$.

As the image of f in T is invertible by construction, by 2.1.5 there is a unique homomorphism of R-algebras $\lambda : R_S \to T$ that extends from

$$R \to T, 1 \mapsto 1 + (fx - 1)$$

The map $\psi \circ \lambda : R_S \to R_S$ with elements of the form $r/1$ is the identity, thus the entire map is the identity by uniqueness. Specifically, λ is injective. λ is also surjective, as it maps to the generators of T. Consequently, T and R_S are isomorphisms.

$$\begin{tikzcd}
R[x] \arrow[r, "\phi"] \arrow[d, "q_{(fx-1)}"'] & R_S \arrow[dl, dashed, bend left, "\lambda"] \\
T = R[x]/(fx-1) \arrow[ur, dashed, "\psi"] &
\end{tikzcd}$$

□

Proposition 2.1.8. *If R is a ring and $\phi : N \to M$ is a homomorphism of R-modules, there is a unique homomorphism of R_S modules $\phi_S : N_S \to M_S$ such that $\phi_S(n/1) = \phi(n)/1$ for all $n \in N$. If $\psi : M \to T$ is another homomorphism of R-modules, then $(\psi \circ \phi)_S = \psi_S \circ \phi_S$.*

Proof. The second part is straightforward. For the first, note that the map is given by $\phi_S(n/m) = \phi(n)/m$, and uniqueness follows. □

Proposition 2.1.9. *Let R be a ring and $S \subseteq R$ be a multiplicative set. Let I be an ideal in R. Then,*

$$R_S/I_S \simeq (R/I)_S$$

Given an R-module M and a submodule $N \subseteq M$,

$$M_S/N_S \simeq (M/N)_S$$

Proof. Consider the map $\phi : R_S \to (R/I)_S$ by $(r/s) \mapsto (q(r)/s)$ where q is the quotient map. This is a well defined and surjective map with kernel I_S. The proof follows by the first isomorphism theorem. The case for modules is similar. □

Definition 2.1.10. *Let*

$$\cdots \to M_i \overset{d_i}{\to} M_{i-1} \overset{d_{i-1}}{\to} \cdots$$

*be a sequence of R-modules with homomorphisms mapping between them such that $d_{i-1} \circ d_i = 0$ for all $i \in \mathbb{Z}$. We call such a sequence a **chain complex** of R-modules. We say that the complex is **exact** if $\operatorname{Ker}(d_{i-1}) = \operatorname{Im}(d_i)$ for all $i \in \mathbb{Z}$.*

Lemma 2.1.11. *Let R be a ring and $S \subseteq R$ be a multiplicative set. Let*

$$\cdots \to M_i \overset{d_i}{\to} M_{i-1} \overset{d_{i-1}}{\to} \cdots$$

be an chain complex of R-modules. If this is exact, the chain

$$\cdots \to (M_i)_S \overset{(d_i)_S}{\to} (M_{i-1})_S \overset{(d_{i-1})_S}{\to} \cdots$$

is also exact. If the second chain is exact for every maximal ideal $\mathfrak{m}$ of R, the first chain is exact.

Proof. We show the first statement first. Let $m/s \in (M_i)_S$. Suppose that $(d_i)_S(m/s) = 0$. Then, $(d_i)_S(m/1) = d_i(m)/1 = 0$. Thus $u \cdot d_i(m) = 0$. Then $um \in \operatorname{Im}(d_{i+1})$ as the first sequence is exact. Thus, there exists a $p \in M_{i+1}$ such that $d_{i+1}(p) = um$, thus $(d_{i+1})_S(p/us) = m/s$.

For the latter, we show the contrapositive. Suppose the first chain complex is not exact. Then, there exists a $i \in \mathbb{Z}$ such that

$$\operatorname{Ker}(d_i)/\operatorname{Im}(d_{i+1}) \neq 0$$

Take a non-zero element a from this set. Let $\mathfrak{m}$ be a maximal ideal containing $\operatorname{Ann}(a)$, which exists as $1 \notin \operatorname{Ann}(a)$ (a is non-zero). Then, $\operatorname{Ker}(d_i)/\operatorname{Im}(d_{i+1}) \neq 0$ as else there is a $u \in R \backslash \mathfrak{m} \subseteq R \backslash \operatorname{Ann}(a)$ with $u \cdot a = 0$ which is a contradiction. By the first isomorphism theorem, there is a natural isomorphism

$$\operatorname{Ker}(d_i)_{\mathfrak{m}}/\operatorname{Im}(d_{i+1})_{\mathfrak{m}} \simeq (\operatorname{Ker}(d_i)/\operatorname{Im}(d_{i+1}))_{\mathfrak{m}} \not\simeq 0$$

□

Lemma 2.1.12. *Let $\phi : R \to T$ be a ring homomorphism. Let $S \subseteq R$ be a multiplicative set. By Lemma 2.1.5 there is a unique homomorphism of rings $\phi' : R_S \to T_{\phi(S)}$ with $\phi'(r/1) = \phi(r)/1$. Viewning $T_{\phi(S)}$ as an R_S module and T as an R-module, there is a unique isomorphism of R_S modules $\mu : T_S \simeq T_{\phi(S)}$ such that $\mu(a/1) = a/1$ for all $a \in T$ and $\mu \circ \phi_S = \phi'$.*

$$\begin{tikzcd}
R \arrow[r] \arrow[d, "\phi"'] & R_S \arrow[d, dashed, "\phi'"] \arrow[dr, "\phi_S"] & \\
T \arrow[r] & T_{\phi(S)} & T_S \arrow[l, dashed, "\mu"]
\end{tikzcd}$$

Proof. Define $\mu(a/s) = a/\phi(s)$ for every $a \in T$ and $s \in S$. Given $a/s = b/t$, there is a $u \in S$ such that

$$u \cdot (t \cdot a - s \cdot b) = 0$$

The action by R onto T is defined by ϕ, so equivalently,

$$\phi(u)(\phi(t)a - \phi(s)b) = 0$$

meaning $a/\phi(s) = b/\phi(t)$ as $\phi(u)$ is a unit, and thus μ is well-defined. By construction, μ is a map of R_S modules and is also surjective. To see μ is injective, if $\mu(a/s) = 0/1$ for some $a \in T$ and $s \in S$, there is a $u \in S$ such that $\phi(u)a = 0$. Thus, $u \cdot a = 0$ in T, giving $a/1 = 0$ in T_S, implying $a/s = 0$. Thus μ is bijective.

The identity $\mu \circ \phi_S = \phi'$ follows by noting that composition of homomorphisms are homomorphisms and $\mu \circ \phi_S(1/1) = \phi'(1/1)$. □

Remark 2.1.13. Taking the identity map from R to R, we see that localisation of a ring R as viewed as a ring or a module over itself, we get the same R_S-module.

Proposition 2.1.14. *Let R be a ring and $\mathfrak{p}$ be a prime ideal in R. Then $R \backslash \mathfrak{p}$ is a multiplicative set.*

Proof. $1 \notin \mathfrak{p}$ as $\mathfrak{p}$ is prime, and if $x, y \notin \mathfrak{p}$ then $xy \notin \mathfrak{p}$ as it is prime. □

Notation 2.1.15. Write $R_{\mathfrak{p}}$ to denote $R_{R\backslash\mathfrak{p}}$ and if M is an $R-$module, write $M_{\mathfrak{p}}$ to mean $M_{R\backslash\mathfrak{p}}$. Note that the notation in unambiguous as prime ideals never contain 1.

Simiarly, if $\phi : M \to N$ is a homomorphism of R-modules, write $\phi_{\mathfrak{p}}$ for $\phi_{R\backslash\mathfrak{p}} : M_{\mathfrak{p}} \to N_{\mathfrak{p}}$

Proposition 2.1.16. *If $\phi : U \to R$ is a homomorphism of rings and $\mathfrak{p}$ is a prime ideal of R, then ϕ naturally induced a homomorphism of rings $U_{\phi^{-1}(\mathfrak{p})} \to R_{\mathfrak{p}}$*

Proof. Noting that $\phi(U \backslash \phi^{-1}(\mathfrak{p})) \subseteq R \backslash \mathfrak{p}$, we can give a map $(a/s) \mapsto (\phi(a)/\phi(s))$. □

Notation 2.1.17. The above map is often written as $\phi_{\mathfrak{p}}$.

Lemma 2.1.18. *Let R be a ring and $S \subseteq R$ be a multiplicative set. Let $\lambda : R \to R_S$ be the natural ring homomorphism. Then, there is a bijective correspondence with the prime ideals of R_S and $\mathfrak{p}$ of R such that $\mathfrak{p} \cap S = \emptyset$.*

The corresponding prime ideal of R_S is $\iota_{\mathfrak{p},S}(\mathfrak{p}_S) \subseteq R_S$ where $\iota_{\mathfrak{p}} : \mathfrak{p} \to R$ is the inclusion map (which is a homomorphism of R-modules).

Furthermore, $\iota_{\mathfrak{p},S}(\mathfrak{p}_S)$ is the ideal generated by $\lambda(\mathfrak{p})$ in R_S

Proof. We first prove that given any ideal I, $\iota_{I,S}(I_S)$ is the ideal generated by $\lambda(I)$ in R_S. Note that by definition, $\iota_{I,S}(I_S)$ consists of all elements $a/s \in R_S$ for $a \in I$ and $s \in S$. Thus this is an ideal of R_S which contains $\lambda(I)$. As $a/s = (a/1)(1/s)$ every element is contained in the ideal generated by $\lambda(I)$.

We show next bijective correspondence. First, we claim that if J is a proper ideal of R_S, then $\lambda^{-1}(J) \cap S = \emptyset$. Otherwise, choose $s \in \lambda^{-1}(J)$ such that $s \in S$. Then, $\lambda(s) = s/1 \in J$, which is a unit, contradicting with J being a proper ideal. As preimages of prime ideals are prime, λ^{-1} maps prime ideals J of R_S into prime ideals of R such that $\lambda^{-1}(J) \cap S = \emptyset$. To show injectivity of λ^{-1} when restricted to prime ideals, we claim that if J is an ideal of R_S, the ideal generated by $\lambda(\lambda^{-1}(J))$ in R_S is J. Inclusion is obvious. If $a/s \in J$, $a/1 \in J$, meaning $a \in \lambda^{-1}(J)$. As $a/s = (a/1)(1/s)$ is in the ideal generated by $\lambda(\lambda^{-1}(J))$.

For the other direction, we first show that if $\mathfrak{p}$ is a prime ideal of R such that $\mathfrak{p} \cap S = \emptyset$, $\iota_{\mathfrak{p},S}(\mathfrak{p}_S)$ is a prime ideal of R_S. For this, consider the exact sequence of R-modules

$$0 \to \mathfrak{p} \to R \overset{q}{\to} R/\mathfrak{p} \to 0$$

where q is the quotient map. By Lemma 2.1.11, the sequence of R_S modules

$$0 \to \mathfrak{p}_S \to R_S \overset{q_S}{\to} (R/\mathfrak{p})_S \to 0$$

is also exact. By Lemma 2.1.12, $(R/\mathfrak{p})_S$ is isomorphic as an R_S module to $(R/\mathfrak{p})_{q(S)}$. By the First isomorphism theorem, $(R/\mathfrak{p})_S \simeq (R_S)/(\mathfrak{p}_S)$, giving $(R_S)/(\mathfrak{p}_S) \simeq (R/\mathfrak{p})_{q(S)}$. By assumption, $R/\mathfrak{p}$ is a domain, and noting $0 \notin q(S)$ as $S \cap \mathfrak{p} = \emptyset$, $(R/\mathfrak{p})_{q(S)}$ is a domain. Consequently, $\mathfrak{p}_S$ is a prime ideal. Finally, to show that $\iota_{p,S}(\cdot_S)$ is injective when restricted to prime ideals $\mathfrak{p}$ with $\mathfrak{p} \cap S = \emptyset$, we show $\lambda^{-1}(\iota_{p,S}(\mathfrak{p}_S)) = \mathfrak{p}$ if $\mathfrak{p} \cap S = \emptyset$. Noting that $\iota_{\mathfrak{p},S}(\mathfrak{p}_S)$ is the ideal generated by $\lambda(\mathfrak{p})$ in R_S, we have $\lambda^{-1}(\iota_{\mathfrak{p},S}(\mathfrak{p}_S)) \supseteq \mathfrak{p}$. Taking $a \in \lambda^{-1}(\iota_{\mathfrak{p},S}(\mathfrak{p}_S))$, $a/1 = b/s$ for some $b \in \mathfrak{p}$ and $s \in S$. So, for some $u \in S$, $u(sa - b) = 0$, or $usa = ub$. As $ub \in \mathfrak{p}$ and $us \notin \mathfrak{p}$, it follows $a \in \mathfrak{p}$ from the fact $\mathfrak{p}$ is a prime ideal. □

Remark 2.1.19. As a consequence of Lemma 2.1.18, $\mathrm{Spec}(\lambda)(\mathrm{Spec}(R_S))$ consists of prime ideals in $\mathrm{Spec}(R)$ that do not meet S. Given that $S = \{1, f, f^2, \dots\}$, we have

$$\mathrm{Spec}(\lambda)(\mathrm{Spec}(R_S)) = D_f(R)$$

Corollary 2.1.20. *Given that $\mathfrak{p} \in \mathrm{Spec}(R_S)$ then λ induces a natural homomorphism of rings $R_{\lambda^{-1}(\mathfrak{p})} \to (R_S)_{\mathfrak{p}}$. This homomorphism is an isomorphism.*

Proof. Define the map ϕ with $\phi(r/s) = ((r/1)/(s/1))$. It is straightforward that this map is both injective and surjective. □

Corollary 2.1.21. *The nilradical of R is the intersection of every prime ideal.*

Proof. Following the same proof as before, if we have a nilpotent element, it is part of every prime ideal (by quotienting by the prime). Let R be a ring and $r \in R$ is an element that is not nilpotent. Let $S = \{1, r, r^2, \dots\}$. R_S is non-zero as $r/1 \neq 0/1$ by nilpotence. Let $\mathfrak{q}$ be a prime ideal of R_S. By Lemma 2.1.18, this ideal corresponds to a prime ideal $\mathfrak{p}$ of R such that $r \notin \mathfrak{p}$ (doesn't intersect with S). □

Corollary 2.1.22. *Let R be a ring and $\mathfrak{p} \subseteq R$ be a prime ideal. The ring $R_{\mathfrak{p}}$ is local. If $\mathfrak{m}$ is the maximal ideal of $R_{\mathfrak{p}}$ and $\lambda : R \to R_{\mathfrak{p}}$ is the natural homomorphism of rings, $\lambda^{-1}(\mathfrak{m}) = \mathfrak{p}$.*

Proof. By Lemma 2.1.18, prime ideals of $R_{\mathfrak{p}}$ correspond to prime ideals of R that don't meet $R\backslash\mathfrak{p}$. Noting that this correspondence is given by monotonic maps on inclusion, every prime ideal of $R_{\mathfrak{p}}$ is contained in the prime ideal corresponding to $\mathfrak{p}$. Let I be a maximal ideal of $R_{\mathfrak{p}}$. As I is contained in the prime ideal contained in the prime ideal corresponding to $\mathfrak{p}$, it must concide by maximality. Thus the prime ideal $\mathfrak{m}$ corresponding to $\mathfrak{p}$ is maximal and is the only maximal ideal. By the correspondence map, $\lambda^{-1}(\mathfrak{m}) = \mathfrak{p}$. □

3 Prime Ideals

3.1 Nilradical

Definition 3.1.1. *Let R be a ring. The* ***nilradical*** *of R is the set of nilpotent elements of R. We say that R is* ***reduced*** *if its nilradical is $\{0\}$.*

Proposition 3.1.2. *Let R be a ring. The nilradical of R is the intersection of all the prime ideals of R.*

Proof. Let $f \in R$ be a nilpotent element. Let $I \subseteq R$ be a prime ideal. Some power of f is zero, which is an element of I. Specifically, $f + I \in R/I$ is a zero-divisor. As I is prime, R/I is a domain, meaning $f + I = I$. Thus, $f \in I$, meaning f is in the intersection of all the prime ideals of R.

Conversely, suppose $f \in R$ is not nilpotent. Let S be the set of proper ideals I of R such that for all $n \geq 1$, $f^n \notin I$. Note that $(0) \in S$. Giving a partial order on S by inclusion, every total ordered subset in S has an upper bound by union. By Zorn's Lemma, S has a maximal element $\mathfrak{m}$.

We claim $\mathfrak{m}$ is a prime ideal. Then, as $\mathfrak{m} \in S$, $f^n \notin \mathfrak{m}$ for any $n \geq 1$. Specifically, as $f \notin \mathfrak{m}$, f does not lie in the intersection of the prime ideals of R.

To show that $\mathfrak{m}$ is prime, suppose we take $x, y \in R$ and $x, y \notin \mathfrak{m}$. It suffices to show that $xy \notin \mathfrak{m}$. Note first that both $(x) + \mathfrak{m}$ and $(y) + \mathfrak{m}$ are ideals which do not lie in S by maximality. Thus, there exists $n_x, n_y \geq 1$ such that $f^{n_x} \in (x) + \mathfrak{m}$ and $f^{n_y} \in (y) + \mathfrak{m}$ (Note the existence follows as if I is not proper, $I = R$ and $f \in R$). Thus, $f^{n_x} = a_1 x + m_1$ and $f^{n_y} = a_2 y + m_2$ for $a_1, a_2 \in R$ and $m_1, m_2 \in \mathfrak{m}$. Specifically,

$$f^{n_x + n_y} = a_1 a_2 xy + m_3$$

for some $m_3 \in \mathfrak{m}$, using that $\mathfrak{m}$ is an ideal. Thus, $xy \notin \mathfrak{m}$, as else $f^{n_x+n_y} \in \mathfrak{m}$. □

Corollary 3.1.3. *Let R be a ring. The nilradical of R is an ideal.*

Proof. Follows from the fact that the intersection of an arbitrarily set of ideals is an ideal. □

We can prove the above corollary without relying on the previous proposition, by simply showing that the set of nilpotent elements are closed under addition and multiplication by elements of R.

Example 3.1.4. The nilradical of $\mathbb{C}[x]/(x^n)$ for $n \geq 1$ is (x).

3.2 Radical

Definition 3.2.1. *Let $I \subseteq R$ be an ideal. Let $q : R \to R/I$ be the quotient map, and $\mathcal{N}$ be the nilradical of R/I. The* ***radical*** *$\mathfrak{r}(I)$ of I is $q^{-1}(\mathcal{N})$.*

The nilradical of R coincides with the radical $\mathfrak{r}((0))$. As notation, we sometimes write $\mathfrak{r}(R)$ for the nilradical of R. By Proposition 3.1.2, the radical of I has two equivalent definitions :

1. It is the set of elements $f \in R$ such that there exists an integer $n \geq 1$ such that $f^n \in I$.

2. It is the intesection of prime ideals of R which contain I.

Example 3.2.2. Consider $\mathbb{Z}/12\mathbb{Z}$. $\mathfrak{r}(R) = (6)$ is not a prime ideal, so radicals need not be prime.

Proposition 3.2.3. *Let I be an ideal in R. Then, $\mathfrak{r}(\mathfrak{r}(I)) = \mathfrak{r}(I)$.*

Proof. Note that $\mathfrak{r}(I) = \{f \in R \mid f^n \in I,\ n \geq 0\}$. So, $\mathfrak{r}(\mathfrak{r}(I)) = \{f \in R \mid f^{mn} \in I,\ n, m \geq 0\} = \mathfrak{r}(I)$. □

Proposition 3.2.4. *Let I, J be ideals in R. Then, $\mathfrak{r}(I \cap J) = \mathfrak{r}(I) \cap \mathfrak{r}(J)$.*

Proof. Follows from the first equivalent definition. □

Definition 3.2.5. *An ideal that coincides with it's own radical is called a **radical ideal**.*

A trivial radical ideal is the (0) when working with domains.

3.3 Jacobson Radical

Definition 3.3.1. *Let R be a ring. The **Jacobson radical** of R is the intersection of all the maximal ideals of R.*

Note that by definition, the Jacobson radical of R contains the nilradical of R. Also note that if a ring is local, then the Jacobson radical is the maximal ideal of R.

Definition 3.3.2. *Let $I \subseteq R$ be a non-trivial ideal. Let $q : R \to R/I$ be the quotient map and $\mathcal{J}$ be the Jacobson radical of R/I. The **Jacobson Radical of** I is $q^{-1}(\mathcal{J})$. Equivalently, it is the intersection of all the maximal ideals containing I (by taking a larger ideal and showing it is actually the entire set).*

Note that by definition, the Jacobson radical of I contains the radical of I.

Proposition 3.3.3 (Nakayama's Lemma)**.** *Let R be a ring. Let M be a finitely generated R-module. Let I be an ideal of R contained by the Jacobson radical of R. Suppose further that $IM = M$ (where product is the finite sum). Then $M \simeq 0$.*

Proof. Suppose $M \not\simeq 0$. Let $x_1, \dots, x_s$ be the set of generators of M such that s is minimal, where $s \geq 1$ as M is nonzero. By assumption, there exists $a_1, \dots, a_s \in I$ such that

$$x_s = a_1 x_1 + \cdots + a_s x_s$$

Rewriting,

$$(1 - a_s)x_s = a_1 x_1 + \cdots + a_{s-1} x_{s-1}$$

If $1 - a_s$ is not a unit, it would be contained in some maximal ideal $\mathfrak{m}$ by Proposition 1.1.17. As $a_s \in I$ which is inside the Jacobson radical which is inside any maximal ideal, we have $a_s \in \mathfrak{m}$, giving $1 \in \mathfrak{m}$, a contradiction. Thus, $1 - a_s$ is a unit. Rewriting,

$$x_s = (1 - a_s)^{-1} a_1 x_1 + \cdots + (1 - a_s)^{-1} a_{s-1} x_{s-1}$$

contradicting the minimality of s. Thus, $M \simeq 0$. □

Corollary 3.3.4. *let R be a local ring with maximal ideal $\mathfrak{m}$. Let M be a finitely generated R-module. Let $x_1, \dots, x_s \in M$ be elements of M and $x_1 + \mathfrak{m}M, \dots, x_s + \mathfrak{m}M \in M/\mathfrak{m}M$ generate the $R/\mathfrak{m}$-module $M/\mathfrak{m}M$. Then the elements $x_1, \dots, x_s$ generate M.*

Proof. Let $M' \subseteq M$ be the submodule generated by $x_1, \dots, x_s$. By assumption, $M' + \mathfrak{m}M = M$, thus, $\mathfrak{m}(M/M') = M/M'$. By Nakayama's lemma, we have $M/M' \simeq (0)$, giving $M = M'$. □

Corollary 3.3.5. *Let R be a local ring with maximal ideal $\mathfrak{m}$. Let M, N be finitely generated R-modules and $\phi : M \to N$ be a homomorphism of R-modules. Suppose the induced homomorphism*

$$M/\mathfrak{m}M \to N/\mathfrak{m}N$$

is surjective. Then ϕ is surjective.

Proof. Let $x_1, \dots, x_s$ be generators of M. By assumption, $\phi(x_1) + \mathfrak{m}, \dots, \phi(x_s) + \mathfrak{m}$ generate $N/\mathfrak{m}$. Thus, by Corollary 3.3.4, $\phi(x_1), \dots, \phi(x_s)$ generate N. In particular, ϕ is surjective. □

Definition 3.3.6. *A ring R is called a* ***Jacobson ring*** *if for all the proper ideals I of R, the Jacobson radical of I coincides with the radical of I.*

Proposition 3.3.7. *A ring R is a Jacobson ring if and only if every prime ideal I is the intersection of maximal ideals containing I.*

Proof. If R is Jacobson, every Jacobson radical of I coincides with the radical of I. Thus, for any prime I, the intersection of maximal ideals containing I is equal to the intersection of prime ideals containing I, which is just I.

Conversely, let every prime ideal be the intersection of maximal ideals containg itself. Then, for any ideal I, the radical of I is the intersection of maximal ideals containing a prime ideal which contains I. As any maximal ideal is prime, this is just the intersection of maximal ideals containing I, which is the Jacobson radical of I. □

Proposition 3.3.8. *Any quotient of a Jacobson ring is also Jacobson.*

Proof. Let R be a Jacobson ring. Let R/I be the quotient ring with some ideal I. It suffices to show every prime ideal of R/I is the intersection of maximal ideals containing it. For any prime ideal J containing I, as R is a Jacobson ring,

$$J = \bigcap_{J \subseteq \mathfrak{m}} \mathfrak{m}$$

for maximal ideals $\mathfrak{m}$. By correspondence, takig quotients,

$$J/I = \bigcap_{J \subseteq \mathfrak{m}} \mathfrak{m}/I$$

writes any prime ideal of R/I as the intersection of maximal ideals containing it. □

Example 3.3.9. The following are examples of Jacobson rings.

1. The ring $\mathbb{Z}$
2. Any field
3. Given a field K, the polynomial ring $K[x]$
4. Any finitely generated algebra over a Jacobson ring

Contrary to this, a local domain is never Jacobson unless it is a field. This follows as (0) is prime, which equals the intersection of maximal ideals, which is just $\mathfrak{m}$. As this is (0), it is a field. As a corollary, the ring of p-adic integers $\mathbb{Z}_p$ for prime p is not Jacobson.

3.4 Spectrum

Definition 3.4.1. *Let R be a ring. The* ***spectrum*** *of R written* $\operatorname{Spec}(R)$ *is the set of prime ideals of R.*

Furthermore, given an ideal I of R, define

$$V(I) = \{\mathfrak{p} \in \operatorname{Spec}(R) \mid I \subseteq \mathfrak{p}\}$$

which is the set of prime ideals containing I.

Proposition 3.4.2. *The function $V(\cdot)$ has the following properties*

1. $V(I) \cup V(J) = V(I \cdot J)$
2. $\cap_{I \in \mathcal{I}} V(I) = V(\sum_{I \in \mathcal{I}} I)$
3. $V(R) = \emptyset$
4. $V((0)) = \operatorname{Spec}(R)$

Proof. (1) Double inclusion. One direction is clear, as $IJ \subseteq I$ and $IJ \subseteq J$. If $K \in V(IJ)$, $IJ \subseteq K$ where K is prime. Suppose for a contradiction $I \not\subseteq K$ and $J \not\subseteq K$. Take elements $i \in I \backslash K$ and $j \in J \backslash K$. As $ij \in K$, $i \in K$ or $j \in K$, which contradicts choice.

(2) Double inclusion. One direction is clear, as $J \subseteq \sum_{I \in \mathcal{I}} I$ for any $J \in \mathcal{I}$. For the other direction, suppose we have a prime K such that $I \subseteq K$ for every $I \in \mathcal{I}$. Then we note $\sum_{I \in \mathcal{I}} I \subseteq K$, as for any element in the sum decomposed to elements from I, they are in K, whose sum is also in K.

(3), (4) are immediate. □

Definition 3.4.3. *The topology induced by setting $V(I)$ to be closed sets form a topology called the* ***Zariski Topology****. In this topology, the closed points (in* $\operatorname{Spec}(R)$*) are exactly the maximal ideals of R.*

If R is a Jacobson ring, any nonempty closed set contains a maximal ideal of R. As every prime ideal is also the limit (intersection) of maximal ideals, it follows that the set of closed points is a dense subset of $\operatorname{Spec}(R)$. (MOVE LATER!!!!)

Suppose we have a homomorphism $\phi : R \to T$. This induces a homomorphism

$$\operatorname{Spec}(\phi) : \operatorname{Spec}(T) \to \operatorname{Spec}(R)$$

by the map $\mathfrak{p} \mapsto \phi^{-1}(\mathfrak{p})$. Note this is well-defined as preimages of prime ideals are prime.

If I is an ideal in R and $J = (\phi(I))$ is an ideal in T, we have $\operatorname{Spec}(\phi)^{-1}(V(I)) = V(J)$. Consequently, $\operatorname{Spec}(\phi)$ is a continuous map for the Zariski topologies on source and target. Note also that by definition, $\operatorname{Spec}(\phi) \circ \operatorname{Spec}(\psi) = \operatorname{Spec}(\psi \circ \phi)$.

Lemma 3.4.4. *Let $\phi : R \to T$ be a surjective homomorphism of rings. Then* $\operatorname{Spec}(\phi)$ *is injective and* $\operatorname{Im}(\operatorname{Spec}(\phi)) = V(\operatorname{Ker}(\phi))$.

Proof. To show that $\operatorname{Spec}(\phi)$ is injective, note that for any $\mathfrak{p} \in \operatorname{Spec}(T), \mathfrak{p} = \phi(\phi^{-1}(\mathfrak{p}))$ by surjectivity. In particular, distinct elements of $\operatorname{Spec}(T)$ get sent to distinct elements in $\operatorname{Spec}(R)$.

We show the second by double inclusion. Note first that the image of $\operatorname{Spec}(\phi)$ is contained in $V(\operatorname{Ker}(\phi))$ as the preimage of a prime ideal by ϕ always contains the kernel (equivalently, any prime ideal contains 0).

On the other hand, fixing a $\mathfrak{p}$ to be a prime ideal containing $\mathrm{Ker}(\phi)$, it suffices to show $\mathrm{Spec}(\phi)(\phi(\mathfrak{p})) = \mathfrak{p}$. To do this, we show that $\phi(\mathfrak{p})$ is prime, and $\phi^{-1}(\phi(\mathfrak{p})) = \mathfrak{p}$. First, we clearly have $\mathfrak{p} \subseteq \phi^{-1}(\phi(\mathfrak{p}))$. Taking any $r \in \phi^{-1}(\phi(\mathfrak{p}))$, there exists $r' \in \mathfrak{p}$ such that $\phi(r) = \phi(r')$. As $\mathfrak{p}$ contains the kernel of ϕ, it follows $r \in \mathfrak{p}$, thus equality. To show that $\phi(\mathfrak{p})$ is a prime ideal, taking $x, y \in T$ such that $xy \in \phi(\mathfrak{p})$, choosing x', y' such that $\phi(x') = x$ and $\phi(y') = y$, $x'y' \in \phi^{-1}(\phi(\mathfrak{p})) = \mathfrak{p}$. Thus $x' \in \mathfrak{p}$ or $y' \in \mathfrak{p}$. The proof follows.

□

Proposition 3.4.5. *Fix $f \in R$. Define*

$$D_f(R) = \{\mathfrak{p} \in \mathrm{Spec}(R) \mid f \notin \mathfrak{p}\}$$

These form open sets in $\mathrm{Spec}(R)$ *and is a basis for the Zariski Topology.*

Proof. First note that

$$\mathrm{Spec}(R)\backslash D_f(R) = V((f))$$

Noting every closed set in $\mathrm{Spec}(R)$ can be expressed as $V(I)$ for some I,

$$\bigcup_{f \in I} D_f(R) = \{p \in \mathrm{Spec}(R) \mid I \not\subseteq \mathfrak{p}\} = \mathrm{Spec}(R)\backslash V(I)$$

So is a basis. □

Lemma 3.4.6. *Given a ring R,* $\mathrm{Spec}(R)$ *is compact.*

Proof. We use the notion that $\mathrm{Spec}(R)$ is compact if every open cover by basis elements has a finite subcover. Note that for any $S \subseteq R$,

$$\begin{aligned} \mathrm{Spec}(R)\backslash \bigcup_{f \in S} D_f &= \bigcap_{f \in S} (\mathrm{Spec}(R)\backslash D_f) \\ &= \bigcap_{f \in S} V((f)) \\ &= V(\sum_{f \in S} (f)) \end{aligned}$$

For any cover $\mathcal{F}$, taking $S = \mathcal{F}$, $V(\sum_{f \in \mathcal{F}}((f))) = \emptyset$. Thus, $\sum_{f \in \mathcal{F}}((f))$ is not contained in any prime ideal. By Proposition 1.1.17, every proper ideal has a maximal ideal (which is prime) containing it, meaning $\sum_{f \in \mathcal{F}}((f)) = R$. Then, we can write 1_R as a finite linear sum of elements of $\mathcal{F}$. These elements form a fintie subset $\mathcal{F}_0$ that generate R, and $\mathrm{Spec}(R)\backslash \bigcup_{f \in \mathcal{F}_0} D_f = V(R) = \emptyset$ □

Lemma 3.4.7. *Let I and J be ideals in R. Then, $V(I) = V(J)$ if and only if $\mathfrak{r}(I) = \mathfrak{r}(J)$.*

Proof. (⇒) Suppose that for every prime ideal $\mathfrak{p}$, $I \subseteq \mathfrak{p}$ if and only if $J \subseteq \mathfrak{p}$. Then, as radicals are intersections of prime ideals containing it, equality follows.

(⇐) Suppose for a contradiction that $V(I) \neq V(J)$. Without loss of generality, there exists $\mathfrak{p}$ such that $I \subseteq \mathfrak{p}$ and $J \not\subseteq \mathfrak{p}$. Then, $J \not\subseteq \mathfrak{r}(J)$, which contradicts definition. □

Consequently, there is a bijective correspondence between radical ideals in R and closed subsets of $\mathrm{Spec}(R)$. The closed subsets corresponding to prime ideals are called **irreducible**.

Proposition 3.4.8. *If I and J are radical ideals, $I \subseteq J$ if and only if $V(J) \subseteq V(I)$*

Proof. ($\Rightarrow$) is immediate. For ($\Leftarrow$), we have $J \subseteq \mathfrak{p}$ implies $I \subseteq \mathfrak{p}$. As I and J are radical ideals, they are intersections of prime ideals containing it. The proof follows. □

Corollary 3.4.9. *The quotient map from R into $R/\mathfrak{r}((0))$ is a homeomorphism. Thus, closed sets are determied by radical ideals and are unchanged by quotients with the nilradical.*

Remark 3.4.10. Given two ideals I, J of a ring R, we have

$$(I \cap J) \cdot (I \cap J) \subseteq I \cdot J \subseteq I \cap J$$

Thus $\mathfrak{r}(I \cdot J) = \mathfrak{r}(I \cap J)$ which follows from the fact $V(I \cdot J) = V(I \cap J)$, supported by the identity $V(I) \cup V(J) = V(I \cdot J)$.

Also, given that I and J are radical ideals, $I \cap J$ is a radical ideal, whereas $I \cdot J$ need not be.

Lemma 3.4.11. *Let R be a ring and $I \lhd R$. Then $V(I)$ has a minimal element up to inclusion. Moreover, if $\mathfrak{p} \supseteq I$ is prime, $\mathfrak{p}$ contains such an ideal.*

Proof. Define $\leq$ on prime ideals containing I but is contained by $\mathfrak{p}$ by $\supseteq$. Take any chain T. Then we claim $\mathcal{T}$ has a maximal element $\bigcap_{\mathfrak{p} \in \mathcal{T}} \mathfrak{p}$. Note first this clearly contains I, is maximal, and is an ideal. To show it is prime, suppose $xy \in \bigcap_{\mathfrak{p} \in \mathcal{T}} \mathfrak{p}$ but $x, y \notin \bigcap_{\mathfrak{p} \in \mathcal{T}} \mathfrak{p}$. Then we can find $\mathfrak{p}_i, \mathfrak{p}_j$ such that $x \notin \mathfrak{p}_i$ and $y \notin \mathfrak{p}_j$. Without loss of generality, as $\mathcal{T}$ is a chain, suppose $\mathfrak{p}_i \leq \mathfrak{p}_j$. Then as $xy \in \mathfrak{p}_j$, $x \in \mathfrak{p}_j$. This contradicts the $\leq$ condition. Thus by Zorn's Lemma, there is a maximal element $\mathfrak{m}$ up to the relation $\leq$. This corresponds to a minimal prime containing I that is contained in $\mathfrak{p}$. □

3.5 Primary Decomposition

Proposition 3.5.1. *Let $\mathfrak{p}_1, \ldots \mathfrak{p}_k$ be prime ideals of R. Let I be an ideal of R. If $I \subseteq \bigcup_{i=1}^k \mathfrak{p}_i$, then there is some $i_0 \in \{1, \ldots, k\}$ such that $I \subseteq \mathfrak{p}_{i_0}$.*

Proof. By induction on k. The case for $k = 1$ holds tautologically. For a general k, if $I \subseteq \bigcup_{i \neq j}^k \mathfrak{p}_i$, we are done by the inductive hypothesis. Otherwise, we can find $x_1, \ldots, x_k \in I$ such that for all $i \in \{1, \ldots, k\}$, $x_i \in \mathfrak{p}_i$ but $x_i \notin \mathfrak{p}_j$ for any $i \neq j$. Consider

$$y = \sum_{j=0}^{k} x_1 x_2 \cdots x_{j-1} x_{j+1} \cdots x_k$$

where $x_0 = x_{k+1} = 1$. Note that by construction $x_1 x_2 \cdots x_{j-1} x_{j+1} \cdots x_k \in \mathfrak{p}_i$ if $i \neq j$. As $y \in I$, $y \in \mathfrak{p}_i$ for some $i \in \{1, \ldots, k\}$. Then,

$$y - \sum_{j \neq i}^{k} x_1 x_2 \cdots x_{j-1} x_{j+1} \cdots x_k \in \mathfrak{p}_i$$

So $x_1 x_2 \cdots x_{i-1} x_{i+1} \cdots x_k \in \mathfrak{p}_i$, which contradicts construction as $\mathfrak{p}_i$ is a prime ideal. □

Proposition 3.5.2. *Let $I_1, \ldots, I_k$ be ideals of R and $\mathfrak{p}$ be a prime ideal of R. Suppose that $\mathfrak{p} \supseteq \bigcap_{i=1}^k I_i$. Then, there exists a $i_0 \in \{1, \ldots, k\}$ such that $p \supseteq I_{i_0}$. If $\mathfrak{p} = \bigcap_{i=1}^k I_i$, there is a i_0 such that $p = I_{i_0}$.*

Proof. For the first case, suppose for a contradiction that for every $i \in \{1, \ldots, k\}$ there is an element $x_i \in I_i$ such that $x_i \notin \mathfrak{p}$. But $x_1 x_2 \cdots x_k \in \bigcap_{i=1}^k I_i \subseteq \mathfrak{p}$ and as $\mathfrak{p}$ is prime, one of x_i lies in $\mathfrak{p}$, a contradiction. The second case follows immediately as a consequence, noting $\bigcap_{i=1}^k I_i \subseteq I_{i_0}$. □

Remark 3.5.3. Noting the proof in Proposition 3.5.1, any cover of an ideal by two ideals is covered by a single ideal.

Definition 3.5.4. *An ideal I of R is called **primary** if it is proper and all the zero-divisors of R/I are nilpotent.*

In other words, if $xy \in I$ and $x, y \notin I$, there exists $l, n > 1$ such that $x^l \in I$ and $y^n \in I$. Consequently, every prime ideal is primary. The converse need not be true. Ideals $(p^n) \in \mathbb{Z}$ are primary if p is prime and $n > 0$ but for $n > 1$ is not a prime ideal.

Lemma 3.5.5. *Suppose that I is a primary ideal of R. Then $\mathfrak{r}(I)$ is a prime ideal.*

Proof. Let $x, y \in R$ and suppose $xy \in \mathfrak{r}(I)$. Then, there is a $n > 0$ with $x^n y^n \in I$. By primarity, $x^n \in I$, or $y^n \in I$, or $x^{ln} \in I$ and $y^{nk} \in I$ for some $l, k > 1$. In any case, $x \in I$ or $y \in I$. □

Definition 3.5.6. *Following the previous lemma, given a prime ideal $\mathfrak{p}$ and ideal I, we say that I is $\mathfrak{p}$-**primary** if $\mathfrak{r}(I) = \mathfrak{p}$.*

$\mathfrak{p}$-primary ideals I have the property that if $ab \in I$, without loss of generality, if $a \notin I$, then $b \in \mathfrak{p}$.

Example 3.5.7. Consider $\mathbb{Z}[x, y]$ and the ideal (xy). Now, $\mathfrak{r}((xy)) = (x, y)$ who is clearly prime. However (xy) is not primary. Specifically, the radical of an ideal being prime does not imply the original ideal is primary.

However, we have the following.

Lemma 3.5.8. *Let J be a (proper) ideal of R. Suppose that $\mathfrak{r}(J)$ is a maximal ideal. Then J is primary.*

Proof. By assumption, the nilradical of R/J is a maximal ideal (by correspondence). Thus, R/J is local, as any maximal ideal of R/J contains $\mathfrak{r}(R/J)$. Hence every element of R/J is either a unit or is nilpotent. Specifically, J is primary. □

Definition 3.5.9. *If $I, J \subseteq R$ are ideals in R, we write*

$$(I : J) = \{r \in R \mid rJ \subseteq I\}$$

Note that $(I : J)$ is also an ideal and $((0) : J) = \mathrm{Ann}(J)$. When it is clear, we write x to mean (x) for some $x \in R$ (e.g. $(x : I)$ to mean $((x) : I)$).

Note the identity $I \subseteq (I : J)$.

Proposition 3.5.10. *Given ideals I, J, M of R, we have*

$$(I : M) \cap (J : M) = (I \cap J : M)$$

Proof. By double inclusion. □

Lemma 3.5.11. *Let $\mathfrak{p}$ be a prime ideal and I be a $\mathfrak{p}$-primary ideal. Fix any $x \in R$. Then,*

1. *If $x \in I$, $(I : x) = R$*
2. *If $x \notin I$, $\mathfrak{r}(I : x) = \mathfrak{p}$*

3. If $x \notin \mathfrak{p}$, $(I : x) = I$

Proof. The first and third cases follow immediately. For the second case, suppose $y \in \mathfrak{r}(I : x)$. By definition, there exists some $n > 0$ such that $xy^n \in I$. As $x \notin I$, $y^n \in \mathfrak{p} = \mathfrak{r}(I)$, so $y^{ln} \in I$ for some $l > 0$. Thus, $y \in \mathfrak{r}(I)$. Thus $\mathfrak{r}(I : x) \subseteq \mathfrak{p}$. Now clearly $I \subseteq \mathfrak{r}(I : x) \subseteq \mathfrak{p}$. As $\mathfrak{r}$ is monotonic, $\mathfrak{r}(I) = \mathfrak{p} \subseteq \mathfrak{r}(\mathfrak{r}(I : x)) = \mathfrak{r}(I : x) \subseteq \mathfrak{r}(\mathfrak{p}) = \mathfrak{p}$, giving $\mathfrak{r}(I : x) = \mathfrak{p}$. □

Lemma 3.5.12. *Let $\mathfrak{p}$ be a prime ideal and $J_1, \dots, J_k$ be $\mathfrak{p}$-primary ideals. Then $J = \bigcap_{i=1}^k J_i$ is also $\mathfrak{p}$-primary.*

Proof. Applying $\mathfrak{r}$,

$$\mathfrak{r}(J) = \mathfrak{r}(\bigcap_{i=1}^{k} J_i) = \bigcap_{i=1}^{k} \mathfrak{r}(J_i) = \mathfrak{p}$$

Thus, it remains to check that J is primary. Suppose $xy \in J$ with $x, y \notin J$. Then we can find $i, j \in \{1, \dots, k\}$ such that $x \notin J_i$ and $y \notin J_j$. Hence there exists $l, t > 0$ such that $y^l \in J_i$ and $x^t \in J_j$ (as $xy \in J_i$ and $xy \in J_j$). Thus, $x \in \mathfrak{r}(J_j) = \mathfrak{r}(J) = \mathfrak{r}(J_i) \ni y$, yielding that J is primary. □

Definition 3.5.13. *An ideal $I \triangleleft R$ is **decomposable** if there exists a finite collection $J_1, \dots, J_k$ of primary ideals in R such that $I = \bigcap_{i=1}^k J_i$. The sequence is called a **primary decomposition** of I. A primary decomposition is called **minimal** if*

1. *The radicals $\mathfrak{r}(J_i)$ are distinct*

2. *For all $i \in \{1, \dots, k\}$, $J_i \not\supseteq \bigcap_{j \neq i} J_i$*

Note that any primary decomposition can be reduced to a minimal primarity decomposition by

1. Using Lemma 3.5.12 and replacing all primary ideals with the same radical with their intersection to achieve (1)

2. Remove any primary ideal that covers the entire set

Theorem 3.5.14. *Let I be a decomposable ideal. Let $J_1, \dots, J_k$ be primary ideals and $I = \cap_{i=1}^k J_i$ be a minimal primary decomposition of I. Define $\mathfrak{p}_i = \mathfrak{r}(J_i)$ (such that $\mathfrak{p}_i$ are prime). Then,*

$$\{p_i \mid i \in \{1, \dots, k\}\} = \{prime\ \mathfrak{r}(I : x) \mid x \in R\}$$

Proof. Take $x \in R$. Note that $(I : x) = \bigcap_{i=1}^k (J_i : x)$ and $\mathfrak{r}(I : x) = \bigcap_{i=1}^k \mathfrak{r}(J_i : x)$ by preservation of $\mathfrak{r}$ under intersection. Thus, by Lemma 3.5.11, $\mathfrak{r}(I : x) = \bigcap_{i, x \notin J_i} \mathfrak{p}_i$. If $\mathfrak{r}(I : x)$ is prime, by Proposition 3.5.2, $\mathfrak{r}(I : x) = \mathfrak{p}_{i_0}$ for some $i_0 \in \{1, \dots, k\}$.

Conversely, taking any $i_0 \in \{1, \dots, k\}$, we can find a $x \in J_{i_0}$ such that $x \notin J_i$ for $i \neq i_0$ by minimality of decomposition. Given such x, $\mathfrak{r}(I : x) = \bigcap_{i, x \notin J_i} \mathfrak{p}_i = \mathfrak{p}_{i_0}$ by above. □

Remark 3.5.15. By Theorem 3.5.14, we can associate any decomposable ideal I in R with a unique set of prime ideals. Specifically, this set is fixed for any primary decomposition. We then say that these prime ideals are **associated** with I. Also note that the intersection of these primes give $\mathfrak{r}(I)$ (by choosing x to be a unit and taking $(I : x) = I = \bigcap_i \mathfrak{p}_i$).

Given an ideal that is decomposable into radical ideals, it has a minimal primary decomposition by prime ideals, and these prime ideals are the associated primes. Noting Proposition 3.5.2, any two minimality primary decomposition by prime ideals of a radical ideal coincide.

While out of scope, any minimal primary decomposition of a radical consists only of prime ideals. Specifically, a decomposable radical ideal has a unique primary decomposition by prime ideals.

Example 3.5.16. If $n = \pm p_1^{n_1} \cdots p_k^{n_k} \in \mathbb{Z}$ where p_i are distinct prime numbers and $n_i > 0$, a parimary decomposition of (n) is given by $(n) = \bigcap_{i=1}^k (p^{n_i})$ by the Chinese Remainder Theorem. The set of prime ideals associated with this is given by $\{p_1, \ldots, p_k\}$.

Example 3.5.17. Consider the ideal $(x^2, xy) \subseteq \mathbb{C}[x, y]$. Now,

$$(x^2, xy) = (x) \cap (x, y)^2$$

so the associated set of prime ideals is $\{(x), (x, y)\}$. To see equality, note that elements of $(x, y)^2$ are pf tje form $x^2 P(x, y) + xyQ(x, y) + y^2 T(x, y)$, thus the right side consists of polynomials of such form where $T(x, y)$ is divisible by x. Double inclusion follows. To see that these are both primary, we note $\mathbb{C}[x, y]/(x) \simeq \mathbb{C}[y]$ meaning (x) is prime (thus primary), and from $\mathbb{C}[x, y]/(x, y) \simeq \mathbb{C}$, using Lemma 3.5.8, $(x, y)^2$ is also primary.

Lemma 3.5.18. *Let I be a decomposable ideal. Let $\mathcal{S}$ be the set of prime ideals associated with some minimal primary decomposition of I. View $\mathcal{S}$ as a poset by inclusion. Then, the minimal elements of $\mathcal{S}$ coincide with the minimal elements of $V(I)$.*

Proof. The minimal elements of $V(I)$ denoted $V(I)_{\min}$ are minimal elements of $\mathcal{S}$ denoted $\mathcal{S}_{\min}$ by definition (by considering any primary decomposition, we can throw in any element of $\mathcal{I}_{\min}$ into the decomposition to make a decomposition containing this element).

To show the other direction, note that $\mathfrak{r}(I) = \bigcap_{\mathfrak{p} \in \mathcal{S}} \mathfrak{p}$, thus $\mathfrak{r}(I) = \bigcap_{\mathfrak{p} \in \mathcal{S}_{\min}} \mathfrak{p}$. Suppose that $\mathfrak{p}_0 \in \mathcal{S}_{\min}$ and that $\mathfrak{p}_0 \notin V(I)_{\min}$. Then, we can find a $\mathfrak{p}_0' \in V(I)$ such that $I \subseteq \mathfrak{p}_0' \subsetneq \mathfrak{p}_0$. By Proposition 3.5.2, we can find a $\mathfrak{p} \in \mathcal{S}_{\min}$ such that $\mathfrak{p} \subseteq \mathfrak{p}_0'$. This contradicts minimality of $\mathfrak{p}_0$, giving $\mathcal{S}_{\min} = V(I)_{\min}$. □

Definition 3.5.19. *Elements of $\mathcal{S}_{\min}$ are called **isolated** or **minimal** prime ideals associated with I. The elements $\mathcal{S} \backslash \mathcal{S}_{\min}$ are called **embedded** prime ideals.*

Remark 3.5.20. If I is a decomposable radical ideal, the associated primes of I are isolated. This follows immediately from the fact that I has a minimal primary decomposition by prime ideals.

If I is a decomposable ideal, then $V(I)_{\min}$ is a finite set. By the previous lemma, this is exactly the isolated ideals associated with I.

3.6 Noetherian Rings

Definition 3.6.1. *Let R be a ring. We say that R is **noetherian** if every ideal of R is finitely generated. That is, for any $I \lhd R$, $I = (r_1, \ldots, r_k)$ for some $r_i \in R$.*

Example 3.6.2. Fields and PIDs are noetherian, as every ideal is generated by a single element. For instance, $\mathbb{Z}$, $\mathbb{C}$ are noetherian. Given any field K, $K[x]$ is also noetherian as a polynomial over a field is an ED (which is a PID).

Lemma 3.6.3. *The ring R is noetherian if and only if for any chain $I_1 \subseteq I_2 \subseteq \cdots$ is a chain of ideals, there exists a $k \geq 1$ such that $I_k = I_{k+i} = \bigcup_{t=1}^\infty I_t$ for all $i \geq 0$.*

Proof. ($\Rightarrow$) Suppose R is noetherian. Let $I_1 \subseteq I_2 \subseteq \cdots$. The set $\bigcup_{t=1}^\infty I_t$ is an ideal, who is finitely generated by assumption. Given such a finite set, it must lie in I_k for some $k \geq 1$. The conclusion follows.

($\Leftarrow$) Suppose whenever $I_1 \subseteq I_2 \subseteq \cdots$ is an ascending chain of ideals, $k \geq 1$ such that $I_k = I_{k+i} = \bigcup_{t=1}^\infty I_t$ for all $i \geq 0$. Let $J \subseteq R$ be an ideal. Suppose for a contradiction J is not finitely generated. Then we can inductively produce a chain of strictly increasing ideals (by choosing elements not yet in the ideal produced by the prefix set), which contradicts our assumption. □

Lemma 3.6.4. *Let R be a noetherian ring and $I \lhd R$. Then R/I is noetherian.*

Proof. Let $q : R \to R/I$ be the quotient map. Let J be any ideal of R/I. The ideal $q^{-1}(J)$ is finitely generated by assumption, and the image of these generators generate J. □

Lemma 3.6.5. *Let R be a noetherian ring and $S \subseteq R$ be a multiplicative set. Then R_S is noetherian.*

Proof. Let $\lambda : R \to R_S$ be the natural ring homomorphism. By Lemma 2.1.18 the ideal generated by $\lambda(\lambda^{-1}(I)) = I$. Thus, the image of any finite set of generators of $\lambda^{-1}(I)$ under λ generates I. □

Lemma 3.6.6. *Let R be a noetherian ring and M be a finitely generated R-module. Then any submodule of M is also finitely generated.*

Proof. By assumption we have a surjective map of R-modules $q : R^n \to M$ for some $n \geq 0$. To show that $N \subseteq M$ is finitely generated, it is enough to show that $q^{-1}(N)$ is finitely generated. As this lies in R^n, we may assume that $M = R^n$.

We now do induction on n. The case $n = 1$ is immediate as submodules of R correspond to ideals and R is noetherian. Suppose $\phi : R^n \to R$ be the projection on the last factor. Let $N \subseteq R^n$ be a submodule. We have the exact sequence

$$0 \to N \cap R^{n-1} \to N \to \phi(N) \to 0$$

where R^{n-1} is viewed as a submodule of R^n via the map $(r_1, \ldots, r_{n-1}) \mapsto (r_1, \ldots, r_{n-1}, 0)$. $\phi(N)$ is finitely generated as it is an ideal in R, and $N \cap R^{n-1}$ is finitely generated by the inductive hypothesis.

Let $a_1, \ldots, a_k \in N \cap R^{n-1}$ generate $N \cap R^{n-1}$ and $b_1, \ldots, b_l \in \phi(N)$ generate $\phi(N)$. Let $b'_1, \ldots, b'_l \in R^n$ be such that $\phi(b'_i) = b_i$ for all $i \in \{1, \ldots, l\}$. Then, $\{a_1, \ldots, a_k, b'_1, \ldots, b'_k\}$ generate N, noting $(N \cap R^{n-1}) \times \phi(N) \simeq N$. □

Lemma 3.6.7. *Let R be a noetherian ring. If $I \lhd R$, there is a $t \geq 1$ such that $\mathfrak{r}(I)^t \subseteq I$. Consequently, some power of the nilradical of R is the 0-ideal.*

Proof. Noting $\mathfrak{r}(I)$ is an ideal, it is finitely generated, say $\mathfrak{r}(I) = (a_1, \ldots, a_k)$ for some $a_i \in R$. By definition of the radical, there exists an $n \geq 1$ such that $a_i^n \in I$ for all $i \in \{1, \ldots, k\}$. Define $t = k(n-1)+1$. Then, $\mathfrak{r}(I)^t \subseteq (a_1^n, \ldots, a_k^n) \subseteq I$ where the first inclusion comes from the pigenhole principle. □

Theorem 3.6.8 (Hilbert Basis Theorem)**.** *Let R be noetherian. Then, the polynomial ring $R[x]$ is also noetherian.*

Proof. Let $I \subseteq R[x]$ be an ideal. The leading coefficients of the non-zero polynomials in I (with 0) form an ideal J of R. As R is noetherian, J has a finite set of generators, say $a_1, \ldots, a_k$. For each $i \in \{1, \ldots, k\}$ choose $f_i \in I$ such that $f_i(x) - a_i x^{n_i}$ has degree lower than n_i. Define $n = \max_i n_i$. Let $I' = (f_1(x), \ldots, f_k(x)) \subseteq I$ be the ideal generated by $f_i(x)$. Define M to be the polynomials in I with degree less than n.

Suppose we choose $f(x) \in I \backslash (I' + M)$ of smallest possible degree m. Pick $a \in R$ such that $f - ax^m$ has degree lower than m. As $a \in J$, we have $a = r_1 a_1 + \cdots + r_k a_k$ for some $r_1, \ldots, r_k \in R$. Suppose $m \geq n$. Then,

$$f(x) - r_1 f_1(x) x^{m-n_1} - \cdots - r_k f_k(x) x^{m-n_k}$$

is degree less than m (by cancelling leading term) and lies in I by construction. By minimality of m, this lies in $I' + M$, so $f(x) \in I' + M$, which is a contradiction. If $m < n$, $f(x) \in M$, another contradiction. Consequently, $I = I' + M$.

R is an R-submodule (ideal) of the R-module consisting of polynomials of degree less than n, which is clearly finitely generated as an R-module. Thus, by Lemma 3.6.6, M is finitely generated as an R-module by $g_1(x), \dots, g_t(x) \in M$. Then, $g_1(x), \dots, g_t(x), f_1(x), \dots, f_k(x)$ is a set of generators of I as an ideal. □

Remark 3.6.9. As a consequence of the Hilbert Basis theorem, we see that $R[x_1, \dots, x_k]$ is noetherian for any $k \geq 0$. By noting Lemma 3.6.4, we see that every finitely generated algebra over a noetherian ring is noetherian.

Theorem 3.6.10 (Artin-Tate)**.** *Let T be a ring and $R, S \subseteq T$ be subrings. Suppose $R \subseteq S$ and R is noetherian. Suppose further that T is finitely generated as an R-algebra and that T is finitely generated as an S-module. Then, S is finitely generated as an R-algebra.*

Proof. Let $r_1, \dots, r_k$ be generators of T as an R-algebra. Let $t_1, \dots, t_l$ be generators of T as an S-module. By assumption, for any $a \in \{1, \dots, k\}$ we can write

$$r_a = \sum_{j=1}^{l} s_{ja} t_j$$

where $s_{ja} \in S$. Similarly, for any $b, d \in \{1, \dots, k\}$ we have,

$$t_b t_d = \sum_{j=1}^{l} s_{jbd} t_j$$

where $s_{jbd} \in S$, both of which we use the fact the left side in an element of T.

Define S_0 to be the R-subalgebra generated by all s_{ja} and s_{jbd}. As every element of T can be written as an R-linear combination of products of r_a, we see that T is finitely generated as an S_0-module with $t_1, \dots, t_l$. Note also that S_0 is a finitely generated R-algebra by construction.

The R-algebra S is naturally an S_0 algebra (by inclusion), specifically an S_0 module, and a S_0 submodule of T. As R is noetherian, S_0 is noetherian (as it is finitely generated by R). As S is a submodule of a finitely generated S_0-module (T), S is also finitely generated as a S_0 submodule by Lemma 3.6.6. Specifically, S is finitely generated as an S_0-algebra, and as S_0 is finitely generated over R, so is S.

$$\begin{tikzcd}
R \arrow[d] & S_0 \arrow[d, dashed] \arrow[dr, hook, "\iota"'] \arrow[dr, dashed, shift left=2] & \\
R[x_1, \dots, x_k] \arrow[ur, two heads] \arrow[r, two heads] & T & S \arrow[l, "\supseteq"']
\end{tikzcd}$$

Simple illustration above with abuse of notation, where dotted arrows are induced S_0 modules. □

Definition 3.6.11. *Let $I \lhd R$. We say that I is **irreducible** if whenever I_1 and I_2 are ideals of R and $I = I_1 \cap I_2$, $I = I_1$ or $I = I_2$. We say that an ideal is **decomposable by irreducible ideals** or dic if it has a finite intersection of irreducible ideals.*

Proposition 3.6.12. *Given $I \lhd R$, and R is noetherian, there exists irreducible ideals $I_1, \dots, I_k$ such that $I = \bigcap_{i=1}^{k} I_i$*

Proof. Suppose J is not dic. Specifically, J is not irreducible, and there exists ideals M, N such that $J = M \cap N$ and $J \subsetneq M$ and $J \subsetneq N$. As J is not dic, either N or M is not dic. Without loss of generality, suppose M is not dic. Repeating this produces a strictly increasing chain of non-dic ideals, contradicting the fact R is noetherian. □

Proposition 3.6.13. *Irreducible ideals are primary.*

Proof. Let J be an irreducible ideal and suppose that J is not primary. Then, there exists $x \in R/J$ who is a zero-divisor but not nilpotent. Let $q : R \to R/J$ be the quotient map. Now, consider the sequence

$$\operatorname{Ann}(x) \subseteq \operatorname{Ann}(x^2) \subseteq \operatorname{Ann}(x^3) \subseteq \cdots$$

Noting R/J is noetherian, the sequence must stop at some k such that

$$\operatorname{Ann}(x^k) = \operatorname{Ann}(x^{k+1}) = \operatorname{Ann}(x^{k+2}) = \cdots$$

for some $k \geq 1$.

Consider the ideal $(x^k) \cap \operatorname{Ann}(x^k)$. If $\lambda x^k \in (x^k) \cap \operatorname{Ann}(x^k)$ for some $\lambda \in R/J$, $\lambda x^{2k} = 0$, thus $\lambda \in \operatorname{Ann}(x^{2k})$. As $\operatorname{Ann}(x^{2k}) = \operatorname{Ann}(x^k)$, $\lambda x^k = 0$. Thus, $(x^k) \cap \operatorname{Ann}(x^k) = (0)$. That is, $q^{-1}(x^k) \cap q^{-1}(\operatorname{Ann}(x^k)) = J$. On the other hand, $(x^k) \neq (0)$ by nilpotence and $\operatorname{Ann}(x^k) \neq 0$ by construction. Hence, $q^{-1}(x^k) \neq J$ and $q^{-1}(\operatorname{Ann}(x^k)) \neq J$. This contradicts irreducibility. Thus, J is primary. □

Example 3.6.14. Primary ideals are not necessarily irreducible. Consider the ideal $(x, y)^2 \subseteq \mathbb{Q}[x, y]$. This is primary as $\mathfrak{r}((x, y)^2) = (x, y)$ is a maximal ideal by Lemma 3.5.8. However, this is the intersection of ideals (x, y^2) and (x^2, y).

Proposition 3.6.15 (Lasker-Noether)**.** *Let R be a noetherian ring. Then every ideal of R is decomposable.*

Proof. Follows from Propositions 3.6.12 and 3.6.13. □

Let R be a noetherian ring and $I \subseteq R$ be a radical ideal. As a consequence of Lasker-Noether and the remark after primary decomposition, we have a unique set $\{\mathfrak{q}_1, \ldots, \mathfrak{q}_k\}$ of distinct prime ideals in R such that

- $I = \bigcap_{i=1}^k \mathfrak{q}_i$
- for all $i \in \{1, \ldots, k\}$, $\mathfrak{q}_i \not\supseteq \bigcap_{j \neq i} \mathfrak{q}_j$

Moreover, the set $\{\mathfrak{q}_1, \ldots, \mathfrak{q}_k\}$ is the set of prime ideals that are minimal among the prime ideals containing I. In other words, $V(I)$ is the union of the closed sets $V(\mathfrak{q}_i)$.

If $\mathfrak{p}_1, \ldots, \mathfrak{p}_l$ is the set of minimal prime ideals of R, then there is a natural injective homomorphism of rings

$$R/\mathfrak{r}((0)) \hookrightarrow \prod_{i=1}^{l} R/\mathfrak{p}_i$$

4 Extensions

4.1 Integral Extensions

Definition 4.1.1. *Let B be a ring and $A \subseteq B$ be a subring. Let $b \in B$. We say that b is* ***integral*** *over A if there is a monic polynomial in $A[x]$ that annihalates b. Concretely, we have a $P(x) = x^n + a_{n-1}x^{n-1} + \ldots a_0 \in A[x]$ such that $P(b) = 0$.*

We say that b is ***algebraic*** *over A if there is a $Q(x) \in A[x]$ such that $Q(b) = 0$.*

Note that if A is a field, b is algebraic over A if and only if it is integral over A.

Definition 4.1.2. *Let $S \subseteq B$ be a subset, $A \subseteq B$ be a subring. Write $A[S]$ for the intersection of all the subrings of B which contain A and S. Note that $A[S]$ is naturally an A-algebra.*

As usual notation, we omit the set notation when it is clear (e.g., we write $A[b]$ for $A[\{b\}]$). If S is finite, we have

$$A[b_1, \dots, b_k] = \{Q(b_1, \dots, b_k) \mid Q(x_1, \dots, x_k) \in A[x_1, \dots, x_k]\}$$

which is the set of polynomials in A evaluated at $\{b_1, \dots, b_k\}$. Also Consequently, we have

$$A[b_1, \dots, b_k] = A[b_1] \cdots [b_k]$$

Proposition 4.1.3. *Let R be a ring and M be a finitely generated R-module. Let $\phi : M \to M$ be a homomorphism of R-modules. Then there exists a monic polynomial $Q(x) \in R[x]$ such that $Q(\phi) = 0$.*

Proof. By assumption, there is a surjective homomorphism of R-modules $\lambda : R^n \to M$ for some $n \geq 0$. Let $b_1, \dots, b_n$ be the natural basis for R^n. For each b_i, choose an element $v_i \in R^n$ such that $\lambda(v_i) = \phi(\lambda(b_i))$. Define a homomorphism of R-modules $\tilde{\phi} : R^n \to R^n$ by $\tilde{\phi}(b_i) = v_i$. By construction, we have $\lambda \circ \tilde{\phi} = \phi \circ \lambda$, thus $\lambda \circ \tilde{\phi}^n = \phi^n \circ \lambda$ for all $n \geq 0$. Hence, it is sufficient to find a monic polynomial $Q(x) \in R[x]$ such that $Q(\tilde{\phi}) = 0$. We may therefore assume that $M = R^n$.

Now, ϕ is described by an $n \times n$ matrix $C \in \mathrm{Mat}_{n\times n}(R)$. We thus need to find a monic polynomial $Q(x) \in R[x]$ such that $Q(C) = 0$.

Let $h : \mathbb{Z}[x_{11}, x_{12}, \dots, x_{21}, x_{22}, \dots, x_{nn}] \to R$ be a ring homomorphism sending x_{ij} to c_{ij}. Let D be a matrix whose image under h is C. If there is a monic polynomial $T(x) \in (\mathbb{Z}[x_{11}, x_{12}, \dots, x_{21}, x_{22}, \dots, x_{nn}])[x]$ such that $T(D) = 0$, then the monic polynomial $Q(x)$ whose coefficients are images of the coefficients of $T(x)$ under h has the property that $Q(C) = 0$. Thus it is sufficient to show for $R = \mathbb{Z}[x_{11}, x_{12}, \dots, x_{21}, x_{22}, \dots, x_{nn}]$.

Let K be the fraction field of R. The natural homomorphism of rings $R \to K$ is injective as $R = \mathbb{Z}[x_{11}, x_{12}, \dots, x_{21}, x_{22}, \dots, x_{nn}]$ is a domain. We may thus view R as a subring of K.

By Cayley-Hamilton, the polynomial $Q(x) = \det(xI - C) \in K[x]$ is monic and $Q(C) = 0$ when C is viewed as an element of $\mathrm{Mat}_{n\times n}(K)$. Since $Q(x)$ is a polynomial with coefficients of C, it has coefficients in R. □

Proposition 4.1.4. *Let A be a subring of the ring B. Let $b \in B$ and let C be a sunbring of B containing A and b. Then,*

1. *If the element $b \in B$ is integral over A, then the A-algebra $A[b]$ is finitely generated as an A-module*

2. *If C is finitely generated as an A-module, then b is integral.*

Proof. (i) If b is integral over A, we have

$$b^n = -a_{n-1}b^{n-1} - \cdots - a_1 b - a_0$$

for some $a_i \in A$. Thus b^{n+k} is in the A-submodule of B generated by $1, b, \dots, b^{n-1}$ for all $k \geq 0$. In particular, $A[b]$ is generated by $1, b, \dots, b^{n-1}$ as an A-module.

(ii) Let $[b] : C \to C$ be the homomorphism of A-modules such that $[b](v) = b \cdot v$ for all $v \in C$. By Proposition 4.1.3, there is a monic polynomial $Q(x) \in A[x]$ such that $Q([b]) = 0$. In particular, taking $Q([b])(1)$ shows b is integral over A. □

Lemma 4.1.5 (Generalization of Tower Law)**.** *let $\phi : R \to T$ be a homomorphism of rings and let N be a T-module. If T is finitely generated as an R-module and N is finitely generated as an T-module, N is finitely generated as an R-module.*

Proof. Suppose $t_1, \dots, t_k \in T$ are generators of T as an R-module and $l_1, \dots, l_s$ are generators of N as a T-module. Then, $t_i l_j$ are generators of N as an R-module. □

Corollary 4.1.6. *Let A be a subring of B. Let $b_1, \dots, b_k \in B$ be integral over A. Then, $A[b_1, \dots, b_k]$ is finitely generated as an A-module.*

Proof. By Proposition 4.1.4, $A[b_1]$ is finitely generated as an A-module, and $A[b_1, b_2] = A[b_1][b_2]$ is finitely generated as an $A[b_1]$-module, thus is finitely generated as an A-module. The proof follows by induction. □

Corollary 4.1.7. *Let A be a subring of B. The subset of elements of B which are integral over A form a subring of B.*

Proof. Let $b, c \in B$ be integral. Then, $b + c, bc \in A[b, c]$ and is finitely generated as an A-module. Thus by Proposition 4.1.4, $b + c$ and bc are integral over A. □

Definition 4.1.8. *Let $\phi : A \to B$ be a ring homomorphism. We say that B is **integral** over A if all the elements of B are integral over $\phi(A)$.*

*B is **finite** over A, or a **finite A-algebra** if B is a finitely generated $\phi(A)$-module.*

Note the identity that B is a finite A-algebra if and only if B is a finitely generated integral A-algebra.

Definition 4.1.9. *If A is a subring of a ring B, the set of elements of B which are integral over A is called the **integral closure** of A in B.*

*If A is a domain and K is the fraction field of A, A is said to be **integrally closed** if the integral closure of A in K is A.*

Example 4.1.10. $\mathbb{Z}$ is integrally closed, and if K is a field, so is $K[x]$. The integral closure of $\mathbb{Z}$ in $\mathbb{Q}(i)$ is $\mathbb{Z}(i)$.

Lemma 4.1.11. *Let $A \subseteq B \subseteq C$, wehere A is a subring of B and B is a subring of C. If B is integral over A and C is integral over B, then C is integral over A. Let $c \in C$. We have by assumption,*

$$c^n + b_{n-1}c^{n-1} + \cdots + b_0 = 0$$

for some $b_i \in B$. Define $B' = A[b_0, \dots, b_{n-1}]$. We use Proposition 4.1.4. Now, c is integral over B' and so $B'[c]$ is finitely generated as a B'-module. Thus $B'[c]$ is finitely generated as an A-module. Thus c is integral over A.

Consequently, the integral closure in C of the integral closure of A in B is the integral closure of A in C.

Lemma 4.1.12. *Let A be a subring of B. Let S be a multiplicative subset of A. Suppose that B is integral (respectively finite) over A. Then the natural ring homomorphism $A_S \to B_S$ makes B_S into an integral (respectively finite) A_S-algebra.*

Proof. We first prove the integrality case. Suppose that B is integral over A. We use the natural ring homomorphism from $A_S \to B_S$. Note first that this map is injective.

Let $b/s \in B_S$ where $b \in B$ and $s \in S$. By assumption, we have

$$b^n + a_{n-1}b^{n-1} + \cdots + a_0 = 0$$

for some $a_i \in A$. Thus,

$$(b/s)^n + (a_{n-1}/s)(b/s)^{n-1} + \cdots + a_0/s^n = (1/s^n)(b^n + a_{n-1}b^{n-1} + \cdots + a_0 = 0) = 0/1$$

Thus, b/s is integral over A_S.

For the finiteness, suppose that $a_1, \dots, a_k$ are generators for B as an A-module. Then $a_1/1, \dots, a_k/1 \in B_S$ are generators of B_S as an A_S module, so B_S is also finite over A_S. □

Lemma 4.1.13. *Suppose that C is a subring of a ring D. Suppose that D is a domain and that D is integral over C. Then D is a field if and only if C is a field.*

Proof. If either of the rings is 0, then both are the 0 ring, and the proof follows. We now suppose that C and D are not the zero ring.

($\Rightarrow$) Suppose that D is a field. Let $c \in C\backslash\{0\}$. We want to show that $c^{-1} \in D$ lies in C. By assumption, D is integral over C, so there is a polynomial $P(t) = t^n + a_{n-1}t^{n-1} + \cdots + a_0 \in C[t]$ such that $P(c^{-1}) = 0$ Thus, $c^{n-1}P(c^{-1}) = 0$. That is,

$$c^{-1} + a_{n-1} + \cdots + a_0 c^{n-1} = 0$$

implying that $c^{-1} \in C$.

($\Leftarrow$) Suppose that C is a field. Take $d \in D\backslash\{0\}$. We want to show that d has an inverse in D. Let $C[t] \to D$ be the C-algebra sending t to d. The kernel of this map is a prime ideal as D is a domain, and is non-zero as d is integral over C. Prime ideals are maximal in $C[t]$ as it is a PID, so the image of ϕ is a field, meaning d has an inverse in D. □

Corollary 4.1.14. *Let A be a subring of B and $\phi : A \to B$ be the inclusion map. Suppose that B is integral over A. Let $\mathfrak{q}$ be a prime ideal of B. Then $\mathfrak{q} \cap A$ is a maximal ideal of A if and only if $\mathfrak{q}$ is a maximal ideal of B.*

Proof. The induced map $A/(\mathfrak{q} \cap A) \to B/\mathfrak{q}$ is injective as the natural map from A to $B/\mathfrak{q}$ has kernel $\mathfrak{q} \cap A$. This makes $B/\mathfrak{q}$ into an integral $A/(\mathfrak{q} \cap A)$ algebra, by considering the same monic polynomial in $(A/(\mathfrak{p} \cap A)[x])$. Note that these are both domains, so the proof follows by Lemma 4.1.13. □

Theorem 4.1.15 (Going Up Theorem (Partial))**.** *Let A be a subring of B and let $\phi : A \to B$ be the inclusion map. Suppose that B is integral over A. Then* $\mathrm{Spec}(\phi) : \mathrm{Spec}(B) \to \mathrm{Spec}(A)$ *is surjective.*

Proof. Write $B_\mathfrak{p}$ for the localisation $B_{\phi(A/\mathfrak{p})}$ of the ring B at the multiplicative set $\phi(A/\mathfrak{p})$. By lemma 2.1.12, B is isomorphic to the localisation of B at $\mathfrak{p}$ when B is viewed as an A-module. We thus have a unique ring homomorphism $\phi_\mathfrak{p} : A_\mathfrak{p} \to B_\mathfrak{p}$ such that $\phi_\mathfrak{p}(a/1) = \phi(a)/1$. Write $\lambda_A : A \to A_\mathfrak{p}$ and $\lambda_B : B \to B_\mathfrak{p}$ for the natural ring homomorphisms. Then, we have $\lambda_B \circ \phi = \phi_\mathfrak{p} \circ \lambda_A$. This induces a commutative diagram

$$\begin{tikzcd}
\mathrm{Spec}(B_\mathfrak{p}) \arrow[r, "\mathrm{Spec}(\lambda_B)"] \arrow[d, "\mathrm{Spec}(\phi_\mathfrak{p})"] & \mathrm{Spec}(B) \arrow[d, "\mathrm{Spec}(\phi)"] \\
\mathrm{Spec}(A_\mathfrak{p}) \arrow[r, "\mathrm{Spec}(\lambda_A)"] & \mathrm{Spec}(A)
\end{tikzcd}$$

By Lemma 2.1.22, $\mathfrak{p}$ is the image of the maximal ideal $\mathfrak{m}$ of $A_\mathfrak{p}$ under the map $\operatorname{Spec}(\lambda_A)$. Thus it suffices to show that there is a prime ideal $\mathfrak{q}$ in $B_\mathfrak{p}$ such that $\phi_\mathfrak{p}^{-1}(\mathfrak{q}) = \operatorname{Spec}(\phi_\mathfrak{p})(\mathfrak{q}) = \mathfrak{m}$. By Lemma 4.1.12, $B_\mathfrak{p}$ is integral over $A_\mathfrak{p}$. By Corollary 4.1.14, choosing any maximal ideal $\mathfrak{q}$ of $B_\mathfrak{p}$, $\phi_\mathfrak{p}^{-1}(\mathfrak{q})$ is also a maximal ideal. As $A_\mathfrak{p}$ is local, $m = \phi_\mathfrak{p}^{-1}(\mathfrak{q})$. □

Corollary 4.1.16. *Let $\phi : A \to B$ be a homomorphism of rings. Suppose that B is integral over A. Then the map $\operatorname{Spec}(\phi) : \operatorname{Spec}(B) \to \operatorname{Spec}(A)$ is closed.*

Proof. Let $\mathfrak{p}$ be an ideal of B. We want to show that $\operatorname{Spec}(\phi)(V(\mathfrak{p}))$ is closed in $\operatorname{Spec}(A)$. Let $q_\mathfrak{p} : B \to B/\mathfrak{p}$ be the quotient map, and define $\mu := q_\mathfrak{p} \circ \phi : A \to B_\mathfrak{p}$. Also let $q_\mu : A \to A/\ker(\mu)$ be the quotient map, and $\psi : A/\ker(\mu) \to B$ be the ring homomorphism induced by μ Then, we have the following commutative diagram :

$$\begin{tikzcd}
A \arrow[r, "\phi"] \arrow[d, "q_\mu"] \arrow[dr, "\mu"] & B \arrow[d, "q_\mathfrak{p}"] \\
A/\ker(\mu) \arrow[r, "\psi"] & B/\mathfrak{p}
\end{tikzcd}$$

As B is integral over A, $B/\mathfrak{p}$ is integral over $A/\ker(\mu)$. Also, ψ is injective by construction. By Theorem 4.1.15, we have $\operatorname{Spec}(\psi)(\operatorname{Spec}(B/\mathfrak{p})) = \operatorname{Spec}(A/\ker(\mu))$. By Lemma 3.4.4, we have

$$\operatorname{Spec}(q_\mathfrak{p})(\operatorname{Spec}(B/\mathfrak{p})) = V(\ker(q_\mathfrak{p})) = V(\mathfrak{p})$$

and

$$\operatorname{Spec}(q_\mu)(\operatorname{Spec}(A/\ker(\mu))) = V(\ker(\mu))$$

Thus, $\operatorname{Spec}(\phi)(V(\mathfrak{p})) = V(\ker(\mu))$, which is closed. □

Consequently, if ϕ is surjective, then $\operatorname{Spec}(\phi)$ is a closed map. Specifically, $\operatorname{Spec}(\phi)$ is injective and continuous, thus is a homeomorphism onto its image.

Proposition 4.1.17. *Let $\phi : A \to B$ be a ring homomorphism and suppose that B is finite over A. Then the map $\operatorname{Spec}(\phi)$ has finite fibres (for any $\mathfrak{p} \in \operatorname{Spec}(A)$, $\operatorname{Spec}(\phi)^{-1}(\{\mathfrak{p}\})$ is finite).*

Proof. Let $q : A \to A/\ker(\phi)$ be the quotient map. The map $\operatorname{Spec}(q)$ has finite fibres (by bijective correspondence between primes). We can therefore consider $A/\ker(\phi) \simeq \operatorname{im}(\phi)$ instead of A, and view it as a subring of B.

Now let $\mathfrak{p}$ be a prime ideal of A. We want to show that there are finitely many prime ideals $\mathfrak{q}$ such that $\mathfrak{q} \cap A = \mathfrak{p}$ ($\mathfrak{q} \cap A$ is the preimage of $\mathfrak{q}$ under inclusion).

Let $\overline{\mathfrak{p}}$ be the ideal of B generated by $\mathfrak{p}$. Let ψ be the ring homomorphism induced by ϕ.

$$\begin{tikzcd}
\operatorname{Spec}(B/\overline{\mathfrak{p}}) \arrow[r, "\operatorname{Spec}(\overline{q})"'] \arrow[d, "\operatorname{Spec}(\psi)"'] & \operatorname{Spec}(B) \arrow[d, "\operatorname{Spec}(\phi)"] \arrow[dl] \\
\operatorname{Spec}(A/\mathfrak{p}) \arrow[r, "\operatorname{Spec}(q)"'] & \operatorname{Spec}(A)
\end{tikzcd}$$

Any prime ideal $\mathfrak{q} \in \operatorname{Spec}(B)$ such that $\mathfrak{q} \cap A = \mathfrak{p}$ has the property that $\mathfrak{q} \supseteq \overline{\mathfrak{p}}$, we see any such prime ideal lies in the image of $\operatorname{Spec}(\overline{q})$. The corresponding prime ideals of $\operatorname{Spec}(B/\overline{\mathfrak{p}})$ are prime ideals I such that $\psi^{-1}(I) = (0)$. Thus, it suffices to show that $\operatorname{Spec}(\psi)^{-1}((0))$ is a finite set.

Let $S = (A/\mathfrak{p})\backslash\{0\}$. Define $\lambda_{A/\mathfrak{p}} \to A/\mathfrak{p} \to (A/\mathfrak{p})_S$ and $\lambda_B/\overline{\mathfrak{p}} : B/\overline{\mathfrak{p}} \to (B/\overline{\mathfrak{p}})_{\psi(S)}$ be the natural ring homomorphisms. There is a natural ring homomorphism ψ_S that is compatible with these morphisms to obtain a commutative diagram

$$\begin{tikzcd}
\mathrm{Spec}((B/\overline{\mathfrak{p}})_{\psi(S)}) \arrow[r, "\mathrm{Spec}(\lambda_{B/\overline{\mathfrak{p}}})"] \arrow[d, "\mathrm{Spec}(\psi_S)"] & \mathrm{Spec}(B/\overline{\mathfrak{p}}) \arrow[d, "\mathrm{Spec}(\psi)"] \\
\mathrm{Spec}((A/\mathfrak{p})_{\psi(S)}) \arrow[r, "\mathrm{Spec}(\lambda_{A/\mathfrak{p}})"] & \mathrm{Spec}(A/\mathfrak{p})
\end{tikzcd}$$

If $q \in \mathrm{Spec}(B/\overline{\mathfrak{p}})$, then $\psi^{-1}(\mathfrak{q}) = (0)$ if and only if $\mathfrak{q} \cap \psi(S) = \emptyset$.

□

5 Noether Normalization + Hilbert's Nullstellensatz

Theorem 5.0.1 (Noether's Normalization Lemma)**.** *Let K be a field and R be a non-zero finitely generated K-algebra. Then, there exists an injective homomorphism of K-algebras $K[y_1, \dots, y_t] \to R$ for some $t \geq 0$ such that R is finite as a $K[y_1, \dots, y_t]$ module.*

Proof. We only prove the case for when K is infinite.

Let $r_1, \dots, r_n \in R$ be the generators of minimal size of R as a K-algebra. We prove by induction on n. If $n = 1$, then $R \simeq K[x]$ or $R \simeq K[x]/I$ for some proper ideal I in $K[x]$. In the first case, the proof follows by setting $t = 1$. In the second case, we set $t = 0$, noting that the K-dimension of $K[x]/I$ is bounded above by the degree of any non-zero polynomial in I. So this is true for $n = 1$.

Up to relabelling, we may assume there is a $k \in \{1, \dots, n\}$ such that for all $i \in \{1, \dots, k\}$, r_i is not algebraic over $K[r_1, \dots, r_{i-1}]$ and that r_{k+i} is algebraic over $K[r_1, \dots, r_k]$. We do this by repeatedly choosing elements that are not algebraic over $K[r_1, \dots, r_k]$ from $k = 0$. In the case that every generator is algebraic over K, they are integral over K. Then setting $t = 0$, it follows $R = K[r_1, \dots, r_n]$ is finite over K.

Now we may also assume that $k < n$, as else we may set $t = k = n$, sending x_i to the generators. Thus, r_n is algebraic over $K[r_1, \dots, r_{n-1}]$. Let $P_1(x) \in K[r_1, \dots, r_{n-1}][x]$ be a non-zero polynomial such that $P_1(r_n) = 0$. Since $K[r_1, \dots, r_{n-1}]$ is the image of $K[x_1, \dots, x_{n-1}]$ sending x_i to r_i, there is a non-zero polynomial

$$P(x_1, \dots, x_n) \in K[x_1, \dots, x_{n-1}][x_n] = K[x_1, \dots, x_n]$$

such that $P(r_1, \dots, r_n) = 0$.

Now let $F(x_1, \dots, x_n)$ be the sum of monomials of degree $d = \deg(P)$ which appear in P, such that $\deg(P - F) < d$. Choose $\lambda_i \in K$ such that

$$F(\lambda_1, \dots, \lambda_{n-1}, 1) \neq 0$$

To see why such set exists, as F is a homogenous polynomial, the polynomial $F(x_1, \dots, x_{n-1}, 1)$ is a sum of homogenous polynomials of distinct degrees and thus is non-zero (else by grouping we see the original polynomial is zero). This has some set that evaluates to a nonzero value, as K is infinite. To see this, we use the fact polynomials in $K[x]$ can only have finitely many roots, so it cannot vanish on every $F(x, \lambda_2, \dots, \lambda_{n-1}, 1) \in K[x]$.

Setting $u_i = r_i - \lambda_i r_n$, we have

$$\begin{aligned} 0 &= P(r_1, \dots, r_n) \\ &= P(u_1 + \lambda_1 r_n, \dots, u_{n-1} + \lambda_{n-1} r_n, r_n) \\ &= F(\lambda_1, \dots, \lambda_{n-1}, 1) r_n^d + O(r_n^{d-1}) \end{aligned}$$

In particular, r_n is integral over $K[u_1, \dots, u_{n-1}]$. By the inductive hypothesis, there is an injective homomorphism of K-algebras

$$K[y_1, \dots, y_t] \to K[u_1, \dots, u_{n-1}]$$

for some $t \geq 0$ such that $K[u_1, \dots, u_{n-1}]$ is integral over $K[y_1, \dots, y_t]$. Thus, $R = K[r_1, \dots, r_n] = K[u_1, \dots, u_n - 1][r_n]$ is integral over $K[y_1, \dots, y_t]$ (transitivity of integrality, algebraicity follows immediately). □

Corollary 5.0.2 (Weak Nullstellensatz)**.** *Let K be a field and R be a finitely generated K-algebra. Suppose that R is a field. Then R is finite over K.*

Proof. Let $K[y_1, \dots, y_t] \to R$ as in Noether's Normalization Lemma. By Theorem 4.1.15, $\operatorname{Spec}(R) \to \operatorname{Spec}(K[y_1, \dots, y_t])$ is surjective. As R is a field, $\operatorname{Spec}(R)$ has one element, so $\operatorname{Spec}(K[y_1, \dots, y_t])$ has one element. Thus $t = 0$ (else, consider the ideal (y_1), and note it is contained in some maximal ideal). Consequently, R is integral over K. As R is finitely generated over K, it must be finite over K. □

Corollary 5.0.3. *Let K be an algebraically closed field. Let $t \geq 1$. The ideal of $K[x_1, \dots, x_t]$ is maximal if and only if it has the form $(x_1 - a_1, \dots, x_t - a_t)$ for some $a_1, \dots, a_t \in K$. A polynomial Q lies in this ideal if and only if $Q(a_1, \dots, a_t) = 0$.*

Proof. We start with the first statement. ($\Leftarrow$) The ideal $(x_1 - a_1, \dots, x_t - a_t)$ is the kernel of the evaluation map

$$K[x_1, \dots, x_t] \to K \qquad p(x_1, \dots, x_t) \mapsto p(a_1, \dots, a_t)$$

which is a surjective morphism onto a field, thus the kernel is a maximal ideal. ($\Rightarrow$) Suppose that I is maximal. $K[x_1, \dots, x_t]/I$ is a field, which is also a finitely generated K-algebra. Thus, by Corollary 5.0.2, $K[x_1, \dots, x_t]/I$ is finite, thus algebraic over K. As K is algebraically closed, $K[x_1, \dots, x_t]/I \simeq K$.

$$\begin{tikzcd} K[x_1, \dots, x_t] \arrow[d, "q_I"'] \arrow[dr, dashed, "\phi"] & \\ K[x_1, \dots, x_t]/I \arrow[r, "\psi"'] & K \end{tikzcd}$$

Consider ϕ as the induced homomorphism of K-algebras. By construction, I contains the ideal $(x_1 - \phi(x_1), \dots, x_t - \phi(x_t))$ (by isomorphism, as ϕ takes this to 0, q_I also takes this to 0). Ideals of this form are maximal, so in particular this coincides with I.

For the second part, note the homomorphism of K-algebras $\psi : K[x_1, \dots, x_t] \to K$ such that $\psi(P(x_1, \dots, x_t)) = P(a_1, \dots, a_t)$ is surjective and the $\ker(\psi) \supseteq (x_1 - a_1, \dots, x_t - a_t)$. As ψ is nonzero, $\ker(\psi)$ is maximal, and $\ker(\psi) = (x_1 - a_1, \dots, x_t - a_t)$. □

Corollary 5.0.4. *Let K be a field. Let R be a finitely generated K-algebra. Then R is a Jacobson ring.*

Proof. Let $I \subseteq R$ be an ideal. We want to show that the Jacobson radical of I coincides with the radical of I. So, we want to show that the nilradical of R/I coincides with the Jacobson radical of (0) in R/I. Thus we may replace R with R/I and suppose that $I = (0)$.

Let $f \in R$ and suppose that f is not nilpotent. It is sufficient by showing that there exists a maximal ideal $\mathfrak{m}$ in R such that $f \notin \mathfrak{m}$. Let $S = \{1, f, f^2, \dots\}$. As f is not nilpotent, the localisation is non-zero. Let $\mathfrak{q}$ be a maximal ideal of R_S. Since R_S is a finitely generated K-algebra, the quotient ring is also finitely generated over K. By weak Nullstellensatz, the canonical homomorphism of rings $K \to R_S/\mathfrak{q}$ makes $R_S/\mathfrak{q}$ into a finite field extension of K. Define ϕ to be the natural homomorphism that composes the homomorphisms from $R \to R_S$ and $R_S \to R_S/\mathfrak{q}$. Then $\mathrm{im}(\phi)$ is a domain, which is integral over K. By Lemma 4.1.13, this is a field. Thus $\ker(\phi)$ is maximal ideal of R.

By construction, $\ker(\phi)$ is the inverse image of $\mathfrak{q}$ by the natural homomorphism $R \to R_S$. As $f/1$ is a unit in R_S, $f/1 \notin \mathfrak{q}$, thus $f \notin \ker(\phi)$. We set $\mathfrak{m} = \ker(\phi)$ and are done. □

Corollary 5.0.5 (Strong Nullstellensatz)**.** *Let K be an algebraically closed field. Let $t \geq 1$ and $I \subseteq K[x_1, \dots, x_t]$ be an ideal. Define*

$$Z(I) = \{(c_1, \dots, c_t) \in K^n \mid P(c_1, \dots, c_n) = 0 \text{ for all } P \in I\}$$

Let $Q(x_1, \dots, x_t) \in K[x_1, \dots, x_t]$. Then $Q \in \mathfrak{r}(I)$ if and only if $Q(c_1, \dots, c_t) = 0$ for all $(c_1, \dots, c_t) \in Z(I)$.

Proof. Let $R = K[x_1, \dots, x_t]$.

($\Rightarrow$) Take any $Q \in \mathfrak{r}(I)$ and $(c_1, \dots, c_t) \in Z(I)$. We want to show $Q(c_1, \dots, c_t) = 0$. If $Q \in \mathfrak{r}(I)$, there exists some m such that $Q^m \in I$. Thus, $Q^m(c_1, \dots, c_t) = 0$. As we are in a field, this shows $Q(c_1, \dots, c_t) = 0$.

($\Leftarrow$) Let $Q(x_1, \dots, x_t) \in K[x_1, \dots, x_t]$ and suppose that $Q(c_1, \dots, c_t) = 0$ for all $(c_1, \dots, c_t) \in Z(I)$. Suppose for contradiction that $Q \notin \mathfrak{r}(I)$. By Corollary 5.0.4, R is a Jacobson ring, thus there exists a maximal ideal $\mathfrak{m} \supseteq I$ and $Q \notin \mathfrak{m}$.

By Corollary 5.0.3, we have $\mathfrak{m} = (x_1 - a_1, \dots, x_t - a_t)$ for some a_i. By construction, $P(a_1, \dots, a_t) = 0$ for all $P \in I \subseteq \mathfrak{m}$. Thus $(a_1, \dots, a_t) \in Z(I)$. By Corollary 5.0.3 again, $Q(a_1, \dots, a_t) \neq 0$ as $Q \notin \mathfrak{m}$, which is a contradiction. Thus $Q \in \mathfrak{r}(I)$. □

Lemma 5.0.6. *Let K be a field. Let $t \geq 1$ and let $P(x_1, \dots, x_t)$ and let $P(x_1, \dots, x_t) \in K[x_1, \dots, x_t]$. Then there exists a non-zero prime ideal in $K[x_1, \dots, x_t]$ which does not contain $P(x_1, \dots x_t)$.*

Proof. Let $L = K(x_1, \dots, x_{t-1})$ be the quotient field of $K[x_1, \dots, x_{t-1}]$ where $L = K$ if $t = 1$. Let

$$\iota : K[x_1, \dots, x_t] = K[x_1, \dots, x_{t-1}][x_t] \to L[x_t]$$

be the natural injective map. If there is a prime ideal $\mathfrak{p}$ in $L[x_t]$ such that $\iota(P) \notin \mathfrak{p}$, the prime ideal $\iota^{-1}(\mathfrak{p})$ will not contain P, so we may assume that $t = 1$.

Write $x_t = x_1 = x$ so $K[x_1, \dots, x_t] = K[x]$. Assume without loss of generality that $P(x)$ is monic. Also assume that $P(x)$ is not constant (else any maximal ideal suffices).

Let Q be an irreducible factor of $1 + P$. The ideal (Q) does not contain P as else $(Q) = K[x]$, but (Q) is prime. □

Lemma 5.0.7 (Alternative Proof for Weak Nullstellensatz)**.** *Let K be a field and R be a finitely generated K-algebra. Suppose that R is a field. Then R is finite over K.*

Proof. Let $r_1, \dots, r_k$ be generators of R over K. Suppose that r_i are numbered in a way that $r_1, \dots, r_l$ are algebraically independent over K and that r_{k+l} are algebraic over $K(r_1, \dots, r_l)$.

We may also take $l \geq 1$ as else R is a finite field extension of K (as R is integral and finitely generated K-algebra), thus we are done.

As R is a field, the quotient field $L \simeq K(x_1, \dots, x_l)$ of $K[x_1, \dots, x_l] \simeq K[r_1, \dots, r_l]$ (by first isomorphism) can be viewed as a subfield of R. Now R is generated by $r_{l+1}, \dots, r_k$ as an L-algebra and generators are algebraic over L as they are algebraic over $K(r_1, \dots, r_l)$. As L is a field, they are integral over L, and thus R is a finite field extension of L.

By the Artin-Tate Lemma, L is finitely generated as an K-algebra. In particular $K(x_1, \dots, x_l) \simeq L$ is finitely generated as a $K[x_1, \dots, x_l]$ algebra. Let $P_1(x)/Q_1(x), \dots, P_a(x)/Q_a(x)$ be the generators of $K(x_1, \dots, x_l)$ as an $K[x_1, \dots, x_l]$-algebra. Let $Q(x) = \prod_{i=1}^{a} Q_i(x)$ and $S = \{1, Q(x), Q^2(x), \dots\}$. As $K[x_1, \dots, x_l]$ is a domain, the localisation $K[x_1, \dots, x_l]_S$ can be viewed as a subring of $K(x_1, \dots, x_l)$. As every element can be written as a quotient $R(x)/Q^b(x)$ for some $b \geq 0$, $K[x_1, \dots, x_l]_S = K(x_1, \dots, x_l)$. As the field has one prime ideal, we know that any non-zero prime ideal contains $Q(x)$.

This contradicts Lemma 5.0.6, thus $l = 0$, meaning R is a finite field extension of K. □

Lemma 5.0.8. *Let R ba a Jacobson ring. Suppose that R is a domain. Let $b \in R$ and $S = \{1, b, b^2, \dots\}$. Suppose that R_S is a field. Then R is a field.*

Proof. We know by Lemma 2.1.18, there is a bijective correspondence with prime ideals of R that don't meet b with the prime ideals of R_S. As R_S is a field, we only have the (0) ideal. Hence every non-zero prime ideal of R meets b.

Suppose for a contradiction that (0) is not the maximal ideal of R. The radical of (0) is just (0) as R is a domain, but as R is Jacobson, (0) is the intersection of maximal ideals of R, all of which should contain b, a contradiction. Thus (0) is a maximal ideal. R is thus a field. □

Corollary 5.0.9. *Let T be a field and $R \subseteq T$ be a subring. Suppose that R is Jacobson. Suppose also that T is finitely generated over R. Then R is a field. Consequently, T is finite over R.*

Proof. Let $K \subseteq T$ be the fraction field of R. By Weak Nullstellensatz, T is a finite extension of K. Let $t_1, \dots, t_k \in T$ be the generators of T as an R-algebra. Take the set of monic polynomial over K that annihalate t_i. Let b be the product of every denominator that appears as coefficients in thesep polynomials, and set $S = \{1, b, b^2, \dots\}$. Then there is a natural injective homomorphism of R-algebras from R_S into K as R is a domain, and we may view R_S as a sub-R-algebra of K. By construction T is generated by t_i as an R_S algebra and the elements are integral over R_S. Thus T is finite over R_S. By Lemma 4.1.13, R_S is a field. By 5.0.8, R is a field. □

Corollary 5.0.10. *Let T be a field and $R \subseteq T$ be a subring. Suppose that R is noetherian. Suppose also that T is finitely generated over R. Then R is a field. Again, thus, T is finite over R.*

Proof. Let $K \subseteq T$ be the fraction field of R. By Weak Nullstellensatz T is a finite extension of K. Then K is finitely generated over R by Artin Tate. By taking the generators and multiplying the denominators together, we can form a multiplicative set generated by a single element of R such that $K = R_S$. Thus R is a field by Lemma 5.0.8. □

Corollary 5.0.11. *Let $\psi : R \to T$ be a homomorphism of rings. Suppose that R is Jacobson and that T is a finitely generated R algebra. Let $\mathfrak{m}$ be a maximal ideal of T. Then $\psi^{-1}(\mathfrak{m})$ is a maximal ideal of R and the induced map $R/\psi^{-1}(\mathfrak{m}) \to T/\mathfrak{m}$ makes $T/\mathfrak{m}$ into a finite field extension of $R/\psi^{-1}(\mathfrak{m})$.*

Proof. Note that $T/\mathfrak{m}$ is a field that is finitely generated over $R/\psi^{-1}(\mathfrak{m})$

$$\begin{tikzcd}
 & R \arrow[rr, "q_{\psi^{-1}(\mathfrak{m})}"] \arrow[dl, "\iota"'] \arrow[dd, "\psi"] & & R/\psi^{-1}(\mathfrak{m}) \arrow[dl] \arrow[dd, dashed] \\
R[x_1, \dots, x_n] \arrow[rr, dashed] \arrow[dr, two heads] & & R/\psi^{-1}(\mathfrak{m})[x_1, \dots, x_n] \arrow[dr, dashed] & \\
 & T \arrow[rr, "q_{\mathfrak{m}}"] & & T/\mathfrak{m}
\end{tikzcd}$$

Quotients of Jacobson ring are Jacobson, so it follows by Corollary 5.0.9. □

Theorem 5.0.12. *A finitely generated algebra over a Jacobson ring is Jacobson.*

Proof. Let R be a Jacobson ring and T be a finitely generated R-algebra. Let $I \subseteq T$ be an ideal. We want to show that the Jacobson radical of I of T coincides with the radical of I. Thus, we want to show that the nilradical of T/I coincides with the Jacobson radical of the zero ideal in T/I. As T/I is also finitely generated over R, we may replace T by T/I and suppose that $I = 0$.

Suppose that $f \in T$ and that f is not nilpotent. We want to show that there exists a maximal ideal $\mathfrak{m}$ in T such that $f \notin \mathfrak{m}$. Let $S = \{1, f, f^2, \dots\}$. By non-nilpotence, the localisation is not the zero-ring. Let $\mathfrak{q}$ be a maximal ideal of T_S. T_S is a finitely generated R-algebra as T is a finitely generated R-algebra, thus $T_S/\mathfrak{q}$ is finitely generated over R.

Let ϕ be the canonical ring homomorphism. From Corollary 5.0.11, noting that the kernel of ϕ is just the preimage of $\mathfrak{q}$ in R, we see that $\ker(\phi)$ is a maximal ideal and $T_S/\mathfrak{q}$ is a finite field extension of $R/\ker(\phi)$.

$$\begin{tikzcd}
R \arrow[r] \arrow[d] \arrow[dr, "\phi"] & R/\ker(\phi) \arrow[d, hook, dashed] \\
T_S \arrow[r] & T_S/\mathfrak{q}
\end{tikzcd}$$

Considering the natural map $\Phi : T \to T_S/\mathfrak{q}$, the image $\mathrm{im}(\Phi)$ is an R-subalgebra, thus a $R/\ker(\phi)$-subalgebra of $T_S/\mathfrak{q}$. As $T_S/\mathfrak{q}$ is integral over $R/\ker(\phi)$, $\mathrm{im}(\Phi)$ is integral over $R/\ker(\phi)$, by Lemma 4.1.13, is a field. Thus, $\ker(\Phi)$ is a maximal ideal of T. By construction, $\ker(\Phi)$ is the inverse image of $\mathfrak{q}$ by the natural homomorphism $T \to T_S$ and $f/1 \notin \mathfrak{q}$ as f is a unit in T_S. Thus $f \notin \ker(\Phi)$. The proof concludes by choosing $\mathfrak{m} = \ker(\Phi)$. □

Remark 5.0.13. Noting that $\mathbb{Z}$ is Jacobson, any finitely generated algebra over $\mathbb{Z}$ is a Jacobson ring.

6 Dimension

Definition 6.0.1. *Let R be a ring. The **dimension** of R is*

$$\dim(R) = \sup\{n \mid \mathfrak{p}_0 \supsetneq \mathfrak{p}_1 \supsetneq \cdots \supsetneq \mathfrak{p}_n, \mathfrak{p}_0, \dots, \mathfrak{p}_n \in \mathrm{Spec}(R)\}$$

*If $\mathfrak{p}$ is a prime ideal of R, the **codimension** (or **height**) of $\mathfrak{p}$ is*

$$\mathrm{ht}(\mathfrak{p}) = \sup\{n \mid \mathfrak{p} \supsetneq \mathfrak{p}_1 \supsetneq \cdots \supsetneq \mathfrak{p}_n, \mathfrak{p}_0, \dots, \mathfrak{p}_n \in \mathrm{Spec}(R)\}$$

Note that dimension need not be finite. Note that if $\mathfrak{q}$ is a prime ideal and $\mathfrak{q} \subsetneq \mathfrak{p}$, then $\operatorname{ht}(\mathfrak{p}) > \operatorname{ht}(\mathfrak{q})$ given that $\operatorname{ht}(\mathfrak{p})$ is finite. If N is the nilradical of R, then it is contained in every prime ideal of R, thus

$$\dim(R) = \dim(R/N)$$

where $\operatorname{ht}(\mathfrak{p} \bmod N) = \operatorname{ht}(\mathfrak{p})$. Finally,

$$\dim(R) = \sup\{\operatorname{ht}(\mathfrak{p}) \mid \mathfrak{p} \in \operatorname{Spec}(R)\}$$

Notably, for any ideal $I \subseteq R$, $\dim(R) \geq \dim(R/I)$ by bijective correspondence of ideals.

Lemma 6.0.2. *Let R be a ring and $\mathfrak{p} \in \operatorname{Spec}(R)$. Then $\operatorname{ht}(\mathfrak{p}) = \dim(R_{\mathfrak{p}})$. Also,*

$$\dim(R) = \sup\{\operatorname{ht}(\mathfrak{p}) \mid \mathfrak{p} \text{ is a maximal ideal of } R\}$$

Proof. By Lemma 2.1.18, the primes in $R_{\mathfrak{p}}$ are in one to one correspondence with the prime ideals contained in $\mathfrak{p}$. The correspondence preserves inclusion. Thus the first case follows immediately.

For the second case, note that

$$\dim(R) \geq \sup\{\operatorname{ht}(\mathfrak{p}) \mid \mathfrak{p} \text{ is a maximal ideal of } R\}$$

so we only need the reverse inequality. For this, suppose $\mathfrak{p}$ is a prime ideal which is not maximal. Consider a chain of prime ideals

$$\mathfrak{p} \supsetneq \mathfrak{p}_1 \supsetneq \cdots \supsetneq \mathfrak{p}_n$$

and let $\mathfrak{m}$ be a maximal ideal containing $\mathfrak{p}$. Then we have a chain

$$\mathfrak{m} \supsetneq \mathfrak{p} \supsetneq \mathfrak{p}_1 \supsetneq \cdots \supsetneq \mathfrak{p}_n$$

thus $\operatorname{ht}(\mathfrak{m}) \geq \operatorname{ht}(\mathfrak{p})$, and hence follows. □

Remark 6.0.3. We record a consequence of the previous lemma. If R is a ring and S is a multiplicative subset of R. Let $\mathfrak{p}$ be a prime ideal of R_S and $\lambda : R \to R_S$ be the natural ring homomorphism. Then $\operatorname{ht}(\mathfrak{p}) = \operatorname{ht}(\lambda^{-1}(\mathfrak{p}))$ by Lemma 2.1.18.

Definition 6.0.4. *Let R be a ring and $I \subseteq R$ be an ideal. Define the **codimension** or **height** $\operatorname{ht}(I)$ of I as*

$$\operatorname{ht}(I) = \min\{\operatorname{ht}(\mathfrak{p}) \mid \mathfrak{p} \in \operatorname{Spec}(R), \mathfrak{p} \supseteq I\}$$

This is a generalization of the definition from prime ideals to ideals. By definition, if J is another ideal such that $J \subseteq I$, then $\operatorname{ht}(J) \leq \operatorname{ht}(I)$. Also, by definition, given $\operatorname{ht}(I) < \infty$, there is some prime ideal $\mathfrak{p}$ which is minimal among the prime ideals containing I such that $\operatorname{ht}(\mathfrak{p}) = \operatorname{ht}(I)$.

Definition 6.0.5. *Let k be a field and K be a field containing k. If $S \subseteq K$ is a finite subset of K, write $k(S)$ for the smallest subfield of K containing k and S. By construction, this is isomorphic to the field of fractions of the k-algebra $k[S] \subseteq K$. As usual, we write $k(\alpha_1, \ldots, \alpha_n)$ for $k(\{\alpha_1, \ldots, \alpha_n\})$.*

Note the identity, $k(S_1 \cup S_2) = k(S_1)(S_2)$ (by definition).

Lemma 6.0.6. *If the elements of a finite S are algebraic over k, then $k(S) = k[S]$.*

Proof. It suffices to show the case for one element and use the identity above for induction. We now have a homomorphism $k[t] \to K$ that sends t to s. As the image of this map is a domain, the kernel is a prime ideal, and is non-zero as s is algebraic over k. As $k[t]$ is a PID, non-zero prime ideals are maximal. Thus, $k[s]$ is a field. □

Also note that if all the elements of S are algebraic over k, then it is integral over k, $k(S)$ is a finite extension of k.

If there is a finite subset S of K such that $K = k(S)$, we say that K is finitely generated over k as a field. This is strictly weaker than a finitely generated k-algebra (consider $k(x)$), but coincides when all the elements of S are algebraic over k.

Definition 6.0.7. *Let S be subset of K. Then S is a* ***finite transcendence basis*** *of K over k if*

- *S is finite*
- *the elements of S are algebraically independent over k*
- *K is algebraic over the field $k(S)$*

Lemma 6.0.8. *If K is finitely generated over k as a field, then K has a transcendence basis over k.*

Proof. Start with a finite set S such that $K = k(S)$. Take a subset S' that is algebraically independent with maximal cardinality. Then, the elements of $S \backslash S'$ are algebraic over $k(S')$ and thus K is algebraic over $k(S')$. This gives a transcendence basis over k. □

Proposition 6.0.9. *Let K be a field and $k \subseteq K$ be a subfield. Suppose that K is finitely generated over k as a field. Let S and T be two transcendence bases of K over k. Then $|S| = |T|$.*

Proof. Write $S = \{\gamma_1, \ldots, \gamma_n\}$ and $T = \{\rho_1, \ldots, \rho_m\}$ such that $n = |S|$ and $m = |T|$. We will show $m = n$ by induction on $\min(m, n)$.

In the case $\min(m, n) = 0$, either S or T is empty, so K is algebraic over k, meaning both S and T must be empty.

Without loss of generality, we may assume that $S \cap T = \emptyset$. To see this, suppose that $S \cap T = U$ and $U \neq \emptyset$. Then, $S \backslash U$ and $T \backslash U$ are transcendence bases for K over $k(U)$. Also,

$$\min(|S \backslash U|, |T \backslash U|) = \min(m, n) - |U|$$

Thus by induction, $|S \backslash U| = |T \backslash U|$, so $|S| = |T|$.

We also claim that m or n is minimal among the cardinalities of all possible transcendence bases of K over k. To see this, suppose that without loss of generality that $m \leq n$ such that $m = \min(m, n)$. Suppose that $m = |T|$ is not minimal. Choose a transcendence basis T' of K over k such that $|T'| < m$ that is minimal. Then, $\min(|T|, |T'|) < \min(m, n)$, thus by induction $|T'| = |T| = m$, a contradiction. Consequently, m is minimal.

Suppose without loss of generality that m is minimal among the cardinalities of all possible transcendence bases of K over k, swapping S and T if necessary. By assumption, there is a non-zero polynomial

$$P(x_0, \ldots, x_m) \in k[x_0, \ldots, x_m]$$

such that $P(\gamma_1, \rho_1, \ldots, \rho_m) = 0$. To see this, note that γ_1 is algebraic over $k(\rho_1, \ldots, \rho_m) \simeq \text{Frac}(k[x_1, \ldots, x_m])$, thus there is a non-zero annihalating polynomial for γ_1. We can thus make a polynomial over $k[x_1, \ldots, x_m]$ that annihalates γ_1. Take P to be of minimal degree with such property.

By assumption, $P(x_0, \ldots, x_m)$ contains monomials with positive powers of x_k for some $k \geq 1$, as else γ_1 is algebraic over k. By reordering, suppose this is x_1. Thus,

$$P(x_0, \ldots, x_m) = \sum_j P_j(x_0, x_2, \ldots, x_m) x_1^j$$

As P contains monomials with positive powers of x_1, there is some $j_0 > 0$ such that $P_{j_0}(x_0, x_2, \ldots, x_m) \neq 0$. Take a maximal such j_0. Also, $P_{j_0}(\gamma_1, \ldots, \rho_2, \ldots, \rho_m) \neq 0$ by the minimality of the degree of P. Then, as

$$P(\gamma_1, \rho_1, \ldots, \rho_m) = \sum_j P_j(\gamma_1, \rho_2, \ldots, \rho_m)\rho_1^j = 0$$

we see that ρ_1 is algebraic over $k(\gamma_1, \rho_2, \ldots, \rho_m)$.

Hence, $k(\gamma_1, \rho_1, \ldots, \rho_m)$ is algebraic over $k(\gamma_1, \rho_2, \ldots, \rho_m)$ and thus K is algebraic over $k(\gamma_1, \rho_2, \ldots, \rho_m)$ (by using Proposition 4.1.4 and Corollary 4.1.6).

As m is minimal, γ_1 is algebraically independent with $\rho_2, \ldots, \rho_m$, thus $\{\gamma_1, \rho_2, \ldots, \rho_m\}$ is a transcendence basis of K. In particular, $\{\gamma_2, \ldots, \gamma_n\}$ and $\{\rho_2, \ldots, \rho_m\}$ are transcendence bases of K over $k(\gamma_1)$. By induction, $m - 1 = n - 1$, so the proof follows. □

Definition 6.0.10. *Let k be a subfield of K and suppose that K is finitely generated over k as a field. Following the previous Proposition, define the **transcendence degree** $\mathrm{tr}(K|k)$ of k over K as the cardinality of any transcendence basis of K over k.*

For example, $\mathrm{tr}(k(x_1, \ldots, x_n)|k) = n$ for any field k.

Definition 6.0.11. *A **ring grading** on R is the datum of a sequence $R_0, R_1, \ldots$ of additive subgroups of R such that $R = \bigoplus_{i\geq 0} R_i$ and $R_i \cdot R_j \subseteq R_{i+j}$.*

*If $r \in R$, write $[r]_i$ for the projection of r to R_i and is called the **i-th graded component** of r.*

By definition, R_0 is a subring of R and for any i_0, $\bigoplus_{i\geq i_0} R_i$ is an ideal of R. Each R_i naturally carries a structure of an R_0-module.

Finally, the natural map $R_0 \to R/(\bigoplus_{i\geq 1} R_i)$ is an isomorphism of rings (as the natural map from $R \to R_0$ has kernel $\bigoplus_{i\geq 1} R_i$). In general, there is a natural isomorphism of R_0 modules $R_{i_0} \simeq (\bigoplus_{i\geq i_0} R_i)/(\bigoplus_{i\geq i_0+1} R_i)$ for any $i_0 \geq 0$, by first isomorphism theorem by considering it's natural map.

If k is a field, then the ring $k[x]$ has a natural grading given by $(k[x])_i = \{a \cdot x^i \mid a \in k\}$. Any ring carries a trivial grading such that $R_0 = R$ and $R_i = 0$ for all $i \geq 0$.

Definition 6.0.12. *Suppose that R is a graded ring. Suppose further that M is an R-module. A grading on M (relative to the grading on R) is the datum of a sequence $M_0, M_1, \ldots$ of additive subgroups of M such that $M = \bigoplus_{i\geq 0} M_i$ and $R_i \cdot M_j \subseteq M_{i+j}$. Then, we say that M is **graded as a R-module** (but the underlying grading of R is important).*

Lemma 6.0.13. *Let R be a graded ring with grading $R_i, (i \geq 0)$. The following are equivalent*

1. *The ring R is noetherian*
2. *The ring R_0 is noetherian and R is finitely generated as an R_0-algebra*

Proof. The implication $(ii) \implies (i)$ is a consequence of the Hilbert's basis theorem and Lemma 3.6.4.

We show the implication $(i) \implies (ii)$. Note first the ring R_0 is noetherian as it is a quotient of a noetherian ring. We now want to show that R is finitely generated as an R_0-algebra.

Let $a_1, \ldots, a_k$ be the generators of $\bigoplus_{i>0} R_i$ viewed as an ideal of R (as R is noetherian). We claim that the component of a_i generate R as an R_0-algebra, noting that each a_i has finitely many graded components.

We proceed by induction on $i \geq 0$ that R_i lies inside the R_0-subalgebra generated by the graded components of $a_1, \ldots, a_k$. As R is generated by all the R_i, this proves the claim. The claim is immediate for $i = 0$. Suppose that $i > 0$ and $R_0, \ldots, R_{i-1}$ all lie inside the R_0-subalgebra generated by the graded components of $a_1, \ldots, a_k$.

Let $r \in R_i$. By assumption, there are elements $t_i, \ldots, t_k \in R$ such that $r = t_1 a_1 + \cdots + t_k a_k$ (as they generate $\bigoplus_{i>0} R_i$). Now,

$$r = [r]_i = \sum_{j=1}^{k} \sum_{u=1}^{i} [t_j]_{i-u} [a_j]_u$$

Noting that $[t_j]_{i-u} \in R_0 \oplus R_1 \oplus \cdots \oplus R_{i-1}$, $[t_j]_{i-u}$ lies in the R_0-subalgebra generated by the graded components of $a_1, \ldots, a_k$ by the inducitve hypothesis. Now r lies in the R_0-subalgebra also, thus completes the proof. □

Definition 6.0.14. *Let R be a ring and M be an R-module. A **descending filtration** $M_\bullet$ of M is a sequence of R-submodules*

$$M = M_0 \supseteq M_1 \supseteq M_2 \supseteq \cdots$$

*of M. If I is an ideal of R, then $M_\bullet$ is said to be an I-**filtration** if $IM_i \subseteq M_{i+1}$ for all $i \geq 0$. An I-filtration $M_\bullet$ is said to be **stable** if $IM_i = M_{i+1}$ for all i larger than some fixed natural number.*

Definition 6.0.15. *Suppose we have a ring R and an ideal I of R, an R-module M and an I-filtration $M_\bullet$ on M. The directed sum of R-modules $R^\# = \bigoplus_{i \geq 0} I^i$ as an external sum (where $I^0 = R$) carries a natural structure of a graded ring, with the grading given as follows.*

*If $\alpha \in I^i$ and $\beta \in I^j$, then the product of α and β in $R^\#$ is given by the product of α and β in R, viewed as an element of I^{i+j}. The ring $R^\#$ is often called the **blow-up algebra** associated with R and I.*

The directed sum $M^\# = \bigoplus_{i \geq 0} M_i$ of R-modules carries a natural structure of graded $R^\#$ module, where if $a \in I^i$ and $\beta \in M_j$, the multiplication is of β by α in M viewed as an element in M_{i+j}, which it lies in as $M_\bullet$ is an I-filtration.

We can view $R^\#$ as an R-algebra by the natural injective map from $r \in R$ to the corresponding element of degree 0. The R-module structure on $M^\#$ is given by $M^\#$ viewed as a direct sum of R-modules.

Lemma 6.0.16. *Let R be a ring and $I \subseteq R$ be an ideal. Suppose that R is noetherian. Then the ring $R^\#$ associated with R and I is also noetherian.*

Proof. Let $r_1, \ldots, r_k \in I$ be generators of I (which exists as R is noetherian). There is a homomorphism of rings $\phi : R[x_1, \ldots, x_k] \to R^\#$ by $P(x_1, \ldots, x_k) \mapsto P(r_1, \ldots, r_k)$ where $r_1, \ldots, r_k$ are viewed as elements of degree 1 in $R^\#$ and the coefficients of the polynomial are viewed as elements of degree 0, such that ϕ is a homomorphism of R-algebras.

By construction, ϕ is surjective, thus $R^\#$ is surjective, thus finitely generated R-algebra, thus noetherian by Hilbert basis and Lemma 3.6.4. □

Lemma 6.0.17. *Let R be a ring. Let $I \subseteq R$ be an ideal. Let $M_\bullet$ be an I-filtration on M. Suppose that M_j is finitely generated as an R-module for all $j \geq 0$. Let $R^\#$ be the corresponding graded ring and $M^\#$ be the corresponding graded $R^\#$ module. The following are equivalent*

1. *The $R^\#$ module $M^\#$ is fintiely generated*

2. *The filtration $M_\bullet$ is stable*

Proof. Let $n \geq 0$ and consider the graded subgroup

$$M^{\#}_{(n)} = (\bigoplus_{j=0}^{n} M_j) \bigoplus (\bigoplus_{k=1}^{\infty} I^k M_n)$$

of $M^{\#}$ (where the left side is the n-head of $M^{\#}$ and the right is the subgroup tails of M_{n+k}). Note that each $M^{\#}_{(n)}$ is a $R^{\#}$-submodule of $M^{\#}$ by construction. Also, each M_j with $j \in \{0, \ldots, n\}$ is finitely generated as an R-module by assumption, and thus $M^{\#}_{(n)}$ is finitely generated as an $R^{\#}$-module (generated by $\bigoplus_{j=0}^{n} M_j$). We also have the inclusions

$$M^{\#}_{(0)} \subseteq M^{\#}_{(1)} \subseteq M^{\#}_{(2)} \subseteq \cdots$$

and $M^{\#} = \bigcup_{i=0}^{\infty} M^{\#}_{(i)}$.

Also, saying that the I-filtration $M_{\bullet}$ is stable is equivalent to saying that $M^{\#}_{(n_0+k)} = M^{\#}_{(n_0)}$ for all $k \geq 0$ and some $n_0 \geq 0$. We claim this is the case if and only if $M^{\#}$ is finitely generated as an $R^{\#}$ module.

If $M^{\#}$ is finitely generated as an $R^{\#}$-module, then as there exists some n_0 such that $M^{\#}_{(n_0)}$ contains all generators, the proof follows. On the other hand, if $M^{\#}_{(n_0+k)} = M^{\#}_{(n_0)}$ for all $k \geq 0$, then $M^{\#} = M^{\#}_{(n_0)}$, which we know is finitely generated. □

Proposition 6.0.18 (Artin-Rees Lemma)**.** *Let R be a noetherian ring. Let $I \subseteq R$ be an ideal. Let M be a finitely generated R-module and let $M_{\bullet}$ be a stable I-filtration on M. Let $N \subseteq M$ be a submodule. Then the filtration $N \cap M_{\bullet}$ is a stable I-filtration of N.*

Proof. By construction, there is a natural inclusion of $R^{\#}$-modules $N^{\#} \subseteq M^{\#}$. By Lemma 6.0.17, the $R^{\#}$ module is finitely generated. By Lemma 3.6.6, noting $R^{\#}$ is noetherian by Lemma 6.0.16, submodules of finitely generated modules are finitely generated, thus $N^{\#}$ is finitely generated. Thus the filtration $N \cap M_{\bullet} = N_{\bullet}$ is a stable I-filtration of N. □

Corollary 6.0.19. *Let R be a noetherian ring. Let $I \subseteq R$ be an ideal and let M be a finitely generated R-module. Let $N \subseteq M$ be a submodule. Then, there is a natural number $n_0 \geq 0$ such that*

$$I^n(I^{n_0}M \cap N) = I^{n_0+n}M \cap N$$

for all $n \geq 0$.

Proof. Apply Artin-Rees to the filtration $I^{\bullet}M = \bigoplus_{i \geq 0} I^i M$ of M. □

Corollary 6.0.20 (Krull's Theorem)**.** *Let R be a noetherian ring. Let $I \subseteq R$ be an ideal and let M be a finitely generated R-module. Then,*

$$\bigcap_{n \geq 0} I^n M = \bigcup_{r \in 1+I} \ker([r])$$

where $[r] : M \to M$ is defined by $m \mapsto r \cdot m$.

Proof. Let $N = \bigcap_{n \geq 0} I^n M$. By Corollary 6.0.19, there is a natural number $n_0 \geq 0$ such that

$$I(I^{n_0}M \cap N) = IN = I^{n_0+1}M \cap N = N$$

By using the general form of Nakayama's Lemma, there exists some $r \in 1+I$ such that $rN = 0$. Hence $N = \bigcap_{n\geq 0} I^n M \subseteq \bigcup_{r \in 1+I} \ker(r_M)$.

On the other hand, if $r \in 1+I$, $y \in M$ and $ry = 0$, $(1+a)y = y + ay = 0$ for some $a \in I$, thus $y \in IM$. By the same logic, $y \in I^2M$ and so on, giving $y \in N$. □

Corollary 6.0.21 (of Krull's Theorem)**.** *Let R be a noetherian domain. Let I be a proper ideal of R. Then $\bigcap_{n\geq 0} I^n = 0$.*

Proof. Apply Krull's Theorem with $M = R$ and notice that for a nonzero r, $[r]$ always has 0 kernel in a domain. Clearly $0 \notin 1+I$ as I is proper. □

Corollary 6.0.22 (of Krull's Theorem)**.** *Let R be a noetherian ring and I be an ideal of R. Let M be a finitely generated R-module. Suppose that I is contained in the Jacobson radical of R. Then $\bigcap_{n\geq 0} I^n M = 0$.*

Proof. If $r \in 1+I$, then r is a unit. Else, r is contained in some maximal ideal $\mathfrak{m}$. As I is contained in the Jacobson radical of R, it is contained in $\mathfrak{m}$. But now 1 is contained in $\mathfrak{m}$, a contradiction. Thus $\ker(r_M) = 0$, and the result follows by Krull's Theorem. □

The final corollary is especially useful when R is local, as then any proper ideal I is always contained in the Jacobson radical.

Definition 6.0.23. *We say that a ring is **Artinian** if whenever we have a descending sequence of ideals*

$$I_1 \supseteq I_2 \supseteq I_3 \supseteq \cdots$$

in R, then there exists an $n \geq 1$ such that $I_{n+k} = I_n$ for all $k \geq 0$. Then, we say that the sequence $I_\bullet$ stabilises.

Lemma 6.0.24. *Let R be a noetherian local ring with maximal ideal $\mathfrak{m}$. The following are equivalent*

1. $\dim(R) = 0$
2. $\mathfrak{m}$ *is the nilradical of R*
3. $\mathfrak{m}^n = 0$ *for some $n \geq 1$*
4. *R is Artinian*

Proof. $(i) \implies (ii)$ If $\dim(R) = 0$, then every prime ideal of R coincides with $\mathfrak{m}$. Thus $\mathfrak{m}$ is the nilradical of R.

$(ii) \implies (iii)$ Is a consequence of Lemma 3.6.7.

$(iii) \implies (iv)$ Let $I_1 \supseteq I_2 \supseteq \cdots$ be a descending chain of ideals in R. Let $k \geq 0$ be the minimal natural number such that the sequence

$$\mathfrak{m}^k I_1 \supseteq m^k I_2 \supseteq \cdots$$

stabilises. Note that such k exists as $\mathfrak{m}^k = 0$ for some $k \geq 0$. Suppose for a contradiction that $k > 0$. Let $n_0 \geq 1$ be such that $\mathfrak{m}^k I_n = \mathfrak{m}^k I_{n_0}$ for all $n \geq n_0$. Consider the descending sequence

$$\mathfrak{m}^{k-1} I_1 \supseteq \mathfrak{m}^{k-1} I_2 \supseteq \cdots$$

By construction, $\mathfrak{m}^{k-1} I_n \supseteq \mathfrak{m}^k I_{n_0}$ for all $n \geq 1$. Thus, we have the natural inclusions

$$\mathfrak{m}^{k-1} I_1 / \mathfrak{m}^k I_{n_0} \supseteq m^{k-1} I_2 / \mathfrak{m}^k I_{n_0} \supseteq \cdots$$

and for $n \geq n_0$, $\mathfrak{m}(\mathfrak{m}^{k-1}I_n/\mathfrak{m}^k I_{n_0}) = 0$. Thus $(\mathfrak{m}^{k-1}I_n/\mathfrak{m}^k I_{n_0})$ has a natural structure of a $R/\mathfrak{m}$-module if $n \geq n_0$. In particular,

$$\mathfrak{m}^{k-1}I_{n_0}/\mathfrak{m}^k I_{n_0} \supseteq m^{k-1}I_{n_0+1}/\mathfrak{m}^k I_{n_0} \supseteq \cdots$$

is a decreasing sequence of $R/\mathfrak{m}$-modules. These modules (ideals) are finitely generated as R is a noetherian ring.

As $R/\mathfrak{m}$ is a field, we therefore have a descreasing sequence of finite dimensional vector spaces, which must stabilise. Let $n_1 \geq n_0$ be such that

$$\mathfrak{m}^{k-1}I_n/\mathfrak{m}^k I_{n_0} = m^{k-1}I_{n_1}/\mathfrak{m}^k I_{n_0}$$

for all $n \geq n_1$. Then, $\mathfrak{m}^{k-1}I_{n_1} = \mathfrak{m}^{k-1}I_n$. In particular, the sequence $\mathfrak{m}^{k-1}I_n$ also stabilises. This contradicts the minimality of k, thus $k = 0$.

$(iv) \implies (i)$ Suppose that R is Artinian but $\dim(R) \neq 0$. In particular, we can find a prime ideal $\mathfrak{p}$ such that $\mathfrak{p} \subsetneq \mathfrak{m}$. Then $\mathfrak{m}$ is not the nilradical of R as it is contained in $\mathfrak{p}$.

As R is Artinian, we know there is a natural number $n_0 \geq 0$ such that $\mathfrak{m}^{n_0} = \bigcap_{i=0}^{\infty} \mathfrak{m}^i$. By Corollary 6.0.22, this equals 0. In particular, $\mathfrak{m}$ is the nilradical of R, a contradiction. □

Theorem 6.0.25 (Krull's principal ideal theorem)**.** *Let R be a noetherian ring. Let $f \in R$ be an element which is not a unit. Let $\mathfrak{p}$ be minimal among the prime ideals containing f. Then* $\mathrm{ht}(\mathfrak{p}) \leq 1$.

Proof. Note that the maximal ideal of $R_{\mathfrak{p}}$ is minimal among the prime ideals of $R_{\mathfrak{p}}$ containing $f/1 \in R_{\mathfrak{p}}$ (by bijective correspondence). Furthermore, the height of $\mathfrak{p}$ is the same as the height of the maximal ideal of $R_{\mathfrak{p}}$. As $R_{\mathfrak{p}}$ is also noetherian, we may suppose that R is local and that $\mathfrak{p}$ is a maximal ideal.

Now let $\mathfrak{p} \supsetneq \mathfrak{p}_1 \supsetneq \mathfrak{p}_2 \supsetneq \cdots \supsetneq \mathfrak{p}_{k_0}$ be a chain ideals starting with $\mathfrak{p}$. We wish to show that $k_0 \leq 1$. We may suppose that $k_0 > 0$ as else there is nothing to prove.

Write $\mathfrak{q} = \mathfrak{p}_1$. By assumption, $f \notin \mathfrak{q}$. Write $\lambda : R \to R_{\mathfrak{q}}$ for the natural map. For $n \geq 1$, write $\overline{\lambda(\mathfrak{q}^n)}$ for the ideal of $R_{\mathfrak{q}}$ generated by $\lambda(\mathfrak{q}^n)$. We know that $\overline{\lambda(\mathfrak{q}^n)}$ consists of elements of the form r/t where $r \in \mathfrak{q}^n$ and $t \in R \backslash \mathfrak{q}$. Note also the identity $\overline{\lambda(\mathfrak{q}^n)} = \overline{\lambda(\mathfrak{q})}^n$.

Now consider the ideal $I_n = \lambda^{-1}(\overline{\lambda(\mathfrak{q}^n)})$. By construction, we have $I_n \supseteq \mathfrak{q}^n$. Also, by bijective correspondence, $I_1 = \mathfrak{q}$. Note the difference in property is that if $fr \in I_n$ for any $r \in R$, then $r \in I_n$ as $\lambda(fr)(1/f) = \lambda(r) \in \overline{\lambda(\mathfrak{q}^n)}$. Consider the ring $R/(f)$. This is local as R is local. It is a quotient ring of a noetherian ring, so it is also noetherian. The ring $R/(f)$ has dimension 0 as the maximal ideal ($\mathfrak{p}$ mod (f)) is a minimal prime ideal of $R/(f)$ by construction. We now have a descending sequence of ideals $I_1 \supseteq I_2 \supseteq \cdots$. By Lemma 6.0.24, the image of this sequence in $R/(f)$ must stabilise. Thus, there is some $n_0 \geq 1$ such that for any $n \geq n_0$, $I_n \subseteq I_{n+1} + (f)$. Also, if $r \in I_n$, for any $t \in I_{n+1}$ and $h \in R$ such that $r = t + hf$, as $r - t \in I_n$, and $hf \in I_n$ so $h \in I_n$, shows that $I_n \subseteq I_{n+1} + (f)I_n \subseteq I_{n+1} + \mathfrak{p}I_n$. In particular, the natural map $I_{n+1}/\mathfrak{p}I_{n+1} \to I_n/\mathfrak{p}I_n$ is surjective. By Corollary 3.3.5, $I_{n+1} \to I_n$ is surjective, so $I_{n+1} = I_n$. Thus the sequence I_n stabilises at n_0.

Now noting that $I_n \supseteq q^n$ and $\overline{\lambda(I_n)} = \overline{\lambda(\mathfrak{q})}^n = \overline{\lambda(\mathfrak{q})}^n$, we have the descending sequence of ideals of $R_{\mathfrak{q}}$

$$\overline{\lambda(\mathfrak{q})} \supseteq (\overline{\lambda(\mathfrak{q})})^2 \supseteq (\overline{\lambda(\mathfrak{q})})^3 \supseteq \cdots$$

also stabilises at n_0. Now, by Corollary 6.0.22, $\bigcap_{i \geq 0} (\overline{\lambda(\mathfrak{q})})^i = 0$. Thus, we have $\overline{\lambda(\mathfrak{q})}^{n_0}$. Now, as $\lambda(\mathfrak{q})$ is the maximal ideal of R_q, by Lemma 6.0.24, $R_{\mathfrak{q}}$ has dimension 0. In particular, $\mathrm{ht}(\mathfrak{q}) = 0$. Thus q cannot contain any prime ideal other than itself. This gives $k = 1$.

□

Lemma 6.0.26. *Let R be a noetherian ring. Let $\mathfrak{p}$ and $\mathfrak{p}'$ be prime ideals of R and suppose that $\mathfrak{p} \subsetneq \mathfrak{p}'$. Then, there exists a prime ideal $\mathfrak{q}$ such that $\mathfrak{p} \subseteq \mathfrak{q} \subsetneq \mathfrak{p}'$ and $\mathfrak{q}$ is maximal among prime ideals with such property.*

Proof. Suppose not. Let $\mathfrak{q}_1$ be any prime that satisfies the inequality. Then, we can continuously find larger primes from this which are strictly smaller than $\mathfrak{p}$. This contradicts the Noetherian condition on R. □

Corollary 6.0.27. *Let R be a noetherian ring. Let $f_1, \dots, f_k \in R$. Let $\mathfrak{p}$ be a prime ideal minimal among those containing $(f_1, \dots, f_k)$. Then* $\operatorname{ht}(\mathfrak{p}) \leq k$.

Proof. By induction on k. The case $k = 1$ is Krull's principal ideal theorem. Using a similar logic to the start of Krull's principal ideal theorem (by localising at $\mathfrak{p}$), we may suppose that R is a local ring with maximal ideal $\mathfrak{p}$.

Let $\mathfrak{p} \supsetneq \mathfrak{p}_1 \supsetneq \mathfrak{p}_2 \supsetneq \cdots$ be a possibly infinite chain of prime ideals beginning with $\mathfrak{p}$ and of length $\operatorname{ht}(\mathfrak{p})$. We can also assume that there are no prime ideals between $\mathfrak{p}$ and $\mathfrak{p}_1$, extending the chain by such prime ideal if necessary. Also note this condition is automatic if $\operatorname{ht}(\mathfrak{p}) < \infty$.

We wish to show that $\operatorname{ht}(\mathfrak{p}) \leq k$. Suppose that $\operatorname{ht}(\mathfrak{p}) > 0$ as else there is nothing to prove. Let $\mathfrak{q} = \mathfrak{p}_1$. We claim that $\operatorname{ht}(\mathfrak{q}) \leq k - 1$.

From assumptions, there is an f_i such that $f_i \neq \mathfrak{q}$, as else $\mathfrak{p}$ is not the minimal prime. Up to reordering, assume $f_1 \neq \mathfrak{p}$. As there are no prime ideals between $\mathfrak{p}$ and $\mathfrak{q}$, we see that $\mathfrak{p}$ is minimal among prime ideals containing $(\mathfrak{q}, f_1)$. Hence, the ring $R/(\mathfrak{q}, f_1)$ has dimension 0. Thus, by Lemma 6.0.24, the image of all f_i are nilpotent in $R/(\mathfrak{q}, f_1)$. That is, there exists $b_i \in \mathfrak{q}$ and $a_i \in R$ with $n_i \geq 2$ such that

$$f_i^{n_i} = a_i f_1 + b_i$$

Note also that

$$\mathfrak{p} \supseteq (f_1, f_2^{n_2}, \dots, f_k^{n_k}) = (f_1, b_2, \dots, b_k)$$

and that $\mathfrak{p}$ is minimal among the prime ideals containing $f_1, b_2, \dots, b_k$ since

$$\mathfrak{r}((f_1, f_2^{n_2}, \dots, f_k^{n_k})) = \mathfrak{r}((f_1, f_2, \dots, f_k))$$

by definition. Write $J = (b_2, \dots, b_k)$. Note first that $J \subseteq \mathfrak{q}$. Since $\mathfrak{p}$ is minimal among the prime ideals containing f_1 and J, we see that $\mathfrak{p} \bmod J$ is minimal among the prime ideals of R/J containing $f_1 \bmod J$. Hence, $\operatorname{ht}(\mathfrak{p} \bmod J) \leq 1$ by Krull's principal ideal theorem. On the other hand, we have

$$\mathfrak{p} \bmod J \supsetneq \mathfrak{q} \bmod J$$

In particular, $\operatorname{ht}(\mathfrak{q} \bmod J) = 0$. Thus $\mathfrak{q}$ is minimal among the prime ideals containing J. By the inductive hypothesis, $\operatorname{ht}(\mathfrak{q}) \leq k - 1$. This completes the proof. □

Remark 6.0.28. As any ideal is generated by finitely many elements, any prime ideal has finite height. Thus, the dimension of a noetherian local ring is finite.

Note that this is not true if we take the local assumption away. TODO: example??

The above also implies that $\operatorname{ht}((f_1, \dots, f_k)) \leq k$. If we have equality, then any minimal prime ideal associated with $(f_1, \dots, f_k)$ has any height k (as height $\geq k$ by assumption, and $\leq k$ by proof).

Corollary 6.0.29. *Let R be a noetherian ring. Let $\mathfrak{p}_0 \supseteq \mathfrak{p}_1 \supseteq \mathfrak{p}_2 \supseteq \cdots$ be a descending chain of prime ideals of R. Then there is a $i_0 \geq 0$ such that $\mathfrak{p}_{i_0+i} = \mathfrak{p}_{i_0}$ for all $i \geq 0$. Moreover, if $\mathfrak{p}_0$ is generated by c elements, and the inequality is strict until it stabilises, then $i_0 \leq c$.*

Proof. Is a direct consequence of Corollary 6.0.27. □

Corollary 6.0.30. *Let R be a noetherian ring. Let $\mathfrak{p}$ be a prime ideal of height c. Suppose that $0 \leq k \leq c$ and that we have elements $t_1, \ldots, t_k \in \mathfrak{p}$ such that $\mathrm{ht}((t_1, \ldots, t_k)) = k$. Then there are elements $t_{k+1}, \ldots, t_c \in \mathfrak{p}$ such that $\mathrm{ht}(t_1, \ldots, t_c) = c$.*

Proof. Note that by assumption, we have $k \leq c$. Note we set the ideal to 0 if $k = 0$. Also, if $\mathrm{ht}(t_1, \ldots, t_c) = c$, then $\mathfrak{p}$ is a minimal prime ideal associated with the ideal $(t_1, \ldots, t_c)$.

If $c = 0$, then $\mathfrak{p}$ is a minimal prime ideal of R, and $\mathrm{ht}((0)) = c = 0$, so we are done. We proceed by induction. Suppose that $c > 0$. We can also take $k < c$.

By induction on k, it is sufficient to construct an element $t \in \mathfrak{p}$ such that $\mathrm{ht}((t_1, \ldots, t_k, t)) = k+1$. By Corollary 6.0.27 we know the height of this is at most k, so it suffices to find a $t \in \mathfrak{p}$ such that $\mathrm{ht}((t_1, \ldots, t_k, t)) > k$.

Suppose for a contradiction such an element does not exist. Then, we have $\mathrm{ht}((t_1, \ldots, t_k, t)) = k$ for all $t \in \mathfrak{p}$. Specifically, for any $t \in \mathfrak{p}$, there is a prime ideal $\mathfrak{q}$ that contains $(t_1, \ldots, t_k, t)$ and is of height k. Now $\mathfrak{q}$ contains a minimal prime q_1 associated with $(t_1, \ldots, t_k)$ with height k. Note that the height of this it at least k, giving $\mathfrak{q} = \mathfrak{q}_1$. Thus, for all $t \in \mathfrak{p}$, t is contained in a minimal prime ideal of height k associated with $(t_1, \ldots, t_k)$. Consequently, $\mathfrak{p}$ is contained in the union of minimal prime ideals of height k associated with $(t_1, \ldots, t_k)$. Thus $\mathfrak{p}$ is contained in, thus equal to one of these minimal prime ideals. As $\mathrm{ht}(\mathfrak{p}) = c > k$, this contradicts Corollary 6.0.27. □

Lemma 6.0.31. *Let K be a field and let $\mathfrak{p}$ be a non-zero prime ideal of $K[x]$. Then $\mathrm{ht}(\mathfrak{p}) = 1$. In particular, $\dim(K[x]) = 1$.*

Proof. Note that in $K[x]$, non-zero prime ideals are maximal. As the zero-ideal is prime (noting that $K[x]$ is a domain), we must have that the dimension of any non-zero ideal is 1. □

Definition 6.0.32. *Let R be a ring and $\mathfrak{p}$ is an ideal of R, we write $\mathfrak{p}[x]$ for the ideal generated by $\mathfrak{p}$ in $R[x]$. We can note this consists of polynomials with coefficients in $\mathfrak{p}$. If the ideal $\mathfrak{p}$ is prime, so is $\mathfrak{p}[x]$, as*

$$R[x]/\mathfrak{p}[x] \simeq (R/\mathfrak{p})[x]$$

and $(R/\mathfrak{p})[x]$ is a domain, noting that $R/\mathfrak{p}$ is a domain.

Lemma 6.0.33. *Let $\phi : R \to T$ be a ring homomorphism. Let $\mathfrak{p} \in \mathrm{Spec}(R)$ and let I be the ideal generated by $\phi(\mathfrak{p})$ in T. Write $\psi : R/\mathfrak{p} \to T/I$ be the ring homomorphism induced by ϕ, and let $S = (R/\mathfrak{p})\backslash\{0\}$.*

Write $\psi_S : \mathrm{Frac}(R/\mathfrak{p}) \to (T/I)_{\psi(S)}$ for the induced ring homomorphism. Let $\rho : T \to (T/I)_{\psi(T/I)_{\psi(S)}}$ Then, $\mathrm{Spec}(\rho)(\mathrm{Spec}((T/I)_{\psi(S)}))$ consists precisely of the prime ideals $\mathfrak{q}$ of T such that $\phi^{-1}(\mathfrak{q}) = \mathfrak{p}$.

Proof. We have the following commutative diagram of rings.

$$\begin{tikzcd}
T \arrow[r] \arrow[rr, bend left, "\rho"] & T/I \arrow[r] & (T/I)_{\psi(S)} \\
R \arrow[r] \arrow[u, "\phi"] & R/\mathfrak{p} \arrow[r] \arrow[u, "\psi"] & \mathrm{Frac}(R/\mathfrak{p}) \arrow[u, "\psi_S"']
\end{tikzcd}$$

This leads to a commutative diagram of spectra,

$$\begin{tikzcd}
\mathrm{Spec}(T) \arrow[d, "\mathrm{Spec}(\phi)"'] & \mathrm{Spec}(T/I) \arrow[l] \arrow[d, "\mathrm{Spec}(\psi)"'] & \mathrm{Spec}((T/I)_{\psi(S)}) \arrow[l] \arrow[d, "\mathrm{Spec}(\psi_S)"] \arrow[ll, bend right, "\mathrm{Spec}(\rho)"'] \\
\mathrm{Spec}(R) & \mathrm{Spec}(R/\mathfrak{p}) \arrow[l] & \mathrm{Spec}(\mathrm{Frac}(R/\mathfrak{p})) \arrow[l]
\end{tikzcd}$$

Thus, we wish to show that the fibre of $\mathrm{Spec}(\phi)$ above $\mathfrak{p}$ is the image of $\mathrm{Spec}(\rho)$: TODO!! WHAT????

Note first that $\mathrm{Spec}(\mathrm{Frac}(R/\mathfrak{p}))$ consists of one point as it is a field. The image of this point in $\mathrm{Spec}(R/\mathfrak{p})$ is the ideal $(0) \subseteq R/\mathfrak{p}$, and the preimage of this in R is $\mathfrak{p}$. So the image of $\mathrm{Spec}(\rho)$ is contained in the fibre of $\mathrm{Spec}(\phi)$ above $\mathfrak{p}$, noting the diagram is commutative.

Now suppose that $\mathfrak{q} \in \mathrm{Spec}(T)$ with $\phi^{-1}(\mathfrak{q}) = \mathfrak{p}$ ($\mathfrak{q}$ lies inside the fibre of $\mathrm{Spec}(\phi)$ above $\mathfrak{p}$). Then, $\mathfrak{q} \supseteq I$, so there is an ideal $q' \in \mathrm{Spec}(T/I)$ such that $\mathfrak{q}$ is the image of $\mathfrak{q}'$ in $\mathrm{Spec}(T)$. On the other hand, we know that $\psi^{-1}(\mathfrak{q}')$ is the 0 ideal, as $\phi^{-1}(\mathfrak{q}) = \mathfrak{p}$ and the diagram is commutative. Thus, $\mathfrak{q}' \cap \psi(S) = \emptyset$. Consequently, by Lemma 2.1.18, $\mathfrak{q}'$ lies in the image of $\mathrm{Spec}((T/I)_{\psi(S)}) \to \mathrm{Spec}(T/I)$. This completes the proof.

□

Remark 6.0.34. Note that with the correspondence between

- prime ideals $\mathfrak{q}$ such that $\phi^{-1}(\mathfrak{q}) = \mathfrak{p}$
- prime ideals of $(T/I)_{\psi(S)}$

given above, as this is given by $\mathrm{Spec}(\rho)$, respects inclusion in both directions.

Applying the previous lemma with $T = R[x]$, we have

$$(T/I)_{\psi(S)} = (R[x]/\mathfrak{p}[x])_{\psi}(S) \simeq (R/\mathfrak{p})[x]_{(R/\mathfrak{p})^*} \simeq \mathrm{Frac}(R/\mathfrak{p})[x]$$

Note the $A^* = A \backslash \{0\}$ gives the multiplicative structure, noting $R/\mathfrak{p}$ is a domain. Note the final equality comes from the fact

$$(A[x])_S = (A_S)[x]$$

given A is a domain (by considering the map $\sum a_i x^i / s \mapsto \sum (a_i/s) x^i$).

Lemma 6.0.35. *We keep the notation of Lemma 6.0.33. Suppose we have the chain of prime ideals*

$$\mathfrak{q}_0 \supseteq \mathfrak{q}_1 \supseteq \cdots \supsetneq \mathfrak{q}_k$$

in T such that $\phi^{-1}(q_i) = \mathfrak{p}$ for all $i \in \{0, \ldots, k\}$. Then, $k \leq \dim((T/I)_{\psi(S)})$.

Proof. By Lemma 6.0.33 and noting that the bijective correspondence respects inclusion. □

Lemma 6.0.36. *Let R be a ring and let N be the nilradical of R. Then the nilradical of $R[x]$ is $N[x]$.*

Proof. Any element of $N[x]$ is a polynomial with nilpotent coefficients and thus is nilpotent (as the nilradical is an ideal, closed under adding nilpotent elements). Suppose $P(x) = a_0 + a_1 x + \cdots + a_d x^d$ is an element of the nilradical of $R[x]$. Suppose for a contradiction that a_i is not nilpotent. Let $\mathfrak{p} \in \mathrm{Spec}(R)$ be such that $a_i \notin \mathfrak{p}$ (exists, as a_i is not nilpotent). Then $P(x) \bmod \mathfrak{p} \in (R/\mathfrak{p})[x]$ is a non zero nilpotent polynomial. This is a contradiction as $(R/\mathfrak{p})[x]$ is a domain. □

Lemma 6.0.37. *Let R be a noetherian ring and let $\mathfrak{p}_1, \dots, \mathfrak{p}_k$ be the minimal prime ideals of R. Then the minimal prime ideals of $R[x]$ are the ideals $\mathfrak{p}_1[x], \dots, \mathfrak{p}_k[x]$. More generally, if I is an ideal of R and $\mathfrak{p}_1, \dots, \mathfrak{p}_k$ are minimal prime ideals associated with I, then the ideals $\mathfrak{p}_1[x], \dots, \mathfrak{p}_k[x]$ are the minimal primes associated with $I[x]$.*

Proof. For the first, note that $\bigcap_i \mathfrak{p}_i = \mathfrak{r}((0))$, because the nilradical of R is decomposable by the Lasker-Noether Theorem. Consequently, $\mathfrak{r}((0))[x] = (\bigcap_i p_i)[x] = \bigcap_i p_i[x]$ is a minimal primary decomposition of $\mathfrak{r}((0))[x]$ by Proposition 3.5.2. By Lemma 6.0.36, this is the nilradical of $R[x]$ and correspond to the minimal primes by Theorem 3.5.14 and correspondence.

For the second statement, apply the first to p_i mod I, noting that $(R/I)[x] \simeq R[x]/I[x]$. □

Lemma 6.0.38. *Let R be noetherian and let I be an ideal of R. Then* $\operatorname{ht}(I) = \operatorname{ht}(I[x])$*.*

Proof. We first prove the case if I is prime, writing $I = \mathfrak{p} \in \operatorname{Spec}(R)$. Let $c = \operatorname{ht}(\mathfrak{p})$ and let $a_1, \dots, a_c \in \mathfrak{p}$ be such that $\operatorname{ht}((a_1, \dots, a_c)) = c$, such that $\mathfrak{p}$ is a minimal prime associated with $(a_1, \dots, a_c)$. This exists by Corollary 6.0.30. Let $J = (a_1, \dots, a_c)$. By the previous lemma, $\mathfrak{p}[x]$ is a minimal prime ideal associated with $J[x]$. By Corollary 6.0.27, $\operatorname{ht}(\mathfrak{p}[x]) \leq c$ (as $a_1, \dots, a_c$ generate $J[x]$). Also, if

$$\mathfrak{p} \supsetneq \mathfrak{p}_1 \supsetneq \mathfrak{p}_2 \supsetneq \cdots \supsetneq p_c$$

then,

$$\mathfrak{p}[x] \supsetneq \mathfrak{p}_1[x] \supsetneq \mathfrak{p}_2[x] \supsetneq \cdots \supsetneq p_c[x]$$

is also a descending chain of prime ideals in $R[x]$, so $\operatorname{ht}(\mathfrak{p}[x]) \geq c$. Thus we have shown equality.

For the general case, note that there is a minimal prime $\mathfrak{p}$ associated with I such that $\operatorname{ht}(\mathfrak{p}) = \operatorname{ht}(I)$. Thus, $\operatorname{ht}(I[x]) \leq \operatorname{ht}(\mathfrak{p}[x]) = \operatorname{ht}(\mathfrak{p}) = \operatorname{ht}(I)$. On the other hand, there is a minimal prime ideal associated with $I[x]$ such that $\operatorname{ht}(\mathfrak{q}) = \operatorname{ht}(I[x])$. By Lemma 6.0.37, we have $\mathfrak{q} = (\mathfrak{q} \cap R)[x]$, so

$$\operatorname{ht}(I[x]) = \operatorname{ht}(\mathfrak{q}) = \operatorname{ht}((\mathfrak{q} \cap R)[x]) = \operatorname{ht}(\mathfrak{q} \cap R) \geq \operatorname{ht}(I[x] \cap R) = \operatorname{ht}(I)$$

□

Lemma 6.0.39. *Let $\mathfrak{q}$ be a prime ideal of $R[x]$ and let I be an ideal of R such that $I \subseteq \mathfrak{q} \cap R$. Suppose that $\mathfrak{q} \cap R$ is a minimal prime ideal associated with I. Let $\mathfrak{q}' \subseteq \mathfrak{q}$ be a prime ideal of $R[x]$ which is a minimal prime ideal associated with $I[x]$. Then $\mathfrak{q}' = (\mathfrak{q} \cap R)[x]$.*

Proof. We have,

$$\mathfrak{q}' \cap R \supseteq I[x] \cap R = I$$

and note with this that,

$$\mathfrak{q}' \supseteq (\mathfrak{q}' \cap R)[x] \supseteq I[x]$$

By minimality of $\mathfrak{q}'$, we have $\mathfrak{q}' = (\mathfrak{q}' \cap R)[x]$. Now, $\mathfrak{q}' \subseteq \mathfrak{q}$, so

$$\mathfrak{q}' = (\mathfrak{q}' \cap R)[x] \subseteq (\mathfrak{q} \cap R)[x]$$

By Lemma 6.0.37, we know that $(\mathfrak{q} \cap R)[x]$ is a minimal prime associated with $I[x]$, thus $\mathfrak{q}' = (\mathfrak{q} \cap R)[x]$. □

Proposition 6.0.40. *Let R be a noetherian ring and $\mathfrak{p}$ be a prime ideal of $R[x]$. Then,*

$$\operatorname{ht}(\mathfrak{p}) \leq 1 + \operatorname{ht}(\mathfrak{p} \cap R)$$

If $\mathfrak{p}$ is maximal, we have

$$\operatorname{ht}(\mathfrak{p}) = 1 + \operatorname{ht}(\mathfrak{p} \cap R)$$

Proof. Let $\delta = \text{ht}(\mathfrak{p} \cap R)$ and $c = \text{ht}(\mathfrak{p})$. Note that since $(\mathfrak{p} \cap R)[x] \subseteq \mathfrak{p}$, we have $\delta \leq c$ by Lemma 6.0.38.

Let $a_1, \ldots, a_c \in \mathfrak{p}$ be such that $\text{ht}((a_1, \ldots, a_i)) = i$ for $i \in \{1, \ldots, c\}$. This exists by Corollary 6.0.30. By the same corollary, suppose that $a_1, \ldots, a_\delta \in \mathfrak{p} \cap R$. In particular, $(\mathfrak{p} \cap R)[x]$ is a minimal prime ideal associated with $(a_1, \ldots, a_\delta)$.

Now, inductively define a chain of prime ideals

$$\mathfrak{p} = \mathfrak{q}_0 \supsetneq \mathfrak{q}_1 \supsetneq \cdots \supsetneq \mathfrak{q}_c$$

such that $\mathfrak{q}_i$ is a minimal prime associated with $(a_1, \ldots, a_{c-i})$. To construct this, we first let $\mathfrak{q}_0 = \mathfrak{p}$ and suppose that for $i > 0$, the ideals $\mathfrak{q}_0, \ldots, \mathfrak{q}_{i-1}$ are given. Let $\mathfrak{q}_i$ be any minimal prime ideal associated with $(a_1, \ldots, a_{c-i})$, which is contained in $\mathfrak{q}_{i-1}$. This is strict, as the construction gives $\text{ht}(\mathfrak{q}_i) = c - i$ (Corollary 6.0.27).

Now, $\mathfrak{q}_{c-\delta}$ and $(\mathfrak{p} \cap R)[x]$ are minimal prime ideals associated with $(a_1, \ldots, a_\delta)$. By Lemma 6.0.39, we have equality. Thus, for all $i \in \{0, \ldots, c - \delta\}$ we have

$$\mathfrak{p} \supseteq \mathfrak{q}_i \supseteq (\mathfrak{p} \cap R)[x]$$

So,

$$\mathfrak{p} \cap R \supseteq \mathfrak{q}_i \cap R \supseteq \mathfrak{p} \cap R$$

Giving $\mathfrak{q}_i \cap R = \mathfrak{p} \cap R$.

By Lemma 6.0.35,

$$c - \delta \leq \dim((R[x]/(\mathfrak{p} \cap R)[x])_{(R/(\mathfrak{p} \cap R)^*)}) = \dim(\text{Frac}(R/(\mathfrak{p} \cap R))[x])$$

By Lemma 6.0.31, this has dimension at most 1, so the first claim has been shown.

If $\mathfrak{p}$ is maximal, then $\mathfrak{p} \neq (\mathfrak{p} \cap R)[x] = \mathfrak{q}_{c-\delta}$ as $(\mathfrak{p} \cap R)[x]$ is not maximal (by adding (x)), so $c - \delta \geq 1$. In particular, $c = \delta + 1$. □

Theorem 6.0.41. *Let R be a noetherian ring. Suppose that* $\dim(R) < \infty$. *Then* $\dim(R[x]) = \dim(R) + 1$.

Proof. Let $\mathfrak{m}$ be a maximal ideal of $R[x]$ such that $\text{ht}(\mathfrak{m}) = \dim(R[x])$. This exists as the dimension is finite. By the previous proposition, we have $\text{ht}(\mathfrak{m}) = 1 + \text{ht}(\mathfrak{m} \cap R)$. We now claim that $\text{ht}(\mathfrak{m} \cap R) = \dim(R)$. Suppose for a contradiction that $\text{ht}(\mathfrak{m} \cap R) < \dim(R)$. Then, there is a maximal ideal $\mathfrak{p}$ in R such that $\text{ht}(\mathfrak{p}) > \text{ht}(\mathfrak{m} \cap R)$. Let $\mathfrak{n}$ be a maximal ideal of $R[x]$ which contains $\mathfrak{p}[x]$. By maximality, $\mathfrak{n} \cap R = \mathfrak{p}$, giving

$$\text{ht}(\mathfrak{n}) = 1 + \text{ht}(\mathfrak{p}) > 1 + \text{ht}(\mathfrak{m} \cap R) = \text{ht}(\mathfrak{m})$$

which is a contradiction. Thus, $\text{ht}(\mathfrak{m}) = \dim(R[x]) = \dim(R) + 1$. □

Remark 6.0.42. Let R be a noetherian ring and $\mathfrak{p} \subseteq \mathfrak{q}$ be prime ideals of R. Then, we have

$$\text{ht}(\mathfrak{p}) + \text{ht}(\mathfrak{q} \bmod \mathfrak{p}) \leq \text{ht}(\mathfrak{q})$$

but equality does not hold in general. Rings where this holds are called **catenary** domains. Note further that finitely generated algebras over fields are catenary. So equality holds if R is a domain, as they are always finitely generated over some field. (Both results not shown here)

We note that however $\text{ht}((\mathfrak{m} \cap R)[x]) + \text{ht}(\mathfrak{m}/(\mathfrak{m} \cap R)[x]) = \text{ht}(\mathfrak{m})$.

Corollary 6.0.43. *Let R be a noetherian ring. Suppose that* $\dim(R) < \infty$. *Then we have that* $\dim(R[x_1, \ldots, x_t]) = \dim(R) + t$.

Proof. This follows from Theorem 6.0.41 and Hilbert's basis theorem. □

Lemma 6.0.44. *Let R be a subring of T. Let T be integral over R. Let $\mathfrak{q}_1, \mathfrak{q}_2$ be prime ideals of T such that $\mathfrak{q}_1 \cap R = \mathfrak{q}_2 \cap R = \mathfrak{p}$ for some prime $\mathfrak{p}$ in R. If $\mathfrak{q}_1 \subseteq \mathfrak{q}_2$, $\mathfrak{q}_1 = \mathfrak{q}_2$.*

Proof. The ring $R/\mathfrak{p}$ can be viewed as a subring of $T/\mathfrak{q}_1$ (by considering the map from R into $T/\mathfrak{q}_1$ induced by the quotient map). By assumption, we also have $(\mathfrak{q}_2 \bmod \mathfrak{q}_1) \cap R/\mathfrak{p} = (0)$. Without loss of generality, we may therefore view R and T to be domains and $\mathfrak{q}_1$ and $\mathfrak{p}$ are zero ideals.

Take $e \in \mathfrak{q}_2 \backslash \{0\}$ and let $P(x) \in R[x]$ be a non-zero monic polynomial such that $P(e) = 0$. As T is a domain, the constant coefficient of $P(x)$ is non-zero. But the constant term $P(0)$ is a linear combination of positive powers of e, so $P(0) \in R \cap \mathfrak{q}_2 = (0)$, a contradiction. □

Lemma 6.0.45. *Let R be a subring of T. Suppose that T is integral over R. Then* $\dim(T) = \dim(R)$. *This holds if R or T has infinite dimension (then the other has infinite dimension).*

Proof. Suppose first that $\dim(R), \dim(T) < \infty$. Let

$$\mathfrak{p}_0 \supsetneq \mathfrak{p}_1 \supsetneq \cdots \supsetneq \mathfrak{p}_{\dim(R)}$$

be a descending chain of prime ideals in R of maximal length. By Theorem 4.1.15, we can find a prime ideal $\mathfrak{q}_i$ in T such that $\mathfrak{q}_i \cap R = \mathfrak{p}_i$ and

$$\mathfrak{q}_0 \supsetneq \mathfrak{q}_1 \supsetneq \cdots \supsetneq \mathfrak{q}_{\dim(R)}$$

Hence $\dim(T) \geq \dim(R)$. We have

$$\mathfrak{q}_0 \cap R \supsetneq \mathfrak{q}_1 \cap R \supsetneq \cdots \supsetneq \mathfrak{q}_{\dim(T)} \cap R$$

by Lemma 6.0.44. Thus $\dim(T) \leq \dim(R)$. The proof uses adjacent logic for the infinite case. □

Corollary 6.0.46. *Let k be a field and let R be a finitely generated k-algebra. Suppose that R is a domain and let $K =$* $\mathrm{Frac}(R)$. *Then* $\dim(R)$ *and* $\mathrm{tr}(K|k)$ *are both finite and equal.*

Proof. By Noether's Normalization Lemma, there is an injection of rings $k[x_1, \ldots, x_d] \hookrightarrow R$ which makes R into an integral $k[x_1, \ldots, x_d]$-algebra. From the previous lemma, we have $\dim(R) = \dim(k[x_1, \ldots, x_d]) = d$. Also, the fraction field $k(x_1, \ldots, x_d) = \mathrm{Frac}(k[x_1, \ldots, x_d])$ is naturally a subfield of K, and as every element of R is integral over $k[x_1, \ldots, x_d]$, every element of K is algebraic over $k(x_1, \ldots, x_d)$. Thus,

$$\mathrm{tr}(K|k) = \mathrm{tr}(k(x_1, \ldots, x_d)|k) = d = \dim(R)$$

□

7 Other

TODO: orbit stabiliser, structure theorem for finitely generated abelian groups

Lemma 7.0.1. *A finite commutative group G is cyclic if and only if for any $d|\#G$, there is at most one subgroup in G with cardinality $\#G$.*

Proof. In the infinite case, we use the fact $G \simeq \mathbb{Z}$. □

Lemma 7.0.2. *Let G be a finite cyclic group. Let $k := \#G$. Define $I : (\mathbb{Z}/k\mathbb{Z})^* \to \mathrm{Aut}_{\mathrm{Groups}}(G)$ by $a \mapsto (\gamma \mapsto \gamma^a)$. Then I is an isomorphism.*

Proof. Note first that this is well defined as $\gamma^k = e$ for any $\gamma \in G$. Also,

$$I([a][b])(\gamma) = \gamma^{ab} = I([a])(\gamma^b) = (I([a]) \circ I([b]))(\gamma)$$

thus is a homomorphism.

Take any $\psi \in \mathrm{Aut}_{\mathrm{Groups}}(G)$. If g is the generator for G, $\psi(g) = g^a$ must also be a generator, with $\gcd(a, k) = 1$. In particular, $I([a]) = \psi$, thus I is surjective.

Suppose $I([a])$ is the identity automorphism. In particular, $g^a = g$ for a generator g. As G is cyclic, this forces $a = 1 \bmod k$. In particular, $[a] = [1]$. □

Definition 7.0.3. *A group G is **simple** if it has no nontrivial normal subgroups.*

Definition 7.0.4. *A subgroup G of S_n is called **transitive** if it has only one orbit in $\{1, \dots, n\}$.*

7.1 Solvable Group

Definition 7.1.1. *Let G be a group. A **finite filtration** of G is a finite ascending sequence $G_\bullet$ of subgroups*

$$0 = G_0 \subseteq G_1 \subseteq \cdots \subseteq G_n = G$$

such that G_i is normal in G_{i+1} for all $i \in \{0, \dots, n-1\}$.

*The number n is called the **length** of the finite filtration. The finite filtration $G_\bullet$ is said to have **no redundacies** if $G_i \neq G_{i+1}$ for all $i \in \{0, \dots, n-1\}$. It is said to have **abelian quotients** if the quotient group G_{i+1}/G_i is an abelian group for all $i \in \{0, \dots, n-1\}$.*

*The finite filtration $G_\bullet$ is **trivial** if $n = 1$.*

Note that the trivial filtration always exists and is unique.

Definition 7.1.2. *A group is **solvable** if there exists a finite filtration with abelian quotients on G.*

Lemma 7.1.3 (Solvability via restriction and quotient)**.** *Let G be a group and let H be a subgroup. Then H is solvable. If H is normal in G, then the quotient group G/H is also solvable.*

Proof. Let $G_\bullet$ be a finite filtration with abelian quotients on G. Let n be the length of this filtration. We first claim that $H \cap G_i$ is normal in $H \cap G_{i+1}$. In particular, for any $h \in H \cap G_{i+1}$, the automorphism $\gamma \mapsto h^{-1}\gamma h$ of G_{i+1} sends H into H and G_i into G_i, thus sends $H \cap G_i$ into $H \cap G_i$. In particular,

$$0 = G_0 \cap H \subseteq G_1 \cap H \subseteq \cdots \subseteq G_n \cap H = H$$

is a finite filtration of H. Furthermore, we have an injective map of groups

$$\phi : G_{i+1} \cap H / G_i \cap H \hookrightarrow G_{i+1}/G_i$$

given by $[\gamma]_{G_i \cap H} \mapsto [\gamma]_{G_i}$. Thus this gives a finite filtration with abelian quotients for H. In particular, H is solvable.

Suppose now that H is normal. Consider the ascending sequence of subgroups

$$0 = [G_0]_H \subseteq [G_1]_H \subseteq \cdots \subseteq [G_n]_H = G/H$$

of G/H. Using the fact $[\bullet]_H : G \to G/H$ is a morphism of groups, taking $\gamma \in G_{i+1}$ and $\tau \in G_i$, we have

$$[\gamma]_H^{-1}[\tau]_H[\gamma]_H = [\gamma^{-1}\tau\gamma]_H$$

we have $[\gamma]_H^{-1}[\tau]_H[\gamma]_H \in [G_i]_H$, as $\gamma^{-1}\tau\gamma \in G_i$. In particular, $[G_\bullet]_H$ is a finite filtration of G/H.

Also, we have a surjection of groups

$$\mu : G_{i+1}/G_i \to [G_{i+1}]_H/[G_i]_H$$

such that for any $\gamma \in G_{i+1}$, we have

$$\mu([\gamma]_{G_i}) = [[\gamma]_H]_{[G_i]_H}$$

Noting that we are mapping surjectively from a abelian group, the target is also abelian. In particular $[G_\bullet]_H$ is a finite filtration with abelian quotients for G/H. □

Lemma 7.1.4 (Solvability via inflation). *Let G be a group and $H \subseteq G$ be a normal subgroup. If H is solvable and G/H is solvable, then G is solvable.*

Proof. As H is solvable, we have a finite filtration

$$0 = H_0 \subseteq \cdots \subseteq H_n = H$$

with abelian quotients. Similarly, we G/H is solvable, we have a finite filtration of abelian quotients

$$0 = [G_0]_H \subseteq \cdots \subseteq [G_m]_H = G/H$$

Let $\phi : G \to G/H$ be the standard quotient map. Consider,

$$H = \phi^{-1}([G_0]_H) \subseteq \cdots \subseteq \phi^{-1}([G_m]_H) = G$$

For $i \in \{0, \dots, m-1\}$, $\phi^{-1}([G_i]_H)$ is normal in $\phi^{-1}([G_{i+1}]_H)$. By the third isomorphism theorem, we have

$$\phi^{-1}([G_i]_H)/\phi^{-1}([G_{i+1}]_H) \simeq [G_i]_H/[G_{i+1}]_H$$

Thus by gluing the two finite filtrations,

$$0 = H_0 \subseteq \cdots \subseteq H_n = H = \phi^{-1}([G_0]_H) \subseteq \cdots \subseteq \phi^{-1}([G_m]_H) = G$$

gives a finite filtration of abelian quotients in G. □

Proposition 7.1.5. *Let G be a finite group and let p be a prime number. Suppose there is an $n \geq 0$ such that $\#G = p^n$. Then G is solvable.*

Such groups are called p-groups.

Proof. We proceed by induction on n. For $n = 0$, the proposition clearly holds.

Let $\phi : G \to \mathrm{Aut}_{\mathrm{Groups}}(G)$ be the map of groups such that $\phi(g)(h) = ghg^{-1}$. This gives an action of G on G via conjugation. By the orbit stabiliser theorem, and Lagrange's theorem, the orbits of G in G all have a cardinality a power of p. The orbit of the unit element of G is $\{1_G\}$, and as the orbits partition G, we have $g_0 \in G$ with $g_0 \neq 1_G$ such that g_0 is a fixed point of the action of G on G. Now, $g_0 g = (g g_0 g^{-1})g = g g_0$, so $g?0$ commutes with every element of G. In particular, $g_0 \in Z(G)$ is nontrivial. By definition, $Z(G)$ is abelian thus solvable, and $G/Z(G)$ has cardinality p^k for $k < n$, and thus solvable by the inductive hypothesis. Thus, by Lemma 7.1.4, G is solvable. □

Definition 7.1.6. *The* ***length*** *of a finite group* $\operatorname{length}(G)$ *is*

$$\sup\{n \in \mathbb{N} \mid n \textit{ is the length of a finite filtration with no redundancies of } G\}$$

This is well-defined as the length of a finite group is finite, as it cannot be larger than $\#G$.

Lemma 7.1.7. *Suppose that* G *is a finite solvable group and let* $G_\bullet$ *is a finite filtration with no redundancies of length length*(G) *on* G*. Then for all* $i \in \{0, \ldots, \operatorname{length}(G) - 1\}$*, the group* G_{i+1}/G_i *is a cyclic group of prime order.*

Proof. Let $n := \operatorname{length}(G)$. Suppose there exists an i_0 such that G_{i_0+1}/G_{i_0} is not cyclic of prime order. Then, noting G_{i_0+1}/G_{i_0} is solvable, if it is not abelian, it has some nontrivial proper normal subgroup. If it is abelian but not of prime order, by the structure theorem for finitely generated abelian groups, G_{i_0+1}/G_{i_0} is isomorphic to a finite direct sum of cyclic groups each with order a power of a prime number, giving us a nontrivial subgroup.

Call such a subgroup H. Let $q : G_{i_0+1} \to G_{i_0+1}/G_{i_0}$ be the quotient map. Consider the ascending sequence of subgroups

$$0 = G_0 \subseteq G_1 \subseteq \cdots \subseteq G_{i_0} \subseteq q^{-1}(H) \subseteq G_{i_0+1} \subseteq \cdots \subseteq G_n = G$$

There are no redundancies as H is nontrivial and proper. Note first that $G_{i_0} \triangleleft q^{-1}(H)$ is immediate. We have $q^{-1}(H) \triangleleft G_{i_0+1}$ as it is the kernel of the map

$$G_{i_0+1} \to G_{i_0+1}/G_{i_0} \to (G_{i_0+1}/G_{i_0})/H$$

This gives a longer filtration, contradicting the maximality of n, and in particular every quotient has prime order. □

Remark 7.1.8. If G is a finite group and $G_\#$ is a finite filtration with no redundancies, then we can prove similarly that for the longest sequence, G_{i+1}/G_i is a nonzero simple group (intuitively, if we can pick a nontrivial normal subgroup, we can always extend the sequence).

Example 7.1.9. We note the following facts.

- Abelian groups are solvable (trivially)
- S_3 is solvable. The ascending sequence $0 \subseteq A_3 \subseteq S_3$ is a finite filtration of S_3, with quotients $A_3/0 \simeq \mathbb{Z}/3\mathbb{Z}$ and $S_3/A_3 \simeq \mathbb{Z}/2\mathbb{Z}$.
- The group S_4 is also solvable ($0 \subseteq V_4 \subseteq A_4 \subseteq S_4$).
- A_5 is not solvable, as it is simple but non-abelian. Consequently, any group which contains A_5 as a subgroup is not solvable. In particular, S_n for $n \geq 5$ is not solvable (as $A_5 \leq S_5 \leq S_n$).

8 Properties about Commutative Rings

Definition 8.0.1. *For any ring R, there is a unique ring map (homomorphism) $\phi : \mathbb{Z} \to R$ such that*

$$\phi(n) = \overset{n \text{ times}}{1 + \cdots + 1}$$

Define the ***characteristic*** *written* $\operatorname{char}(R)$ *to be the unique $r \geq 0$ such that* $(r) = \ker(\phi)$

Note that if R is a domain, then $\operatorname{char}(R)$ is either 0 or a prime number.

8.1 Fields

Proposition 8.1.1. *Let R be a domain. Then there is a field F and an injective ring map $\phi : R \to F$ such that if*

$$\phi : R \to F_1$$

is a ring map into a field F_1, then there is a unique ring map $\lambda : F \to F_1$ such that $\phi_1 = \lambda \circ \phi$.

Proof. TODO!! □

Definition 8.1.2. *As a consequence of the above proposition, F is determined uniquely up to isomorphism. We call F the* ***field of fractions****, and write* $\operatorname{Frac}(F)$*.*

Note that $\operatorname{Frac}(R) = R_{R \setminus \{0\}}$

Lemma 8.1.3. *Let K be a field and $I \subseteq K$ be an ideal. Then $I = (0)$ or $I = K$.*

Proof. Immediate (any non-zero element has an inverse, thus generates K). □

Lemma 8.1.4. *Let K, L be fields and $\phi : K \to L$ be a ring map. Then ϕ is injective.*

Proof. Consider the kernel of ϕ. This is an ideal, thus is either (0) or K. In the former ϕ is injective (by the First Isomorphism Theorem), in the latter K and L are both zero-rings, so it follows. □

8.2 Polynomial Rings

Definition 8.2.1. *Let R be a ring. Write $R[x]$ to be the ring of polynomials in the variable x and coefficients in R (with standard operations). If $r \geq 0$ is an integer, $K[x_1, \ldots, x_r] := K$ if $r = 0$ and*

$$K[x_1, \ldots, x_r] := K[x_1][x_2] \ldots [x_r]$$

Given $P(x) = a_d x^d + \cdots + a_1 x + a_0 \in R[x]$ with $a_d \neq 0$, $P(x)$ is ***monic*** *if $a_d = 1$ (and $\deg(0) = -\infty$). We define the* ***degree*** *of $P(x)$ written $\deg(P) := d$.*

An element $t \in R$ is a ***root*** *of $P(x)$ if $P(t) = 0$.*

Lemma 8.2.2. *If R is a domain, then $R[x]$ is also a domain.*

Proof. TODO!!! □

Proposition 8.2.3. *If K is a field, $K[x]$ is a euclidian domain.*

Proof. TODO!! □

Consequently, $K[x]$ is a PID.

Definition 8.2.4. *A **unique factorization domain** (UFD) is a domain R such that for any $r \in R\backslash\{0\}$, there is a sequence $r_1, \ldots, r_k \in R$ such that*

1. *r_i is irreducible for all i*
2. *$(r) = (r_1 \cdots r_k)$*
3. *if $r'_1, \ldots, r'_{k'}$ is another such sequence with the above properties, $k = k'$ and there is a permutation $\sigma \in S_n$ such that $(r_i) = (r'_{\sigma(i)})$ for all $i \in \{1, \ldots, k\}$*

Proposition 8.2.5. *Any PID is a UFD.*

Definition 8.2.6. *Write $\gcd(P_1, \ldots, P_k)$ for the unique monic generator of the ideal $(P_1(x), \ldots, P_k(x))$.*

Lemma 8.2.7. *Suppose that R is a UFD. An element $f \in R\backslash\{0\}$ is irreducible if and only if (f) is a prime ideal.*

Proof. The forward direction is immediate, noting that if $f|p_1p_2$, $f|p_1$ or $f|p_2$, from the fact that f is irreducible and p_1, p_2 can be split into irreducible components.

On the other hand, if (f) is a prime ideal and f is not irreducible, then $f = f_1f_2$ for some non-units. But as f is prime, $f|f_1$ or $f|f_2$. Without loss of generality, taking $f|f_1$, we have $f_1f_2|f_1$, meaning f_2 is a unit, a contradiction. □

Lemma 8.2.8. *Let R be a PID. Let $I \lhd R$ be a nonzero prime ideal. Then I is a maximal ideal.*

Proof. Suppose not. Then we can find an element $r \in R$ such that $r \notin I$ and $([r]_I)$ is not R/I. Also, $([r]_I) = [(r, I)]_I$, and $(r, I) \neq R$ and $I \subsetneq (r, I)$. As we are in a PID, we can find $g, h \in R$ such that $(g) = (r, I)$ and $(h) = I$. Then, $g|h$ but $h \not| g$ (thus h is reducible). But h is irreducible as I is prime and R is a UFD, a contradiction. □

Proposition 8.2.9. *Let K be a field and $f \in K[x], a \in K$. Then,*

1. *a is a root of f if and only if $(x - a)|f$*
2. *there is a polynomial $g \in K[x]$ with no roots and a decomposition*

$$f(x) = g(x) \prod_{i=1}^{k} (x - a_i)^{m_i}$$

where $k \geq 0$ and $m_i \geq 1$ and $a_i \in K$.

Proof. Immediate. For the forward case in (i), we use euclidian division on $(x - a)$ and show the remainder is 0. □

Proposition 8.2.10 (Eisenstein Criterion)**.** *Let*

$$f = x^d + \sum_{i=1}^{d-1} a_i x^k \in \mathbb{Z}[x]$$

Let $p > 0$ be a prime number. Suppose $p|a_i$ and $p^2 \not| a_0$. Then f is irreducible in $\mathbb{Z}[x]$.

Proof. Sketch. The idea is that viewing this polynomial in $\mathbb{F}_p[x]$ gives x^d, and we show that if this is reducible, they are x^n and x^{d-n} in the same field. This contradicts with the assumption $p|a_0$. (Need some algebraic manipulation to show the first statement) □

Lemma 8.2.11. *Let $f \in \mathbb{Z}[x]$ be monic. Let $p > 0$ and $f \pmod p \in \mathbb{F}_p[x]$ is irreducible. Then f is irreducible in $\mathbb{Z}[x]$.*

Proof. TODO!!! □

Lemma 8.2.12 (Gauss Lemma)**.** *Let $f \in \mathbb{Z}[x]$. Then f is irreducible in $\mathbb{Z}[x]$ if and only if it is irreducible in $\mathbb{Q}[x]$.*

Proof. TODO!! □

8.3 Action of Groups on Rings

Definition 8.3.1. *Let S be a set and G be a group. Write $\mathrm{Aut}_{\mathrm{Sets}}(S)$ for the group of bijective maps $a : S \to S$ (where the group operator works by composition). An **action** of G on S is a group homomorphism*

$$\phi : G \to \mathrm{Aut}_{\mathrm{Sets}}(S)$$

Notation 8.3.2. Given $\gamma \in G$ and $s \in S$, we write

$$\gamma(s) := \phi(\gamma)(s)$$

or γs for $\gamma(s)$.

Definition 8.3.3. *The set of invariants of S under the action of G is written*

$$S^G := \{s \in S \mid \gamma(s) = s \ \forall \gamma \in G\}$$

If $s \in S$,

$$\mathrm{Orb}(G, s) := \{\gamma(s) \mid \gamma \in G\}$$

*is the **orbit** of s under G, and*

$$\mathrm{Stab}(G, s) := \{\gamma \in G \mid \gamma(s) = s\}$$

*is the **stabiliser** of s. We omit G when it is clear.*

Definition 8.3.4. *The action of G on a ring R is **compatible** with the ring structure of R, or G acts on a ring R if the image of ϕ lies in the subgroup*

$$\mathrm{Aut}_{\mathrm{Rings}}(R) \subseteq \mathrm{Aut}_{\mathrm{Sets}}(R)$$

where $\mathrm{Aut}_{\mathrm{Rings}}(R)$ is the group of bijective maps $R \to R$ which respects the ring structure.

Intuitively, each group element is mapped to a endomorphism which has some structure.

Lemma 8.3.5. *Let G act on a ring R.*

1. *R^G is a subring of R.*
2. *If R is a field, R^G is a field.*

Proof. The first case is immediate by noting $\gamma(ab) = \gamma(a)\gamma(b) = ab$ and $\gamma(a+b) = \gamma(a)+\gamma(b) = a+b$. The second follows from the fact that $1 = \gamma(aa^{-1}) = \gamma(a)\gamma(a^{-1}) = a\gamma(a^{-1})$. □

Definition 8.3.6. *Let R be a ring and $n \geq 1$. There is a natural action of S_n on the ring $R[x_1, \ldots, x_n]$ by*

$$\sigma(P(x_1, \ldots, x_n)) = P(x_{\sigma(1)}, \ldots, x_{\sigma(n)})$$

*Define a **symmetric polynomial** with coefficients in R to be an element in $R[x_1, \ldots, x_n]^{S_n}$.*

Example 8.3.7. For any $k \in \{1, \ldots, n\}$, the polynomial

$$s_k := \sum_{i_1<i_2<\cdots<i_k} \prod_{j=1}^{k} x_{i_j} \in \mathbb{Z}[x_1, \ldots, x_n]$$

is symmetric. We call this the k-th elementary symmetric function (in n variables), and this satisfies

$$(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_d) = x^d - s_1(\alpha_1, \ldots, \alpha_d)x^{d-1} + \cdots + (-1)^d s_d(\alpha_1, \ldots, \alpha_d)$$

Theorem 8.3.8 (Fundamental Theorem of the Theory of Symmetric Functions)**.** *Let $\phi : R[x_1, \ldots, x_n] \to R[x_1, \ldots, x_n]$ be the map of rings which sends x_k to s_k and constants to themselves. Then,*

1. *$R[x_1, \ldots, x_n]^{S_n}$ is the image of ϕ*

2. *ϕ is injective*

Then, by the first isomorphism theorem, we have $R[x_1, \ldots, x_n]^{S_n} = R[s_1, \ldots, s_n]$.

Proof. For the first case, we show that every symmetric polynomial can be expressed as a polynomial in s_i. Define lexicographic ordering on monomials

$$x_1^{\alpha_1} \cdots x_n^{\alpha_n} \leq x_1^{\beta_1} \cdots x_n^{\beta_n}$$

By $\alpha_1 < \beta_1$ or $\alpha_1 = \beta_1$ and $x_2^{\alpha_2} \cdots x_n^{\alpha_n} \leq x_2^{\beta_2} \cdots x_n^{\beta_n}$. Fix any symmetric polynomial f. Let $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ be the largest monomial in f. We need $\alpha_1 \geq \cdots \geq \alpha_n$, as any permutation of the powers must also be in f. Also, the largest monomial in $s_1^{\alpha_1-\alpha_2} s_2^{\alpha_2-\alpha_3} \cdots s_n^{\alpha_n}$ is also $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$. Thus, there exists a $c \in R$ such that all monomials in $f - c \cdot s_1^{\alpha_1-\alpha_2} s_2^{\alpha_2-\alpha_3} \cdots s_n^{\alpha_n}$ are strictly smaller than $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$. By repeating, we can write f as a polynomial in s_i.

To show (ii), we can show that s_i are algebraicly independent, and therefore that the kernel is 0. TODO!!! □

Definition 8.3.9. *Define,*

1. $\Delta(x_1, \ldots, x_n) := \prod_{i<j}(x_i - x_j)^2 \in \mathbb{Z}[x_1, \ldots, x_n]^{S_n}$

2. $\delta(x_1, \ldots, x_n) := \prod_{i<j}(x_i - x_j) \in \mathbb{Z}[x_1, \ldots, x_n]^{A_n}$

3. *If $\sigma \in S_n$, $\delta(x_{\sigma(1)}, \ldots, x_{\sigma(n)}) = \text{sign}(\sigma) \cdot \delta(x_1, \ldots, x_n)$.*

where sign : $S_n \to \{-1, 1\}$ *gives the **sign** of the permutation, and $A_n := \ker(sign)$ is called the **alternating group**. We call $\Delta(x_1, \ldots, x_n)$ the **discriminant**.*

Note the third point follows from the fact that any permutation can be written as a product of transpositions, and $\text{sign}(\sigma) = -1$ if σ is a transposition. The $\in$ in the second point follows from this.

9 Field Extensions

9.1 Field extension

Definition 9.1.1. *Let K be a field. A* ***field extension*** *of K, or K-extension is an injection*

$$K \hookrightarrow M$$

of fields. This injection gives M the structure of a K-vector space. We write $M|K$ for the field extension of K to M.

A map from the K extension $M|K$ to $M'|K$ is a ring map $M \to M'$ that is compatible with the injections $K \hookrightarrow M$ and $K \hookrightarrow M'$. Alternatively, it is a map that makes the following commute.

$$\begin{tikzcd}
K \arrow[d, hook] \arrow[dr, hook] & \\
M \arrow[r] & M'
\end{tikzcd}$$

Given $M|K$ is a field extension, we write $\mathrm{Aut}_{\mathrm{K}}(M)$ for the group of bijective maps of K-extensions from M to M, where the group law is the composition of maps. This is the subgroup of $\mathrm{Aut}_{\mathrm{Rings}}(M)$ which are compatible with the K-extension structure of M. We say that the field extension is **finite** if $\dim_K(M) < \infty$.

If M is a finite extension of K, then by rank nullity, any ring map from M to M is a bijection.

Example 9.1.2. If M is not a finite extension of K, then endomorphisms on M need not be bijective. Consider $\phi : \mathbb{Q}(t) \to \mathbb{Q}(t)$ which sends $t \mapsto t^2$. Consequently, $\dim_M(M)$ need not be 1, depending on the structure of the extension.

Proposition 9.1.3 (Tower Law)**.** *If $L|M$ and $M|K$ are finite field extensions, we have*

$$[M : K] \cdot [L : M] = [L : K]$$

Specificaly, if $m_1, \ldots, m_s$ is a basis of M as a K-vector space and $l_1, \ldots, l_t$ is a basis of L as a M vector space, (as vector spaces induced by the field extensions), then $\{m_i l_j\}$ is a basis for L as a K-vector space (as the composition of extensions).

Proof. TODO!!! □

Definition 9.1.4. *Let $M|K$ be a field extension and $a \in M$. Define*

$$\mathrm{Ann}(a) := \{P(x) \in K[x] \mid P(a) = 0\}$$

We have $\mathrm{Ann}(a) \subseteq K[x]$ is an ideal.

We say that a is ***transcendental*** *over K if $\mathrm{Ann}(a) = (0)$ and* ***algebraic*** *if $\mathrm{Ann}(a) \neq (0)$. If a is algebraic over K, then the* ***minimal polynomial*** *m_a is the unique monic polynomial that generates $\mathrm{Ann}(a)$.*

Alternatively the annihalator is the kernel of the map from $K[x]$ to L.

$$\begin{tikzcd}
K \arrow[d] \arrow[dr, hook, "\phi"] & \\
K[x] \arrow[r, "e_a"'] & M
\end{tikzcd}$$

Consequently, there is a injection $K[x]/\mathrm{Ann}(a) \hookrightarrow M$ where M is a domain. Thus, $\mathrm{Ann}(a)$ is prime. If a is algebraic over K, m_a is irreducible (as (m_a) is a prime ideal in a UFD). Thus a monic irreducible polynomial that annihalates a is the minimal polynomial. Prime ideals in a PID are maximal, so $\mathrm{Ann}(a)$ is maximal.

Definition 9.1.5. *We say that a field extension $M|K$ is **algebraic** if for all $m \in M$, the element m is algebraic over K. Else, we say that the field extension is **transcendental**.*

Lemma 9.1.6. *If $M|K$ is finite, then $M|K$ is algebraic.*

Proof. Let $m \in M$. If m is transcendental over K, there is an injection of a K-vector space $K[x] \hookrightarrow M$. $K[x]$ is infinite dimensional, but this contradicts the fact M is a finite-dimensional vector space over K. □

9.2 Separability

Let K be a field. Let $P(x) \in K[x]$, and suppose

$$P(x) = a_d x^d + a_{d-1}x^{d-1} + \cdots + a_0$$

Define $P'(x) = \frac{\mathrm{d}}{\mathrm{dx}}P(x) := da_d x^{d-1} + (d-1)a_{d-1}x^{d-2} + \cdots + a_1$, where $d-i$ is $1_K + \cdots + 1_K$ $(d-i)$-times. This is a K-linear map from $K[x]$ to $K[x]$ and satisfies

$$\frac{\mathrm{d}}{\mathrm{dx}}(P(x)Q(x)) = \frac{\mathrm{d}}{\mathrm{dx}}(P(x))Q(x) + P(x)\frac{\mathrm{d}}{\mathrm{dx}}(Q(x))$$

Definition 9.2.1. *$P(x)$ has **multiple roots** if $(P(x), P'(x)) = (1)$. Equivalently, we have that $\gcd(P(x), P'(x)) = 1$ (by Bézout's Lemma).*

Given

$$P(x) = (x-\rho_1)(x-\rho_2)\cdots(x-\rho_d)$$

we see that $P(x)$ has multiple roots if and only if there are $i \neq j$ such that $\rho_i = \rho_j$.

Lemma 9.2.2. *Let $L|K$ be a field extension, $P(x), Q(x) \in K[x]$. Write $\gcd_L(P(x), Q(x))$ for the greatest common divisor of $P(x)$ and $Q(x)$ viewed as polynomials with coefficients in L. Then,*

$$\gcd(P(x), Q(x)) = \gcd_L(P(x), Q(x))$$

Proof. We use the fact that a generator of $(P(x), Q(x))$ can be computed using Euclidian division. We note that the sequence in which we get this by euclidian algorithm is unique and is invariant of the field. □

In particular, the definition of multiple roots captures roots that may not yet be in the base field.

Remark 9.2.3. Let K be a field and $P(x) \in K[x]$. Let $L|K$ be a field extension. Then, $P(x)$ has multiple roots as a polynomial with coefficients in K if and only if it has multiple roots as a polynomial with coefficients in L.

Lemma 9.2.4. *Let $P(x), Q(x) \in K[x]$ and suppose $Q(x)|P(x)$. If $P(x)$ has no multiple roots, $Q(x)$ also has no multiple roots.*

Proof. Let $T(x) \in K[x]$ be such that $Q(x)T(x) = P(x)$. By the Leibniz rule,

$$(P, P') = (QT, Q'T + QT')$$

If Q and Q' were both divisible by some polynomial W with positive degree, it also divides $Q'T+QT'$ and QT, thus 1 would be divisible by W, a contradiction. □

Lemma 9.2.5. *Suppose that K is a field and that $P(x) \in K[x]\backslash\{0\}$. Suppose that* $\mathrm{char}(K)$ *does not divide* $\deg(P)$ *and that $P(x)$ is irreducible. Then $(P, P') = (1)$.*

Proof. Let

$$P(x) = a_d x^d + a_{d-1}x^{d-1} + \cdots + a_0$$

where $a_d \neq 0$. First note that $d = 0_K$ in K as $\mathrm{char}(K)$ does not divide d. Thus, $P'(x) \neq 0$. As P is irreducible, any common divisor of P and P' is a non-zero constant or P times a non zero constant. It is not the latter as $\deg(P') < \deg(P)$. Thus, it must be a non-zero constant. In other words, $(P, P') = (1)$. □

Noting the proof, if $P' \neq 0$, and P is irreducible, the same result follows.

Definition 9.2.6. *Let K be a field. We say that $P(x) \in K[x]\backslash\{0\}$ is **separable** if all the irreducible factors of $P(x)$ have no multiple roots.*

Note that by Remark 9.2.3 and Lemma 9.2.4, this notion is invariant under field extensions. Also, by Lemma 9.2.5, irreducible polynomials with coefficients in K whose degree is prime to the characteristic of K is separable. Specificaly, if $\mathrm{char}(K) = 0$, any irreducible polynomial with coefficients in K is separable.

Definition 9.2.7. *Let $L|K$ be an algebraic field extension. We say that $L|K$ is **separable** if the minimal polynomial over K of any element of L is separable.*

Noting the previous paragraph, if K is a field and $\mathrm{char}(K) = 0$, all algebraic extensions of K are separable (noting that minimal polynomials are irreducible in $K[x]$).

Lemma 9.2.8. *Let $M|L$ and $L|K$ be algebraic field extensions. Suppose $M|K$ is separable. Then, $M|L$ and $L|K$ are both separable.*

Proof. By definition, $L|K$ is separable. Let $m \in M$ and let $P(x) \in K[x]$ be the minimal polynomial over K. Let $Q(x)$ be the minimal polynomial of m over L. By assumption, $Q(x)|P(x)$. By assumption, $P(x)$ has no multiple roots over K thus also over L by Remark 9.2.3. By Lemma 9.2.4, $Q(x)$ also has no multiple roots over L, thus is separable. □

Lemma 9.2.9 (MOVE LATER)**.** *Let $M|L$ and $L|K$ be finite separale extensions. Then $M|K$ is separable.*

Proof. Consider the following commutative diagram of extensions:

$$\begin{tikzcd}
 & L' \arrow[r] & M' \\
K \arrow[r] & L \arrow[r] \arrow[u] & M \arrow[u]
\end{tikzcd}$$

where L' is the normal closure of L over K such that $L'|K$ is Galois, and M' is the smallest field containing M and L'. Then note that $L'|K$ is separable (as it is Galois), and by using the fact that

$L'|L$ is separable, $M'|L$ is also separable. Thus, $M'|L'$ is separable. Thus, we may reduce to the case where $L'|K$ is a Galois extension and take $L := L'$, $M := M'$.

Let $\alpha \in M$ be a root of an irreducible polynomial $f \in L[t]$. By assumption, this is separable. Now let $G := \mathrm{Gal}(L|K)$. For each $\sigma \in G$, we have

$$f^{\sigma}(t) = \sigma(f(t)) = \sum_i \sigma(a_i)t^i$$

This is also irreducible and separable. Taking

$$g(t) = \prod_{\sigma \in G} f^{\sigma}(t)$$

we see that $g \in K[t]$ and is also separable as each f^{σ} is separable. Any minimum polynomial of α in K divides g, so in particular is separable. Thus $M|K$ is separable. □

Example 9.2.10. Finite extensions need not be separable. Noting the proof in Lemma 9.2.5, we at least want to find a polynomial P such that $P' = 0$.

Consider $K := \mathbb{F}_2(t)$ where $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$. Let $P(x) := x^2 - t$. As $P(x)$ is of degree 2 and has no roots in K (by considering degrees), it is irreducible.

Define $L := K[x]/(P(x))$. As $P(x)$ is irreducible, $(P(x))$ is prime, thus maximal in $K[x]$, meaning L is a field. However, $P'(x) = 0$, thus $(P', P) = (P) \neq (1)$. As $P(x)$ is the minimal polynomial of $x \in L$, $L|K$ is not separable.

Example 9.2.11. Let p be a prime and take $f \in \mathbb{F}_p(t)$. Write

$$f(t) = \sum_{i=0}^{n} a_i t^i$$

where $a_i \in \mathbb{F}_p$. Then, $D(f)(t) = \sum_{i=1}^{n} i a_i t^{i-1}$ By characteristic, this vanishes if and only if $p | i a_i$ for all i, which is equivalent to $a_i = 0$ whenever $p \not| i$. Hence the only possible nonzero terms in f are those with exponent a multiple of p, so

$$f(t) = \sum_j a_{pj} t^{pj} = \sum_j a_{pj} (t^p)^j = g(t^p)$$

Suppose now that the map $x \mapsto x^p$ is bijective (such fields are called perfect). Then, writing $f(t) = g(t^p)$, we can take $g(t^p) = \sum_{j=0}^{m} b_j t^{pj}$ and picking j such that $c_j^p = b_j$, we have

$$g(t^p) = \sum_j (c_j)^p u^{pj} = \left(\sum_j c_j u^j\right)^p = h(u)^p$$

where $h(u) = \sum_j c_j u^j$. In particular, $f(t) = h(t)^p$. But then f is not irreducible. Thus, if f is irreducible and $\mathbb{F}_p$ is perfect, $D(f) \neq 0$, meaning f is separable.

9.3 Simple Extensions

Definition 9.3.1. *Let $\iota : K \hookrightarrow M$ be a field extension and $S \subseteq M$ be a subset. Define*

$$K(S) := \bigcap_{\text{field } L, L \subseteq M, L \supseteq S, L \supseteq \iota(K)} L$$

This is a subfield of M and is called the ***field generated by S over*** *K, and the elements of S are called* ***generators*** *of $K(S)$. The field extensions $M|K$ is the composition of the natural field extensions $K(S)|K$ and $M|K(S)$.*

Note also that if $S = \{s_1, \dots, s_k\}$, then

$$K(S) = K(s_1)\dots(s_k)$$

We also say that $M|K$ is a **simple extension** if there is a $m \in M$ such that $M = K(m)$.

Example 9.3.2. Some examples of simple extensions:

- Let $K = \mathbb{Q}$ and $M = \mathbb{Q}(i, \sqrt(2))$ be a field generated by i and $\sqrt{2}$ in $\mathbb{C}$. Then M is a simple algebraic extension of K generated by $i + \sqrt{2}$.

- Let $M = \mathbb{Q}(x) = \mathrm{Frac}(\mathbb{Q}[x])$ and let $K = \mathbb{Q}$. Then M is a simple transcendental extension of K, generated by x.

Proposition 9.3.3. *Let $M = K(\alpha)|K$ be a simple algebraic extension. Let $P(x)$ be the minimal polynomial of α over K. Then, there is a natural isomorphism of K-extensions*

$$K[x]/(P(x)) \simeq M$$

which sends x to α.

Proof. We first note that there is a natural map from $K[x]/(P(x))$ to M by evaluation. As $P(x) \neq 0$, we have $(P(x))$ is a maximal ideal. Thus, the image of $K[x]/(P(x))$ in M is a field. By definition, this is the entirety of M. □

Remark 9.3.4. Noting the above proposition, we can note that $[M : K] = \deg(P)$. Then, the set $\{1, x, \dots, x^{\deg(P)-1}\}$ is a basis. Also as a consequence, a finitely generated algebraic extension is a finite extension.

Corollary 9.3.5. *Let $M = K(\alpha)|K$ be a simple algebraic extension. Let $K \hookrightarrow L$ be an extension of fields. Let $P(x)$ be the minimal polynomial of α over K. There is a bijective correspondence with the roots of $P(x)$ in L and the maps of K-extensions $M \hookrightarrow L$.*

Proof. The corresponding map is given by the unique map extended from sending α to the root of $P(x)$ in L. □

Example 9.3.6. Let $M := \mathbb{Q}(i) \subseteq \mathbb{C}$ and let $K = \mathbb{Q}$, and $L = \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{C}$. There is no map of K-extensions $M \hookrightarrow L$ because the roots of $x^2 + 1$ do not lie in $L \subseteq \mathbb{R}$. If we change $L = \mathbb{C}$, then there are two maps of K-extensions $M \hookrightarrow L$ corresponding to the function extended by sending $i \mapsto i$ and $i \mapsto -i$.

9.4 Splitting Fields

Definition 9.4.1. *Let K be a field. Let $P(x) \in K[x]$. We say that $P(x)$* ***splits*** *in K if for some $c \in K$ and sequence of $\{a_i \in K\}$, we have*

$$P(x) = c \cdot \prod_{i=1}^{k} (x - a_i)$$

We call a field ***algebraicly closed*** *if any polynomial with coefficients with L splits in L.*

If $P(x) \in K[x]$ is irreducible and $\deg(P) > 1$, $P(x)$ has no roots in K and thus does not split in K.

Definition 9.4.2. *A field extension $M|K$ is a* ***splitting extension*** *for $P(x) \in K[x]$ if*

1. *$P(x)$ splits in M*
2. *M is generated over K by the roots of $P(x)$ in M.*

Theorem 9.4.3. *Let $P(x) \in K[x]$. Then,*

- *There exists a field extension $M|K$ which is a splitting extension for $P(x)$*
- *If $L|K$ is a splitting extension for $P(x)$, then L and M are isomorphic as K-extensions*
- *Let $L|K$ be a splitting extension for $P(x)$ and $J|K$ be any K-extension. Then, the images of all the maps of K-extensions $L \hookrightarrow J$ coincide.*

Proof. (i) We work by induction on $\deg(P)$. If $\deg(P) = 1$, then $K|K$ is a splitting extension for $P(x)$. Suppose that $\deg(P) > 1$. Let P_1 be an irreducible factor of $P(x)$. Consider $M_1 := K[x]/(P_1(x))$. M_1 is a field, and there is a natural map of rings $K \hookrightarrow M_1$.

By definition, $P(x)$ has a root a in M_1 (which is just x in the presentation $M_1 = K[x]/(P_1(x))$). Let M be a splitting field for $P(x)/(x-a) \in M_1[x]$ over M_1, which exists by the inductive hypothesis. By construction, $P(x)$ splits in M. Let $a_2, \ldots, a_k$ be roots of $P(x)/(x-a)$ in M. By Proposition 9.3.3, $M = K(a)(a_2)\ldots(a_k) = K(a, a_2, \ldots, a_k)$ and thus M is generated over K by roots in M. Consequently, M is a splitting field of $P(x)$ over K.

(ii) We work by induction on $\deg(P)$. If $\deg(P) = 1$, we are done. Suppose $\deg(P) > 1$. Let $a \in M$ be a root of $P(x)$ in M and $Q(x) \in K[x]$ be its minimal polynomial. As $Q(x)|P(x)$, $Q(x)$ splits in M and also in L.

Now let a_1 be a root of $Q(x)$ in L. Note from before that $M|K(a)$ is a splitting extension of $P(x)/(x-a) \in K(a)$. Similarly, $L|K(a_1)$ is a splitting extension of $P(x)/(x-a_1) \in K(a_1)$. Define $J := K[x]/(Q(x))$. This is a field as $Q(x)$ is irreducible, and there are natural isomorphisms $J \simeq K(a)$ and $J \simeq K(a_1)$ of K-extensions. Considering the J-extensions $M|J$ and $L|J$ from these isomorphisms, the inductive hypothesis shows the two are isomorphic as J extensions. By construction, this gives an isomorphism of K-extensions.

(iii) If there are no maps of K-extensions $L \hookrightarrow J$, we are done. Else, suppose there is a map $\phi : L \hookrightarrow J$ of K-extensions. As L is generated over the roots of $P(x)$, the image of ϕ are generated over K by the image of these roots in J under ϕ. We claim these images are the roots of $P(x)$ in J.

To prove the above claim, let $\alpha_1, \ldots, \alpha_d$ be roots of $P(x)$ in L with multiplicities. Then,

$$P(x) = x^d - s_1(\alpha_1, \ldots, \alpha_d)x^{d-1} + \cdots + (-1)^d s_d(\alpha_1, \ldots, \alpha_d)$$

Thus, the elements of $\phi(\alpha_1), \ldots, \phi(\alpha_d)$ are the roots of

$$\begin{aligned} & x^d - s_1(\phi(\alpha_1), \ldots, \phi(\alpha_d))x^{d-1} + \cdots + (-1)^d s_d(\phi(\alpha_1), \ldots, \phi(\alpha_d)) \\ &= x^d - \phi(s_1(\alpha_1, \ldots, \alpha_d))x^{d-1} + \cdots + (-1)^d \phi(s_d(\alpha_1, \ldots, \alpha_d)) \\ &= P(x) \end{aligned}$$

As $P(x)$ has coefficients in K. Now the set of roots of $P(x)$ in J does not depend on ϕ, and so the claim follows. □

Remark 9.4.4. Let K be a field and $P(x) \in K[x]$. Suppose that there is a field extension $K \hookrightarrow L$, where L is algebraicly closed. Let $S \subseteq L$ be the roots of $P(x) \in L$. Then $K(S) \subseteq L$ is a splitting field for $P(x)$. This follows from the fact $P(x)$ splits in $K(S)$ as L is algebraicly closed, and that $K(S)$ is generated by the roots of $P(x)$ by construction.

As a specific example, we can generate a splitting field for any polynomial in $\mathbb{Q}[x]$ by considering $L = \mathbb{C}$.

Remark 9.4.5. Any field K has an algebraic field extension $K \hookrightarrow K'$ such that K' is algebraicly closed. This is unique up to isomorphism and is called the **algebraic closure** of K.

9.5 Normal Extensions

Definition 9.5.1. *An algebraic extension $L|K$ is called* ***normal*** *if the minimal polynomial over K of any element of L splits in L.*

Note that a splitting extension (field) is by definition a normal extension (field).

Example 9.5.2. Some examples of extensions are

- $\mathbb{Q}(\sqrt[3]{2})|\mathbb{Q}$ is not normal, as the minimal polynomial for $\sqrt[3]{2}$, namely $x^3 + 2$, does not split.
- $\mathbb{Q}(\sqrt{2})|\mathbb{Q}$ is normal, noting that as $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$, any minimal polynomial in $\mathbb{Q}(\sqrt{2})$ has degree at most 2, which if it has a root, splits.

Lemma 9.5.3. *Let $M = K(\alpha_1, \ldots, \alpha_k)|K$ be an algebraic field extension. Let $J|K$ be an extension in which the polynomial $\prod_{i=1}^{k} m_{\alpha_i} \in K[x]$ splits. Then the set of maps of K-extensions $M \to J$ is finite and non-empty. If m_{α_i} are all separable, there are $[M : K]$ such maps.*

Proof. We first prove that this set is finite and non-empty. By Corollary 9.3.5, there is an extension of the map $K \hookrightarrow J$ to $K(\alpha_1)$, and only finitely many choices for such extension. The minimal polynomial of α_2 over $K(\alpha_1)$ divides m_{α_2} and has a root in J as m_{α_2} splits in J. Thus, again, there is an extension from the ring map $K(\alpha_1) \hookrightarrow J$ to $K(\alpha_1)(\alpha_2) = K(\alpha_1, \alpha_2) \hookrightarrow J$, and only finitely many such. Repearing shows the same is the case for $K(\alpha_1, \ldots, \alpha_k) = M \hookrightarrow J$.

For the cardinality of the set, we note that there are $[K(\alpha_1) : K] = \deg(m_{\alpha_1})$ extensions of maps $K \hookrightarrow J$ to $K(\alpha_1)$. Continuting, for any ring map $K(\alpha_1) \hookrightarrow J$, there are $[K(\alpha_1, \alpha_2) : K(\alpha_1)]$ extensions of this map to a map $K(\alpha_1, \alpha_2) \hookrightarrow J$. By the tower law, there are

$$[K(\alpha_1) : K][K(\alpha_1, \alpha_2) : K(\alpha_1)] = [K(\alpha_1, \alpha_2) : K]$$

extensions of the map $K \hookrightarrow J$ to a ring map $K(\alpha_1, \alpha_2) \hookrightarrow J$. Continuting,

$$[K(\alpha_1) : K] \cdots [M : K(\alpha_1, \ldots, \alpha_{k-1})] = [M : K]$$

extensions of the map $K \hookrightarrow J$ to a ring map $M \hookrightarrow J$. □

Theorem 9.5.4. *A finite field extension $L|K$ is normal if and only if it is a splitting extension for a polynomial with coefficients in K.*

Proof. ($\Rightarrow$) Suppose that $L|K$ is finite and normal. Let $\alpha_1, \ldots, \alpha_k$ be generators for L over K (as a K-basis). Define

$$P(x) := \prod_{i=1}^{k} m_{\alpha_i}(x)$$

where $m_{\alpha_i}(x)$ is the minimal polynomial for α_i over K. Then, by assumption, $P(x)$ splits in L and the roots of $P(x)$ generate L, so L is a splitting field for $P(x)$.

($\Leftarrow$) Suppose that L is a splitting field of a polynomial in $K[x]$. Let $\alpha \in L$ and $\beta_1, \ldots, \beta_k \in L$ be such that $L = K(\alpha, \beta_1, \ldots, \beta_k)$. Let J be a splitting field of the products of the minimal polynomials over K over the elements $\alpha, \beta_1, \ldots, \beta_k$. Choose a root ρ in J of the minimal polynomial $Q(x)$ of α over K. By Corollary 9.3.5, there is an extension of the map $K \hookrightarrow J$ to a ring map $\mu : K(\alpha) \hookrightarrow J$ such that $\mu(\alpha) = \rho$. By Lemma 9.5.3, there is an extension of μ to a ring map $\lambda : L \hookrightarrow J$. By Theorem 9.4.3, the image of λ on L in J is independent of λ and thus of μ. Consequently, as we have not fixed ρ, the image of λ with L in J contains all the roots of $Q(x)$. Thus, $Q(x)$ splits in the image of λ. As $Q(x)$ has coefficients in K and λ gives an isomorphism between L and the image of λ, $Q(x)$ splits in L. □

Theorem 9.5.5. *Let $L|K$ be a splitting field of a separable polynomial over K. Then we have $\#\mathrm{Aut}_K(L) = [L : K]$.*

Proof. Apply Lemma 9.5.3 with $L = M = J$. □

Theorem 9.5.6. *Let $\iota : K \hookrightarrow L$ be a finite field extension. Then $\mathrm{Aut}_K(L)$ is finite. Furthermore, the following are equivalent :*

1. *$\iota(K) = L^{\mathrm{Aut}_K(L)}$*

2. *$L|K$ is normal and separable*

3. *$L|K$ is a splitting extension for a separable polynomial with coefficients in K.*

Proof. We first note that if $\mathrm{Aut}_K(L)$ were infinite, we can obtain infinitely many maps of K extensions $L \hookrightarrow J$ by composing any map $L \hookrightarrow J$ with elements of $\mathrm{Aut}_K(L)$, which contradicts the result from Lemma 9.5.3.

(i) $\Rightarrow$ *(ii)* Let $P(x)$ be the minimal polynomial of some element $\alpha \in L$. We have to show that $P(x)$ splits and is separable. Define

$$Q(x) := \prod_{\beta \in \mathrm{Orb}(\mathrm{Aut}_K(L), \alpha)} (x - \beta)$$

By definition, $Q(x)$ is separable. Let $d := \#\mathrm{Orb}(\mathrm{Aut}_K(L), \alpha)$. Let $\beta_1, \ldots, \beta_d$ be the elements of $\mathrm{Orb}(\mathrm{Aut}_K(L), \alpha)$. Note that

$$Q(x) = x^d - s_1(\beta_1, \ldots, \beta_d)x^{d-1} + \cdots + (-1)^d s_d(\beta_1, \ldots, \beta_d)$$

For any $\gamma \in \mathrm{Aut}_K(L)$ and for any $i \in \{1, \ldots, d\}$ we have

$$\gamma(s_i(\beta_1, \ldots, \beta_d)) = s_i(\gamma(\beta_1), \ldots, \gamma(\beta_d))$$

Noting that s_i is a symmetric function and γ permutes elements of $\mathrm{Orb}(\mathrm{Aut}_K(L), \alpha)$ (by composition), we have

$$s_i(\gamma(\beta_1), \ldots, \gamma(\beta_n)) = s_i(\beta_1, \ldots, \beta_n)$$

As γ was arbitrary, we see that $s_i(\beta_1, \ldots, \beta_d) \in L^{\mathrm{Aut}_K(L)} = \iota(K)$. Thus, $Q(x) \in \iota(K)[x]$. We can therefore identify $Q(x)$ with a polynomial in $K[x]$ with ι.

However, $\alpha \in \mathrm{Orb}(\mathrm{Aut}_K(L), \alpha)$, so $Q(\alpha) = 0$. By definition of $P(x)$, $P(x)|Q(x)$, so $P(x)$ splits in L and has no multiple roots and therefore is separable.

(ii) ⇒ *(iii)* Let $\alpha_1, \dots, \alpha_k$ be generators of L over K. Let $P(x) := \prod_{i=1}^{k} m_{\alpha_i}(x)$, where $m_{\alpha_i}(x)$ is the minimal polynomial of α_i over K. Then, $P(x)$ is a separable polynomial by construction and L is also a splitting extension for $P(x)$.

(iii) ⇒ *(i)* Note first that by construction, $\iota(K) \subseteq L^{\mathrm{Aut}_K(L)}$ as any element of $\mathrm{Aut}_K(L)$ fixes the image of K in L by definition. So, $L|K$ is the composition of extensions $L^{\mathrm{Aut}_K(L)}|K$ and $L|L^{\mathrm{Aut}_K(L)}$. Note that $L|L^{\mathrm{Aut}_K(L)}$ is also the splitting field of a separable polynomial over $L^{\mathrm{Aut}_K(L)}$ (by taking the same polynomial for $L|K$). Also note the identity $\mathrm{Aut}_{L^{\mathrm{Aut}_K(L)}}(L) = \mathrm{Aut}_K(L)$

Now, by Theorem 9.5.5, we have

$$[L : L^{\mathrm{Aut}_K(L)}] = \#\mathrm{Aut}_{L^{\mathrm{Aut}_K(L)}}(L)$$

and

$$[L : K] = \#\mathrm{Aut}_K(L)$$

giving $[L : L^{\mathrm{Aut}_K(L)}] = [L : K]$. The tower law shows that $[L^{\mathrm{Aut}_K(L)} : K] = 1$, or equivalently, $L^{\mathrm{Aut}_K(L)} = \iota(K)$. □

Corollary 9.5.7. *Let $L|K$ be an algebraic field extension. Suppose that L is generated by $\alpha_1, \dots, \alpha_k \in L$ and the minimal polynomial of each α_i is separable. Then, $L|K$ is separable.*

Proof. By Lemma 9.5.3 and Theorem 9.4.3, there is an extension $M|L$ such that $M|K$ is the splitting field of a separable polynomial (the product of the minimal polynomials). By 9.5.6, the extension $M|K$ is separable. Thus, the extension $L|K$ is also separable. □

9.6 Galois Extensions

Definition 9.6.1. *A field extension $\iota : K \hookrightarrow L$ is called a Galois extension if $L^{\mathrm{Aut}_K(L)} = \iota(K)$. As notation, $\iota(K)$ is often replaced with K (unless there is ambiguity).*

If $L|K$ is a Galois extension, write

$$\mathrm{Gal}(L|K) = \Gamma(L|K) := \mathrm{Aut}_K(L)$$

and call $\mathrm{Gal}(L|K)$ *the Galois group of $L|K$. If $L|K$ is finite, then this is a finite group (by Theorem 9.5.6).*

As a consequence of Theorem 9.5.6, a finite field extension $L|K$ is a Galois extension if and only if L is a splitting field of a separable polynomial over K if and only if it is normal and separable. As a consequence, if $L|K$ is a finite galois extension which is the composition of two extensions $L|K_1$ and $K_1|K$, then $L|K_1$ is a finite galois extension. This is because properties like normal and separable are preserved by such cuts (noting that the minimal polynomial of L over K_1 divides that over K). However, it does not hold in general that $K_1|K$ is a galois extension, noting that this need not be a normal extension.

Definition 9.6.2. *Let K be a field and $P(x) \in K[x]$ be a separable polynomial. Let $L|K$ be a splitting field for $P(x)$. We sometimes write* $\mathrm{Gal}(P) = \mathrm{Gal}(P(x))$ *for* $\mathrm{Gal}(L|K)$. *Note the abuse of notation, as splitting fields are not related by canonical isomorphism. Thus, in the strict sense,* $\mathrm{Gal}(P)$ *refers to an isomorphism class of finite groups.*

Lemma 9.6.3. *Let K be a field and let $G \subseteq \mathrm{Aut}_{\mathrm{Rings}}(K)$ be a finite subgroup. Then $[K : K^G] \leq \#G$.*

Proof. Suppose not. Then, we have a sequence $\alpha_1, \dots, \alpha_d$ of elements of K which is linearly independent over K^G and such that $d > \#G$. Let $n := \#G$ and let $\sigma_1, \dots, \sigma_n \in G$ be the enumeration of G. Consider now the matrix defined by $(\sigma_i(\alpha_j))$. The columns are linearly dependent over K as $n < d$. Thus, we have a sequence $\beta_1, \dots, \beta_d$ with some non-vanishing term such that

$$\sum_{i=1}^{d} \beta_i(\sigma_k(\alpha_i))$$

for all k. Choose a sequence $\beta_1, \dots, \beta_d$ such that

$$r := \#\{i \in \{1, \dots, d\} \mid \beta_i \neq 0\}$$

is minimal. By reordering, suppose that $\beta_1, \dots, \beta_r \neq 0$ and that $\beta_{r+1}, \dots, \beta_d = 0$. Dividing through by β_r, suppose that $\beta_r = 1$. As $\alpha_1, \dots, \alpha_d$ are linearly independent over K^G, (noting that β_i kills the identity) we have some $i_0 \in \{1, \dots, r\}$ such that $\beta_{i_0} \notin K^G$. Note that $r > 1$ as $i_0 \neq r$. By renumbering, we may assume $\beta_1 \notin K^G$.

Now, take $k_0 \in \{1, \dots, n\}$ such that $\sigma_{k_0}(\beta_1) \neq \beta_1$. Applying σ_{k_0} to our first equation, we get

$$\sum_{i=1}^{d} \sigma_{k_0}(\beta_i)(\sigma_{k_0}\sigma_k)(\alpha_i) = 0$$

for all $k \in \{1, \dots, n\}$. Noting that σ only permutes, we have

$$\sum_{i=1}^{d} \sigma_{k_0}(\beta_i)(\sigma_k)(\alpha_i) = 0$$

for all $k \in \{1, \dots, n\}$. Subtracting with the original equation, this gives

$$\sum_{i=1}^{d} (\sigma_{k_0}(\beta_i) - \beta_i)(\sigma_k)(\alpha_i) = 0$$

for all $k \in \{1, \dots, n\}$. Noting the definition of r and from $\beta_r = 1$, we have

$$\sum_{i=1}^{r-1} (\sigma_{k_0}(\beta_i) - \beta_i)(\sigma_k)(\alpha_i) = 0$$

Now, as $\sigma_{k_0}(\beta_1) \neq \beta_1$, we have a non-zero annihlating sum, which contradicts the minimality of r. Thus $d \leq n$. □

Theorem 9.6.4 (Artin's Lemma)**.** *Let K be a field and let $G \subseteq \mathrm{Aut}_{\mathrm{Rings}}(K)$ be a finite subgroup. Then the extension $K|K^G$ is a finite Galois extension, and the inclusion $G \hookrightarrow \mathrm{Aut}_{K^G}(K)$ is an isomorphism of groups.*

Proof. First we claim that

$$K^G = K^{\mathrm{Aut}_{K^G}(K)}$$

First note that $K^G \subseteq K^{\mathrm{Aut}_{K^G}(K)}$ (if you are in K^G, you are fixed by things that fix K^G). On the other hand, $G \subseteq \mathrm{Aut}_{K^G}(K)$ (automorphisms in G fix K^G). Thus, $K^G \supseteq K^{Aut_{K^G}(K)}$. Thus, we have proven the claim.

Now, as $K|K^G$ is a finite extension by Lemma 9.6.3, we have from Theorem 9.5.6 that $K|K^G$ is a splitting extension of a separable polynomial with coefficients in K^G. By Theorem 9.5.5,

$$[K : K^G] = \#\mathrm{Aut}_{K^G}(K)$$

On the other hand, from Lemma 9.6.3, $[K : K^G] \leq \#G$ so, we have $\#\mathrm{Aut}_{K^G}(K) \leq \#G$. Now, $G \subseteq \mathrm{Aut}_{K^G}(K)$ so, $\#G \leq \#\mathrm{Aut}_{K^G}(K)$, giving $\#G = \#\mathrm{Aut}_{K^G}(K)$. Thus, $G = \mathrm{Aut}_{K^G}(K)$.

Finally, Theorem 9.5.6 implies that $K|K^G$ is a finite Galois extension with Galois group G. □

Theorem 9.6.5 (Fundamental Theorem of Galois Theory)**.** *(i) The map*

$$\{\textit{subfields of } L \textit{ containing } \iota(K)\} \mapsto \{\textit{subgroups of } \mathrm{Gal}(L|K)\}$$

given by

$$M \mapsto \mathrm{Gal}(L|M)$$

is a bijection. The inverse is given by the map

$$H \mapsto L^H$$

(ii) Let M be a subfield of L containing $\iota(K)$. We have

$$[L : M] = \#\mathrm{Gal}(L|M)$$

and

$$[M : K] = \frac{\#\mathrm{Gal}(L|K)}{\#\mathrm{Gal}(L|M)}$$

(iii) Let M be a subfield of L containing $\iota(K)$. Then $M|K$ is a Galois extension if and only if the group $\mathrm{Gal}(L|M)$ is a normal subgroup of $\mathrm{Gal}(L|K)$. In that case, there is an isomorphism $I_M : \mathrm{Gal}(L|K)/\mathrm{Gal}(L|M) \simeq \mathrm{Gal}(M|K)$.

Proof. (i) By considering the claimed isomorphisms, we want to show that $M = L^{\mathrm{Gal}(L|M)}$ and $\mathrm{Gal}(L|L^H) = H$ for any intermediate field M and any subgroup $H \subseteq \mathrm{Gal}(L|K)$.

The first equality is a consequence of the fact that $L|M$ is a Galois extension. The second follows from Artin's Lemma.

(ii) The equation $[L : M] = \#\mathrm{Gal}(L|M)$ is a consequence of Theorem 9.5.5. The equation $[M : K] = \#\mathrm{Gal}(L|K)/\#\mathrm{Gal}(L|M)$ is a consequence of the tower law and $\#\mathrm{Gal}(L|K) = [L : K]$.

(iii) Suppose that M is an intermediate field and that $M|K$ is a Galois extension. Then for any $\gamma \in \mathrm{Gal}(L|K)$, $\gamma(M) = M$ by Theorem 9.4.3 (iii). In particular, we have a homomorphism

$$\phi_M(\gamma) = \gamma|_M$$

The kernel of this homomorphism is $\mathrm{Gal}(L|M)$ by definition. Hence, $\mathrm{Gal}(L|M)$ is normal in $\mathrm{Gal}(L|K)$ by the first isomorphism theorem.

On the other hand, suppose that $\mathrm{Aut}_M(L)$ is a normal subgroup of $\mathrm{Gal}(L|K)$. Take $\gamma \in \mathrm{Gal}(L|K)$. By definitions,

$$\begin{aligned}
\mathrm{Aut}_{\gamma(M)}(L) &= \mathrm{Gal}(L|\gamma(M)) = \{\mu \in \mathrm{Gal}(L|K) \mid \mu(\alpha) = \alpha,\ \forall \alpha \in \gamma(M)\} \\
&= \{\mu \in \mathrm{Gal}(L|K) \mid \mu(\gamma(\beta)) = \gamma(\beta),\ \forall \beta \in M\} \\
&= \{\mu \in \mathrm{Gal}(L|K) \mid (\gamma^{-1}\mu\gamma)(\beta) = \beta,\ \forall \beta \in M\} \\
&= \gamma \mathrm{Gal}(L|M)\gamma^{-1} \\
&= \mathrm{Gal}(L|M)
\end{aligned}$$

By bijective correspondence given in (i), we have $M = \gamma(M)$. Thus, we have a homomorphism

$$\phi_M : \mathrm{Gal}(L|K) \to \mathrm{Aut}_K(M)$$

given by $\phi_M(\gamma) = \gamma|_M$. From (ii) and the first isomorphism theorem, $\mathrm{im}(\phi_M) \subseteq \mathrm{Aut}_K(M)$ has cardinality $[M : K]$, with kernel $\mathrm{Aut}_M(L)$. On the other hand, by Artin's Lemma, we know $[M : M^{\mathrm{Im}(\phi)}] = \#\mathrm{Im}(\phi_M)$ such that $[M : M^{\mathrm{Im}(\phi)}] = [M : K]$. By the tower law, $K = M^{\mathrm{Im}(\phi)}$. In particular, $M|K$ is a Galois extension and ϕ_M is therefore surjective.

The isomorphism is uniquely determined by the fact that $I_M(\gamma \bmod \mathrm{Gal}(L|M)) = \gamma|_M$ for any $\gamma \in \mathrm{Gal}(L|K)$. □

Remark 9.6.6. Let $\iota : K \hookrightarrow L$ be a Galois extension. Let $M \subseteq L$ be an intermediate field. Then $M|K$ is a Galois extension if and only if the maps of K-extensions $M \to L$ have the same image (which is M).

If all the maps have M as an image, then for all $\gamma \in \mathrm{Gal}(L|K)$, $\gamma(M) = M$, and thus from the proof above, $M|K$ is a Galois extension. On the other hand, if $M|K$ is a Galois extension, then for all $\gamma \in \mathrm{Gal}(L|K)$, $\gamma(M) = M$ by Theorem 9.4.3 (images of embeddings from splitting fields coincide).

Corollary 9.6.7. *Let $\iota : K \to L$ be a finite separable extension. There are only finitely many intermediate fields between L and $\iota(K)$.*

Proof. Without loss of generality, we can extend L to a Galois extension (by Lemma 9.5.3, taking the splitting field over the minimal polynomials of the generators). The Galois group is finite, and bijectively corresponds to intermediate fields. □

Example 9.6.8. We consider the Galois group of the extension $\mathbb{Q}(\sqrt{2}, i)|\mathbb{Q}$ and of its subfields. Note first that $\mathbb{Q}(\sqrt{2}, i)$ is the splitting field of the polynomial $(x^2 - 2)(x^2 + 1)$ whose roots are $\pm\sqrt{2}, \pm i$. In particular, $\mathbb{Q}(\sqrt{2}, i)|\mathbb{Q}$ is a splitting field of a separable polynomial, thus Galois.

We note the successive extensions $\mathbb{Q}(\sqrt{2}, i)|\mathbb{Q}(\sqrt{2})|\mathbb{Q}$. The minimal polynomial of $\sqrt{2}$ over $\mathbb{Q}$ is $x^2 - 2$, and the polynomial $x^2 + 1$ is the minimal polynomial of i over $\mathbb{Q}(\sqrt{2})$. By the tower law, $[\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}] = 4$. By Theorem 9.5.5, we have $\#\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, i)|\mathbb{Q}) = 4$. Define $G := \mathrm{Gal}(\mathbb{Q}(\sqrt{2}, i)|\mathbb{Q})$. By the classification of finite groups, we know that G is abelian, and that $G \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ or $G \simeq \mathbb{Z}/4\mathbb{Z}$. Note also that $\#\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, i)|\mathbb{Q}(i)) = 2$. This follows from the fact the extension is not trivial (otherwise $[\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}]$ would equal 2). With similar logic, $\#\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, i)|\mathbb{Q}(\sqrt{2})) = 2$. Groups of order 2 are isomorphic to $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, i)|\mathbb{Q}(\sqrt{2})) \simeq \mathrm{Gal}(\mathbb{Q}(\sqrt{2}, i)|\mathbb{Q}(i)) \simeq \mathbb{Z}/2\mathbb{Z}$.

By the fundamental theorem of Galois theory, the two subgroups $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, i)|\mathbb{Q}(i))$ and $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, i)|\mathbb{Q}(\sqrt{2}))$ cannot coincide, as they correspond to different subfields of $\mathbb{Q}(\sqrt{2}, i)$. Consequently, $G \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ has three non trivial subgroups, and we find the third is given by $\mathbb{Q}(i\sqrt{2})$.

Example 9.6.9. We also note some field extensions that are not Galois.

- The extension $\mathbb{Q}(\sqrt[3]{2})|\mathbb{Q}$ is not a normal extension, thus not Galois.
- The extension $\mathbb{F}_2(t)[x]/(x^2 - t)|\mathbb{F}_2(t)$ is not separable, thus not Galois.

Lemma 9.6.10. *Let $L|K$ be a finite Galois extension. Let $\alpha \in L$. Then the minimal polynomial of α over K is the polynomial*

$$\prod_{\beta \in \mathrm{Orb}(\mathrm{Gal}(L|K), \alpha)} (x - \beta)$$

Proof. Let $P(x) = \prod_{\beta \in \mathrm{Orb}(\mathrm{Gal}(L|K),\alpha)}(x-\beta)$. Let $m_\alpha(x) \in K$ be the minimal polynomial of α over K. We know that $P(x) \in K[x]$, thus we have

$$m_\alpha(x)|P(x)$$

It is therefore sufficient to prove that $P(x)$ is irreducible over K. Suppose for contradiction $P(x) = Q(x)T(x)$ for $Q(x), T(x) \in K[x]$ and $\deg(Q), \deg(T) > 1$. Note that if $\rho \in L$ and $Q(\rho) = 0$, $\gamma(Q(\rho)) = Q(\gamma(\rho)) = \gamma(0) = 0$, thus roots of $Q(x)$ in L are stable under the action $\mathrm{Gal}(L|K)$. As $Q(x)$ has a root in L, noting $P(x)$ splits in L and $Q(x)|P(x)$, the set of roots of $P(x)$ contains a strict subset who is stable under $\mathrm{Gal}(L|K)$. This contradicts the fact the set of roots of $P(x)$ is the orbit of α under $\mathrm{Gal}(L|K)$. □

Lemma 9.6.11. *Let K be a field and let $P(x) \in K[x]$. Let $L|K$ be a splitting extension of $P(x)$ and let $\alpha_1, \dots, \alpha_n \in L$ be the roots of $P(x)$ with multiplicities. Then,*

1. *If $P(x)$ has no repeated roots, and $\phi : \mathrm{Aut}_K(L) \to S_n$ satisfies $\gamma(\alpha_i) = \alpha_{\phi(\gamma)(i)}$, then ϕ is an injective group homomorphism.*
2. *If $P(x)$ is irreducible over K and has no repeated roots, the image of ϕ is a transitive subgroup of S_n*
3. *The element $\Delta_P := \Delta(\alpha_1, \dots, \alpha_n)$ lies in K and depends only on $P(x)$*
4. *Suppose that* $\mathrm{char}(K) \neq 2$. *Suppose also that $P(x)$ has no repeated roots. Then the image of ϕ lies inside $A_n \subseteq S_n$ if and only if $\Delta_P \in (K^*)^2$.*

Proof. (i) The map is tautologically a group homomorphism. It is injective as L is generated by the roots, thus an element γ that acts as the identity on the roots must act as the identity on L.

(ii) We only need to show $\mathrm{Aut}_K(L)$ acts transitively on the roots. As $P(x)$ is irreducible, it is the minimal polynomial of any α_i. By Lemma 9.6.10, the roots are an orbit under $\mathrm{Aut}_K(L)$ over any root, so we are done.

(iii) Note first that

$$P(x) = x^d + a_{d-1}x^{d-1} + \dots + a_0 = x^d + s_1(\alpha_1, \dots, \alpha_d)x^{d-1} + \dots + (-1)^d s_d(\alpha_1, \dots, \alpha_d)$$

By The Fundamental Theorem of Symmetric Functions, there is a unique polynomial $Q(x) \in K[x]$ such that $Q(s_1, \dots, s_d) = \Delta(x_1, \dots, x_d)$. Thus,

$$\Delta(\alpha_1, \dots, \alpha_n) = Q(-a_{d-1}, a_{d-2}, \dots, (-1)^d a_0)$$

As this function depends only on $P(x)$ and lies in K, we are done.

(iv) Consider $\delta(\alpha_1, \dots, \alpha_n) := \prod_{i<j}(\alpha_i - \alpha_j)$. For any $\gamma \in \mathrm{Aut}_K(L)$, we have

$$\gamma(\delta(\alpha_1, \dots, \alpha_n)) = \delta(\gamma(\alpha_1), \dots, \gamma(\alpha_n)) = \delta(\alpha_{\phi(\gamma)(1)}, \dots, \alpha_{\phi(\gamma)(n)}) = \mathrm{sign}(\phi(\gamma)) \cdot \delta(\alpha_1, \dots, \alpha_n)$$

As this is a Galois extension, $\delta(\alpha_1, \dots, \alpha_n) \in K$ if and only if the image of ϕ lies in A_n. Now also note that $\delta(\alpha_1, \dots, \alpha_n) \in K$ if and only if $\Delta_P \in (K^*)^2$.

Note the characteristic being non-two is necessary to distinguish between sign, as else $\delta(\alpha_1, \dots, \alpha_n)$ always lies in K.

□

Remark 9.6.12. The key idea is that the Galois group of the splitting field of a degree n polynomial is a subgroup of S_n. Moreover, if $P(x)$ is irreducible, then it is transitive. If n is prime, then this means it contains an n-cycle (though not generally, as V_4 is transitive on $\{1, 2, 3, 4\}$).

The last case is useful to note for when we consider $\text{Gal}(M|K(\sqrt{\Delta_P}))$.

Example 9.6.13. Note that

$$\Delta(x_1, x_2, x_3) = -4s_1^3 s_3 + s_1^2 s_2^2 + 18 s_1 s_2 s_3 - 4s_2^3 - 27s_3^2$$

Taking $P(x) = x^3 - x - \frac{1}{3}$, The polynomial has no roots in $\mathbb{Q}$ (moving it to $\mathbb{Z}[x]$ and seeing it has no roots in $\mathbb{F}_2[x]$), thus irreducible. It also has no multiple roots as the characteristic of $\mathbb{Q}$ is 0.

Let $L|\mathbb{Q}$ be a splitting field for $P(x)$ and take $\alpha_1, \alpha_2, \alpha_3$ to be the roots of $P(x)$ in L. Matching coefficients, $s_3(\alpha_1, \alpha_2, \alpha_3) = -1/3, s_2(\alpha_1, \alpha_2, \alpha_3) = -1, s_1(\alpha_1, \alpha_2, \alpha_3) = 0$, so

$$\Delta_P = -4s_2(\alpha_1, \alpha_2, \alpha_3)^3 - 27s_3(\alpha_1, \alpha_2, \alpha_3)^2 = 4 - \frac{27}{9} = 1$$

In particular, $\Delta_P \in (\mathbb{Q}^*)^2$ (as this is nonzero, it is an alternative way to see it has no repeated roots).

By the previous Lemma, $\text{Gal}(L|\mathbb{Q})$ can be seen as a subgroup of A_3. On the other hand, $\text{Gal}(L|\mathbb{Q})$ has order at least 3 as the extension $K(\alpha_i)|\mathbb{Q}$ has degree 3 for any α_i, as $P(x)$ is irreducible. By the tower law, $\text{Gal}(L|\mathbb{Q})$ has order at least 3, thus $\#A_3 = 3$, giving $\text{Gal}(L|\mathbb{Q}) \simeq A_3$.

Theorem 9.6.14 (Primitive Element Theorem)**.** *Let $L|K$ be a finite separable extension of fields. Then there is an element $\alpha \in L$ such that $L = K(\alpha)$*

Proof. We prove the case for K being finite and infinite separately.

In the finite case, we have $K \simeq \mathbb{F}_{p^n}$ for some prime p and positive integer n. Define $G_d := \{x \mid \text{ord}(x) = d\} \subseteq \{x^d = 1\} \subseteq \mathbb{F}_{p_n}^*$. By definition, if $G_d \neq \emptyset, |G_d| = \phi(d)$ and if $G_d = \emptyset, |G_d| = 0$. Now, we have

$$\begin{aligned} p^n &= |\mathbb{F}_{p_n}^*| + 1 \\ &= \sum_{d|p^n-1} |G_d| + 1 \\ &= \sum_{d|p^n-1} \phi(d) + 1 \\ &= (p^n - 1) + 1 = p^n \end{aligned}$$

In particular, G_{p^n-1} is nonempty, thus we have a generator for the field (that is irrespective of the base field).

If K is an infinite field, noting that L is generated over K by a finite number of elements, induction shows that it is sufficient to prove that L is generated by one element if it is generated by two elements. Suppose that $L = K(\beta, \gamma)$. For $d \in K$, consider the intermediate field $K(\beta + d\gamma)$. As there are finitely many such, and as K is infinite, we can find $d_1, d_2 \in K$ such that $d_1 \neq d_2$ and $K(\beta + d_1\gamma) = K(\beta + d_2\gamma)$. We can find a $P(x) \in K[x]$ such that $\beta + d_1\gamma = P(\beta + d_2\gamma)$, meaning we have

$$\gamma = \frac{P(\beta + d_2\gamma) - (\beta + d_2\gamma)}{d_1 - d_2}$$

and

$$\beta = (\beta + d_2\gamma) - d_2 \frac{P(\beta + d_2\gamma) - (\beta + d_2\gamma)}{d_1 - d_2}$$

and in particular, $K(\beta, \gamma) = K(\beta + d_2\gamma)$. □

Proposition 9.6.15. *Let F be a field of characteristic 0 and let $K = F(\beta, \gamma)$ where β and γ are algebraic over F. Then there exists a d such that $K = F(\beta + c\gamma)$ for some $c \in F$.*

Proof. We give a minimum polynomial argument. Suppose that $\beta + c\gamma$ is not a primitive element, such that $F(\beta + c\gamma) \subsetneq F(\beta, \gamma)$. In particular, $\gamma \notin F(\beta + c\gamma)$. Consider the minimal polynomials of β and γ over $F(\beta + c\gamma)$, calling them $f(X), g(X) \in F(\beta + c\gamma)[X]$, and take a splitting field L containing all roots of $f(X)$ and $g(X)$. Since $\gamma \notin F(\beta + c\gamma)$, there is another root $\gamma' \neq \gamma$ and a field automorphism which fixes $F(\beta + c\gamma)$ and takes $\sigma(\gamma) = \gamma'$. Then,

$$\beta + c\gamma = \sigma(\beta + c\gamma) = \sigma(\beta) + c\sigma(\gamma)$$

implying

$$c = \frac{\sigma(\beta) - \beta}{\gamma - \sigma(\gamma)}$$

As there are only finitely many field automorphisms $\mathrm{Aut}_{F(\beta+c\gamma)}(L)$ (where L is the splitting field), there are only finitely many $c \in F$ that fail to give the primitive element. All other values give $F(\beta + c\gamma) = F(\beta, \gamma)$. □

10 Special Classes of Extensions

10.1 Cyclotomic Extension

Definition 10.1.1. *Let $n \geq 1$. For any field E, define*

$$\mu_n(E) := \{\rho \in E \mid \rho^n = 1\}$$

*The elements of $\mu_n(E)$ are called the **n-th roots of unity**. $\mu_n(E)$ inherits a group structure from E^*.*

Lemma 10.1.2. *The group $\mu_n(E)$ is a finite cyclic group.*

Proof. This group is clearly finite, as there are at most n elements that satisfy $x^d - 1 = 0$ over a field.

Suppose that we have two distinct subgroups H, K of $\mu_n(E)$ of the same cardinality, say d. By Lagrange's Theorem, we have that elements of both H and K are annihalated by $x^d - 1$, but their union has cardinality larger than d. This is a contradiction, thus $\mu_n(E)$ is finite cyclic. □

Definition 10.1.3. *If $\#\mu_n(E) = n$, we call $\omega \in \mu_n(E)$ a **primitive n-th root of unity** if it is a generator of $\mu_n(E)$ (note the initial condition $\#\mu_n(E) = n$).*

Note that if $\omega \in \mu_n(E)$ is a primitive n-th root of unity, all other primitive n-th roots of unity are of the form ω^k where k is an integer coprime to n.

Remark 10.1.4. Let K be a field and suppose that $(n, \mathrm{char}(K)) = (1)$. Let L be a splitting field for the polynomial $x^n - 1 \in K[x]$. We denote this by $K(\mu_n)$ (though abusing language, as L is only well-defined up to non-canonical isomorphism). By construction, $x^n - 1$ has no repeated roots, thus $\#\mu_n(L) = n$ and $L|K$ is a Galois extension. $L|K$ is also a simple extension as L is generated over K by any primitive n-th root of unity in L.

By Lemma 10.1.2, $\mu_n(L) \simeq \mathbb{Z}/n\mathbb{Z}$, there are $\#(\mathbb{Z}/n\mathbb{Z})^* = \Phi(n)$ primitive n-th roots of unity in L.

Definition 10.1.5. *Define*

$$\Phi_{n,K}(x) := \prod_{\omega \in \mu_n(L), \omega \text{ primitive}} (x - \omega)$$

Note that $\deg(\Phi_{n,K}(x)) = \Phi(n)$.

Lemma 10.1.6. *The polynomial $\Phi_{n,K}(x)$ has coefficients in K and depends only on n and K (does not depend on the choice of splitting field).*

Proof. The coefficients of $\Phi_{n,K}(x)$ are symmetric functions in the primitive n-th roots. As these roots are permuted by $\mathrm{Gal}(L|K)$, the coefficients are invariant under $\mathrm{Gal}(L|K)$, and thus lie in K.

The polynomial $\Phi_{n,K}(x)$ only depends on n and K (and not on the choice of extension), as all the splitting K-extensions for $x^n - 1$ are isomorphic. □

Proposition 10.1.7. *There is a natural injection of groups $\phi : \mathrm{Gal}(L|K) \hookrightarrow \mathrm{Aut}_{\mathrm{Groups}}(\mu_n(L)) \simeq (\mathbb{Z}/n\mathbb{Z})^*$. This map is surjective if and only if $\Phi_{n,K}(x)$ is irreducible over K.*

Proof. The first statement is straightforward, noting that $\mu_n(L)$ generates L and $\mathrm{Gal}(L|K)$ acts on L by ring automorphisms.

Let $\omega \in \mu_n(L)$ be a primitive n-th root of unity. Suppose that $\Phi_{n,K}(x)$ is irreducible over K. Since $\Phi_{n,K}(x)$ annihalates ω, it is the minimal polynomial of ω. In particular, $[L : K] \geq \Phi(n)$, and thus $\#\mathrm{Gal}(L|K) \geq \Phi(n)$. On the other hand, we have an injection from $\mathrm{Gal}(L|K) \hookrightarrow (\mathbb{Z}/n\mathbb{Z})^*$, giving $\#\mathrm{Gal}(L|K) \leq \Phi(n)$. Thus $\#\mathrm{Gal}(L|K) = \Phi(n)$, and by injectivity of this map, ϕ is also surjective.

Conversely, if ϕ is surjective, then the minimal polynomial of ω is $\Phi_{n,K}(x)$ by Lemma 7.0.2 and Lemma 9.6.10. □

Proposition 10.1.8. *The polynomial $\Phi_{n,\mathbb{Q}}(x)$ is irreducible and has coefficients in $\mathbb{Z}$.*

Proof. Let L be a splitting field of $x^n - 1 \in \mathbb{Q}[x]$. Let $\omega \in L$ be a primitive n-th root of unity. Let $Q(x)$ be the minimal polynomial of ω over $\mathbb{Q}$. Then $Q(x)|x^n - 1$, thus we can find a polynomial $T(x) \in \mathbb{Q}[x]$ such that $Q(x)T(x) = x^n - 1$. Note that $T(x)$ and $Q(x)$ are monic. Thus $1/c(T)$ and $1/c(Q)$ are both positive integers. On the other hand, $c(x^n - 1) = 1$, and noting that $1 = c(T)c(Q)$, we see that $c(T) = c(Q) = 1$. In particular, $Q(x)$ and $T(x)$ have coefficients in $\mathbb{Z}$.

Fix a prime number p which is coprime to n. We claim that $Q(\omega^p) = 0$. Else, we have $T(\omega^p) = 0$, as $Q(x)T(x) = x^n - 1$. In particular ω is a root of $T(x^p)$. Thus $Q(x)|T(x^p)$. In particular, we have some $H(x)$ such that $Q(x)H(x) = T(x^p)$, where $H(x)$ is also monic. Repeating the same logic as before, $H(x) \in \mathbb{Z}[x]$.

Now,

$$T(x^p)(\text{mod } p) = (T(x)(\text{mod } p))^p$$

in $\mathbb{F}_p[x]$ as the p-power function is additive in $\mathbb{F}_p[x]$. In particular, from $Q(x)H(x) = T(x^p)$, we see that $(Q(x)(\text{mod } p), T(x)(\text{mod } p)) \neq (1)$. Define $J(x) := \gcd(Q(x)(\text{mod } p), T(x)(\text{mod } p))$. Then, $J(x)^2|x^n - 1(\text{mod } p)$, and in particular $x^n - 1(\text{mod } p)$ has multiple roots, which is a contradiction. Thus $Q(\omega^p) = 0$.

Generally, $Q(\omega^k) = 0$ for k coprime to n. Thus, all primitive n-th roots of unity are roots of $Q(x)$. We see that $\deg(Q) \geq \Phi(n)$. By definition, $Q(x)|\Phi_{n,\mathbb{Q}}(x)$, so we have $Q(x) = \Phi_{n,\mathbb{Q}}(x)$. In particular, $\Phi_{n,\mathbb{Q}}(x)$ is irreducible with coefficients in $\mathbb{Z}$.

□

Example 10.1.9. Let $p > 2$ be prime and $\zeta_p := \exp(2\pi i/p)$. Let $K = \mathbb{Q}(\zeta_p)$. The cyclotomic polynomial is

$$f(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + \cdots + x + 1 = \Phi_{p,\mathbb{Q}}(x) = \prod_{i=1}^{p-i}(x - \zeta^i)$$

is by the previous proposition and by Gauss's Lemma irreducible in $\mathbb{Q}[x]$.

In particular $[K : \mathbb{Q}] = p - 1$. So a regular p-gon can be constructed with a ruler and compass only if $p - 1$ is a power of 2 (such as 17).

10.2 Kummer Extension

Definition 10.2.1. *Let K be a field and n be a positive integer with $(n, \mathrm{char}(K)) = (1)$. Suppose that $x^n - 1$ splits in K. Let $a \in K$ and let $M|K$ be a splitting extension for the polynomial $x^n - a$. We call such extension a **Kummer extension***

Note that by construction, $x^n - a$ is a separable polynomial. In particular, $M|K$ is a Galois extension.

Lemma 10.2.2. *Let $M|K$ be a Kummer extension. Let $\rho \in M$ be such that $\rho^n = a$. There is a unique homomorphism $\phi : \mathrm{Gal}(M|K) \to \mu_n(K)$ such that $\phi(\gamma) = \gamma(\rho)/\rho$. The map does not depend on the choice of ρ and is injective.*

Proof. First, $(\gamma(\rho)/\rho)^n = \gamma(\rho^n)/\rho^n = a/a = 1$, so in particular $\gamma(\rho)/\rho \in \mu_n(K)$, giving a well-defined map. Uniqueness follows from the fact the map is defined on all γ.

To see this map does not depend on the choice of ρ, if we have $\rho_1^n = a$, then note that $(\rho/\rho_1)^n = a/a = 1$. Thus, there is an n-th root of unity $\mu \in K$ such that $\mu = \rho/\rho_1$ as $x^n - 1$ splits in K. Now,

$$\gamma(\rho)/\rho = \mu\gamma(\rho)/(\mu\rho) = \gamma(\mu\rho)/(\mu\rho) = \gamma(\rho_1)/\rho_1$$

So ϕ does not depend on ρ.

To see that ϕ is a group homomorphism, for any $\gamma, \lambda \in \mathrm{Gal}(M|K)$, we have

$$\phi(\gamma\lambda) = \gamma(\lambda(\rho))/\rho$$

and

$$\phi(\gamma)\phi(\lambda) = (\gamma(\rho)/\rho)(\lambda(\rho)/\rho)$$

thus it suffices to show

$$\gamma(\lambda(\rho)) = \lambda(\rho)\gamma(\rho)/\rho$$

but this follows immediately from the fact $x^n - 1$ splits in K;

$$\lambda(\rho)/\rho = \gamma(\lambda(\rho)/\rho) = \gamma(\lambda(\rho))/\gamma(\rho)$$

Finally ϕ is injective, as if $\phi(\gamma) = 1$, as γ fixes ρ, it fixes any root of $x^n - a$ and hence $\gamma = 1$. □

Remark 10.2.3. Note that from the above proof, $\mathrm{Gal}(M|K)$ is cyclic. Let it be isomorphic to C_d, and pick a generator σ. In particular, taking any root ρ of $x^n - a$, $\sigma(\rho) = \zeta\rho$ for some ζ with order d. σ^i generate distinct images and by dimension argument, we can see that in fact $M|K$ is a simple extension, generated by any root of $x^n - a$.

Definition 10.2.4. *Let E be a field. Let H be a group. A **character** of H is a group homomorphism $H \to E^*$.*

Proposition 10.2.5 (Dedekind)**.** *Let $\chi_1, \dots, \chi_k$ be distinct characters of H with values in E^*. Let $a_1, \dots, a_k \in E$ be such that*

$$a_1\chi_1(h) + \cdots + a_k\chi(h) = 0$$

for all $h \in H$. Then $a_1 = \cdots = a_k = 0$.

Proof. We proceed by induction on k. The result is immediate for $k = 1$. Suppose $k \geq 2$ and the proposition holds for any smaller parameter. If a_i all vanish, we are done. Else, up to reordering, without loss of generality, suppose that $a_2 \neq 0$.

Pick $\alpha \in H$ such that $\chi_1(\alpha) \neq \chi_2(\alpha)$. Now for any $\beta \in H$, we have

$$\sum_{i=1}^{k} a_i\chi_i(\alpha\beta) = \sum_{i=1}^{k} a_i\chi_i(\alpha)\chi_i(\beta) = 0$$

And

$$\chi_1(\alpha)\sum_{i=1}^{k} a_i\chi_i(\beta) = \sum_{i=1}^{k} a_1\chi_1(\alpha)\chi_i(\beta)$$

Subtracting,

$$\sum_{i=2}^{k} a_i(\chi_i(\alpha) - \chi_1(\alpha))\chi_i(\beta) = 0$$

As this holds for any $\beta \in H$, we have from the inductive hypothesis that $a_2 = 0$, a contradiction. □

Theorem 10.2.6. *Let K be a field and n be a positive integer with $(n, \mathrm{char}(K)) = (1)$. Suppose that $x^n - 1$ splits in K. Suppose also that $L|K$ is a Galois extension and that* Gal$(L|K)$ *is a cyclic group of order n.*

Now let $\sigma \in$ Gal$(L|K)$ *be a generator of* Gal$(L|K)$ *and $\omega \in K$ is a primitive n-th root of unity in K. For any $\alpha \in L$, let*

$$\beta(\alpha) := \alpha + \omega\sigma(\alpha) + \omega^2\sigma^2(\alpha) + \cdots + \omega^{n-1}\sigma^{n-1}(\alpha)$$

Then,

- *For any $\alpha \in L$, $\beta(\alpha)^n \in K$*
- *There is an $\alpha \in L$ such that $\beta(\alpha) \neq 0$.*
- *If $\beta(\alpha) \neq 0$, then $L = K(\beta(\alpha))$ (such that L is the splitting field of $x^n - \beta(\alpha)^n$)*

Proof. Let $\alpha \in L$. Compute

$$\sigma(\beta(\alpha)) = \sigma(\alpha) + \omega\sigma^2(\alpha) + \omega^2\sigma^3(\alpha) + \cdots + \omega^{n-1}\alpha = \omega^{n-1}\beta(\alpha) = \omega^{-1}\beta(\alpha)$$

In particular, $\sigma^i(\beta(\alpha)) = \omega^{-i}\beta(\alpha)$ Furthermore, we have

$$\sigma(\beta(\alpha)^n) = \sigma(\beta(\alpha))^n = \omega^{-n}\beta(\alpha)^n = \beta(\alpha)^n$$

As $L|K$ is Galois, we have $\beta(\alpha)^n \in K$. Note that any element of Gal$(L|K)$ defines a character on L^* with values in L^*. By Dedekind, there is some α such that $\beta(\alpha) \neq 0$. As $\omega^{-i}\beta(\alpha)$ are roots of $x^n - \beta(\alpha)^n$, it splits in L.

Now, Gal$(L|K)$ acts transitively and faithfully (the only element in Gal$(L|K)$ that fixes all the roots is the identity) on the roots of $x^n - (\beta(\alpha))^n$. In particular, $x^n - \beta(\alpha)^n$ is irreducible over K. Thus $[K(\beta(\alpha)) : K] = n = [L : K]$, which from the tower law, we conclude $K(\beta(\alpha)) = L$. Thus L is a splitting field for $x^n - \beta(\alpha)^n$.

□

10.3 Radical Extension

Definition 10.3.1. *The field extension $L|K$ is said to be* ***radical*** *if $L = K(\alpha_1, \dots, \alpha_k)$ and there are natural numbers $n_1, \dots, n_k$ such that $\alpha_1^{n_1} \in K, \alpha_2^{n_2} \in K(\alpha_1), \dots, \alpha_k^{n_k} \in K(\alpha_1, \dots, \alpha_{k-1})$.*

By definition, if $L|K$ and $M|L$ are radical extensions, $M|K$ is a radical extension.

Example 10.3.2. Kummer extensions are radical. This is an immediate consequence of the fact Kummer extensions $L|K$ are simple extensions generated by any root of $x^n - a$ for $a \in K$.

Lemma 10.3.3. *Let $L|K$ be a radical extension and let $J|L$ be a finite extension such that the composed extension $J|K$ is a Galois extension. Then there is a field L' which is intermediate between J and L such that $L'|K$ is Galois and radical.*

Proof. Suppose that $L = K(\alpha_1, \dots, \alpha_k)$ and that we have natural numbers $n_1, \dots, n_k$ such that $\alpha_1^{n_1} \in K, \alpha_2^{n_2} \in K(\alpha_1), \dots, \alpha_k^{n_k} \in K(\alpha_1, \dots, \alpha_{k-1})$. Let $G := \mathrm{Gal}(J|K) = \{\sigma_1, \dots, \sigma_t\}$. Then for any $i \in \{1, \dots, k\}$ and $\sigma \in G$, we have

$$\sigma(\alpha_i^{n_i}) = \sigma(\alpha_i)^{n_i} \in \sigma(K(\alpha_1, \dots, \alpha_{i-1})) = K(\sigma(\alpha_1), \dots, \sigma(\alpha_{i-1}))$$

In particular,

$$K(\alpha_1, \dots, \alpha_k, \sigma_1(\alpha_1), \dots, \sigma_1(\alpha_k), \dots, \sigma_t(\alpha_1), \dots, \sigma_t(\alpha_k)) = K(\mathrm{Orb}(\alpha_1), \dots, \mathrm{Orb}(\alpha_k))$$

is a radical extension of K. Now, given $\sigma \in G$, we have

$$\sigma(K(\mathrm{Orb}(\alpha_1), \dots, \mathrm{Orb}(\alpha_k))) = K(\sigma(\mathrm{Orb}(\alpha_1)), \dots, \sigma(\mathrm{Orb}(\alpha_k))) = K(\mathrm{Orb}(\alpha_1), \dots, \mathrm{Orb}(\alpha_k))$$

we see that $K(\mathrm{Orb}(\alpha_1), \dots, \mathrm{Orb}(\alpha_k))|K$ is a Galois extension (field fixed by Galois group actions). Thus we may set $L' := K(\mathrm{Orb}(\alpha_1), \dots, \mathrm{Orb}(\alpha_k))$.

$$\begin{tikzcd}
K \arrow[r, hook] \arrow[rr, hook, bend left] \arrow[dr, hook] & L = K(\alpha_1, \dots, \alpha_k) \arrow[r, hook] \arrow[d, hook] & J \\
& L' = K(\mathrm{Orb}(\alpha_1), \dots, \mathrm{Orb}(\alpha_k)) \arrow[ur, hook] &
\end{tikzcd}$$

□

10.3.1 Solvability by Radical Extensions

Theorem 10.3.4. *Suppose that* $\mathrm{char}(K) = 0$. *Let $L|K$ be a finite Galois extension.*

If $\mathrm{Gal}(L|K)$ *is solvable, then there exists a finite extension $M|L$ with the following properties*

1. *The composed extension $M|K$ is Galois*

2. *There is a map of K-extensions $K(\mu_{[L:K]}) \hookrightarrow M$*

3. *M is generated by the images of L and $K(\mu_{[L:K]})$ in M.*

4. *The extension $M|K(\mu_{[L:K]})$ is a composition of Kummer extensions. In particular, $M|K$ is a radical extension.*

Conversely, if there exists a finite extension $M|L$ such that the composed extension $M|K$ is radical, then $\mathrm{Gal}(L|K)$ *is solvable.*

Proof. First note that the images of L and $K(\mu_c)$ in M do not depend on the maps of K-extensions $L \hookrightarrow M$ and $K(\mu_{[L:K]}) \hookrightarrow M$ as the two are both galois extensions.

Let $d := \#\mathrm{Gal}(L|K) = [L : K]$. There is a Galois extension of K and maps of K extensions $K(\mu_d) \hookrightarrow J$ and $L \hookrightarrow J$ by the existence of splitting extensions and Lemma 9.5.3. Choose such an extension and maps of K-extensions. Now, let P be the field generated by L and $K(\mu_d)$ in J. Then we have

$$\begin{tikzcd}
& J & \\
& P \arrow[u, hook] & \\
L \arrow[ur, hook] & & K(\mu_d) \arrow[ul, hook'] \\
& K \arrow[ul, hook'] \arrow[ur, hook] &
\end{tikzcd}$$

Let $G := \mathrm{Gal}(J|K)$. We can observe the following:

1. $P|K$ is a Galois extension, as it is fixed by any $\sigma \in G$ (as the fields they are generated by are Galois)

2. $P|K(\mu_d)$ is Galois by lifting from K.

3. The restriction map $\mathrm{Gal}(P|K(\mu_d)) \to \mathrm{Gal}(L|K)$ is injective. If $\sigma \in \mathrm{Gal}(P|K(\mu_d))$ restricts to the identity in L, it fixed both $K(\mu_d)$ and L, thus fixes P.

Suppose now that $\mathrm{Gal}(L|K)$ is solvable. Then, by Lemma 7.1.3 and injectivity of $\mathrm{Gal}(P|K(\mu_d))$ into $\mathrm{Gal}(L|K)$, $\mathrm{Gal}(P|K(\mu_d))$ is solvable. In particular, there is a finite filtration with abelian quotients

$$0 = H_0 \subseteq H_1 \subseteq \cdots \subseteq H_n = \mathrm{Gal}(P|K(\mu_d))$$

By Lemma 7.1.7, we may assume without loss of generality that the quotients of the filtration are cyclic. By the fundamental theorem of Galois Theory, the subgroups H_i correspond to a descreasing sequence of subfields of P

$$P = P_0 \supseteq P_1 \supseteq \cdots \supseteq P_n = K(\mu_d)$$

such that $P_i|P_{i+1}$ is a Galois extension for any i. Also,

$$H_{i+1}/H_i \simeq \mathrm{Gal}(P|P_i)/\mathrm{Gal}(P|P_{i+1}) \simeq \mathrm{Gal}(P_i|P_{i+1})$$

such that $\mathrm{Gal}(P_i|P_{i+1})$ is cyclic. By Lagrange's Theorem (applied repeatedly) $\#(H_{i+1}/H_i)$ is a divisor of $\#\mathrm{Gal}(P|K(\mu_d))$ and thus of $\#\mathrm{Gal}(L|K) = d$. In particular, $x^{\#\mathrm{Gal}(P_i|P_{i+1})} - 1$ splits in $K(\mu_d)$, and so in P_{i+1}. By Theorem 10.2.6, $P_i|P_{i+1}$ is a Kummer extension, thus a radical extension. Setting $M := P$, we have shown this satisfies all our mentioned properties.

To prove the other direction, suppose that we have a finite extension $M|L$ such that the composed extension $M|K$ is radical. We may thus suppose that $M = K(\alpha_1, \ldots, \alpha_k)$ and there are $n_1, \ldots, n_k$ such that $\alpha_1^{n_1} \in K, \ldots, \alpha_k^{n_k} \in K(\alpha_1, \ldots, \alpha_{k-1})$. Let $t := \prod_{i=1}^{k} n_i$. Choose a Galois extension $J|K$

such that there are maps of K-extensions $M \hookrightarrow J$ and $K(\mu_t) \hookrightarrow J$. Fixing maps, let E be the intermediate field generated by M and $K(\mu_t)$ in J. Thus, we have a diagram of extensions

$$\begin{tikzcd}
 & J & \\
 & E \arrow[u, hook] & \\
M \arrow[ur, hook] & & K(\mu_t) \arrow[ul, hook] \\
L \arrow[u, hook] & & K \arrow[u, hook] \arrow[ll, hook']
\end{tikzcd}$$

By definition, $E = K(\mu_t)(\alpha_1, \ldots, \alpha_k)$, and by construction each $K(\mu_t)(\alpha_1, \ldots, \alpha_{i+1})|K(\mu_t)(\alpha_1, \ldots, \alpha_i)$ is a Kummer extension, as $n_i|t$. In particular, the Galois group is abelian. Now $\mathrm{Gal}(K(\mu_t)|K)$ is abelian also. By the Fundamental Theorem for Galois groups, we see that $\mathrm{Gal}(E|K)$ is solvable. Finally, as $\mathrm{Gal}(L|K)$ is a quotient of $\mathrm{Gal}(E|K)$, $\mathrm{Gal}(L|K)$ is solvable. □

Definition 10.3.5. *Let $P(x) \in K[x]$ and let $L|K$ be a splitting extension for $P(x)$. We say $P(x)$ is **solvable by radicals** if there is an extension $M|L$ such that the composed extension $M|K$ is radical (as the splitting extensions are isomorphic, the choice does not matter). By the previous theorem, $P(x)$ is solvable by radicals if and only if* $\mathrm{Gal}(L|K)$ *is solvable.*

Corollary 10.3.6. *Let $n \geq 5$ and K be a field. The extension $K(x_1, \ldots, x_n)|K(x_1, \ldots, x_n)^{S_n}$ is not radical. (Note the action is induced by the action of S_n on $K[x_1, \ldots, x_n]$)*

Proof. By Artin's Lemma, $K(x_1, \ldots, x_n)|K(x_1, \ldots, x_n)^{S_n}$ is a Galois extension. On the other hand, S_n is not solvable for $n \geq 5$, so by Theorem 10.3.4, is not radical. □

Remark 10.3.7. To see $K(x_1, \ldots, x_n)|K(x_1, \ldots, x_n)^{S_n}$ is a Galois extension directly, note that it is the splitting field of the polynomial

$$U_n(x) = x^n - s_1(x_1, \ldots, x_n)x^{n-1} + \cdots + (-1)^n s_n(x_1, \ldots, x_n) \in K(x_1, \ldots, x_n)^{S_n}[x]$$

And the roots are $x_1, \ldots, x_n$ generate the field.

Example 10.3.8 (Solution to the General Cubic Equation)**.** Let K be a field and suppose that $\mathrm{char}(K) = 0$. We wish to solve the cubical equation

$$y^3 + ay^2 + by + c = 0$$

where $a, b, c \in K$. Letting $x = y + \frac{a}{3}$, we see that this is equivalent to solving

$$x^3 + px + q = 0$$

where $p = -\frac{1}{3}a^2 + b$ and $q = \frac{2}{27}a^3 - \frac{1}{3}ab + c$. So let $P(x) = x^3 + px + q$. We wish to find a solution that starts with p, q and iteratively applies multiplication, addition, multiplication by K, extraction of 2nd and 3rd roots.

Let $L|K$ be a splitting extension for $P(x)$. Let $\omega \in K(\mu_3)$ ne a primitive 3rd root of unity. Now by Lemma 9.5.3 we can choose a finite Galois extension $J|K$ and maps of K extensions $L \hookrightarrow J$ and

$K(\mu_3) = K(\omega) \hookrightarrow J$. Let $M = L(\omega)$ be the field generated in J by the images of L and $K(\omega)$ in J. So we have the following

$$\begin{tikzcd}
& M = L(\omega) & \\
L \arrow[ur, hook] & & K(\mu_3) = K(\omega) \arrow[ul, hook'] \\
& K \arrow[ul, hook'] \arrow[ur, hook] &
\end{tikzcd}$$

Now note that $\mathrm{Gal}(L|K)$ is solvable as it injects into S_3, and thus $M|K$ is radical by Theorem 10.3.4 (from which we should be able to retrieve an expression for ω).

Consider the sequence of extensions

$$K \hookrightarrow K(\omega) \hookrightarrow K(\omega, \sqrt{\Delta_P}) \hookrightarrow M$$

As the square root of Δ_P is a polynomial in the roots of $P(x)$, it lies in L.

Now note that

11 Main Ideas in GT - No definitions

The concept of multiple roots (on $P(x) \in K[x]$) is invariant under

- field extension. (Pf. ED algorithm is unique in computing a generator)
- polynomials $Q(x)$ such that $Q(x)|P(x)$

The gcd of P, Q is the generator of (P, Q)

If $P' \neq 0$ and P is irreducible, it has no multiple roots.

Extension of maps :

$$\begin{tikzcd}
K \arrow[r, hook] \arrow[d] & L \\
K(\alpha) \arrow[ur, hook, dashed] &
\end{tikzcd}$$

is determined by sending α to the roots of m_α in L, where m_α is the minimal polynomial of α with coefficients in K. So the cardinality of maps is the number of roots of m_α in L. This is a consequence of the fact $K(\alpha) \simeq K[x]/m_\alpha$.

- composition of normal extensions need not be normal, consider $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt[4]{2})$.

11.1 Relating Field Extensions

- Splitting fields exist for any polynomial

$$\begin{tikzcd}
K \arrow[r, hook, "\exists s_P"] & M
\end{tikzcd}$$

- Lemma 10.3.3: If $L|K$ is a radical extension and $J|L$ is a finite extension such that $J|K$ is a Galois extension, there is an intermediate field L' between J and L such that $L'|K$ is Galois and radical

$$\begin{tikzcd}
K \arrow[r, hook, "r"] \arrow[rr, hook, bend left, "g"] \arrow[dr, hook] & L = K(\alpha_1, \dots, \alpha_k) \arrow[r, hook] \arrow[d, hook, "r"] & J \\
& L' = K(\mathrm{Orb}(\alpha_1), \dots, \mathrm{Orb}(\alpha_k)) \arrow[ur, hook] &
\end{tikzcd}$$

11.2 Examples of Galois Extensions

Example 11.2.1. Consider $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ as a field extension over $\mathbb{Q}$. K is the splitting field over the separable polynomial $(x^2-2)(x^2-3)$, thus is Galois. Field automorphisms must send each generator to their conjugates, so our choice is

$$\sqrt{2} \mapsto \pm\sqrt{2} \qquad \sqrt{3} \mapsto \pm\sqrt{3}$$

giving $G = \mathrm{Gal}(K|\mathbb{Q}) \simeq C_2 \times C_2$. By Galois correspondence, the nontrivial subgroups give intermediate fields, where the correspondence is given by K^H where $H \subseteq G$. Taking the subgroup that flips $\sqrt{2}$, we have

$$K^{H_2} = \{a + c\sqrt{3} \mid a, c \in \mathbb{Q}\} = \mathbb{Q}(\sqrt{3})$$

and similarly with H_3. The map that flips $\sqrt{2}$ and $\sqrt{3}$ would be

$$K^{H_{2,3}} = \{a + \sqrt{d} \mid a, d \in \mathbb{Q}\} = \mathbb{Q}(\sqrt{6})$$

We also give an example of a Kummer extension.

Example 11.2.2. Let $K = \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$ where $\zeta_3 = e^{2\pi i/3}$. This is the splitting field over the separable polynomial $x^3 - 2$. The galois group is generated by choices of maps

$$\sqrt[3]{2} \mapsto \zeta_3^k \sqrt[3]{2}, k = 0, 1, 2 \qquad \zeta_3 \mapsto \zeta_3^{\pm 1}$$

Now note that $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ and $[\mathbb{Q}(\zeta) : \mathbb{Q}] = 2$, and as $\zeta \notin \mathbb{Q}(\alpha)$,$[K : \mathbb{Q}] = 6$ by the tower law. In particular $|G| = 6$, and we can check via relations that this is S_3. The proper subfields correspond to the subgroups of S_3 which correspond to subfields $\mathbb{Q}(\zeta_3), \mathbb{Q}(\sqrt[3]{2}), \mathbb{Q}(\zeta_3\sqrt[3]{2}), \mathbb{Q}(\zeta_3^2\sqrt[3]{2})$.

Example 11.2.3. Taking $K = \mathbb{Q}(\zeta_5)$ where $\zeta_5 = e^{2\pi i/5}$. This is a cyclotomic field which has Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta_5)|\mathbb{Q}) \simeq (\mathbb{Z}/5\mathbb{Z})^\times \simeq C_4$. C_4 has exactly one nontrivial subgroup of order 2, whose automorphism set is $\{\mathrm{id}, \sigma^2\}$. As σ^2 sends ζ_5 to $\zeta_5^4 = \zeta_5^{-1}$, it fixes $\zeta_5 + \zeta_5^{-1}$ whose minimum polynomial is $x^2 + x - 1$.

Remark 11.2.4. The above give rise to a variety of examples $[K : F]$ such that $K|F$ is Galois but there are intermediate fields $F \subsetneq L \subsetneq K$ such that $L|F$ is not Galois. For instance, take $F = \mathbb{Q}$ and $L = \mathbb{Q}(\sqrt[3]{2})$, $K = \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$.

Example 11.2.5. Let $f := t^4 - 4t^2 + 2$ and $\alpha \in \mathbb{C}$ be a root of f. Then $\mathbb{Q}(\alpha)$ is the splitting field of f, by noting how the roots relate to each other. Also, we have the tower of extensions

$$\mathbb{Q} \subsetneq \mathbb{Q}(\sqrt{2}) \subsetneq \mathbb{Q}(\alpha)$$

which shows the extension has degree 4. Explicit mappings of roots shows that $\mathrm{Gal}(\mathbb{Q}(\alpha)|\mathbb{Q}) \simeq C_4$.

11.3 Important Things to Keep in Mind

- Splitting extensions always exist (induction by repeatedly quotienting by irreducible factors of P, and noting this always produces roots)
- Splitting extensions are (non-canonically) isomorphic as K-extensions (induction with quotienting with a min-poly of a root of P)
- Extensions from splitting fields preserve image (because any automorphism only permutes roots)
- Number of injections from simple extensions $K(\alpha)$ to J depends on root presense (of minpoly) in J (bijective correspondence).
- Taking $K(\alpha_1, \ldots, \alpha_k)$, there is a nonempty/finite number of injections to fields where the product of the minpoly split. By bijective correspondence, there are 'tower' many ($[M : K]$ many) when the minpolys separate.
- Normal iff splitting extension for poly with coefficients in K ($\Rightarrow$, consider product of minpoly of generators, $\Leftarrow$, pick any $\alpha \in L$, extend to splitting field of prod of minpoly, induce map λ from L to splitter, by image invariance $\lambda(L)$ contains all roots of α, splits.)
- Galois correspondence with intermediate fields and raising base fields, use Artin with identity ($\mathrm{Gal}(K|K^G) = G$), inverse given by $H \mapsto L^H$
- Lowering to subfield from L to M only works if $\mathrm{Gal}(L|M)$ is a normal subgroup of $\mathrm{Gal}(L|K)$ (use FIT, image fixing of M by $\gamma \in \mathrm{Gal}(L|K)$, kernel argument) (reverse, navigate through to show $\mathrm{Gal}(L|\gamma(M)) = \mathrm{Gal}(L|M)$, which implies $M = \gamma(M)$ by FTGT) (image invariance lets us define maps about M) ($\mathrm{Gal}(L|K)/\mathrm{Gal}(L|M) \simeq \mathrm{Gal}(M|K)$).
- $\uparrow$ also lets us lower galois field by image invariance
- Kummer has cyclic Galois group (injects into roots of unity) (injective by root fixing argument)

- adding ideals, coprime (sums to entire ring)
Some background lemmas :

- Gauss's Lemma (irreducible in $\mathbb{Z}[t]$ implies irreducible in $\mathbb{Q}[t]$), content function to show there exists $\lambda \neq 0$ such that λg, $\lambda^{-1}h \in \mathbb{Z}[t]$.
- Eisenstein

Definition 11.3.1. *A **number field** or **algebraic number field** is a finite extension K of $\mathbb{Q}$. The index $[K : \mathbb{Q}]$ is the **degree** of the number field.*

Theorem 11.3.2. *If K is a number field, then $K = \mathbb{Q}(\theta)$ for some algebraic number $\theta \in K$.*

Theorem 11.3.3. *Let $K = \mathbb{Q}(\theta)$ be a number field of degree n over $\mathbb{Q}$. Then there are exactly n distinct monomorphisms (embeddings)*

$$\sigma_i : K \to \mathbb{C}$$

The elements $\sigma_i(\theta)$ are the distinct zeros in $\mathbb{C}$ of the minimal polynomial m_θ of θ over $\mathbb{Q}$.

Definition 11.3.4. *If $\sigma_i(K) \subseteq \mathbb{R}$, then σ_i is called a **real embedding**, otherwise it is called a **complex embedding**.*

Definition 11.3.5. *A square matrix over $\mathbb{Z}$ is called* ***unimodular*** *if it has determinant ± 1.*

Note that A is unimodular if and only if A^{-1} has coefficients in $\mathbb{Z}$. (Proof sketch, by considering what EROs transform A into an identity.)

Lemma 11.3.6. *Let G be a free abelian group of rank n with $\mathbb{Z}$-basis $\{x_1, \dots, x_n\}$. Suppose (a_{ij}) is a square matrix with integer entries. Let*

$$y_i = \sum_j a_{ij} x_j$$

Then the elements $\{y_1, \dots, y_n\}$ form a $\mathbb{Z}$-basis for G if and only if (a_{ij}) is unimodular.

Proof. TODO!! □

Theorem 11.3.7. *Let G be a free abelian group of rank n, and H be a subgroup. Then G/H is finite if and only if H has rank n. Moreover, if G and H have $\mathbb{Z}$-basis $\{x_1, \dots, x_n\}$ and $\{y_1, \dots, y_n\}$ with $y_i = \sum_j a_{ij} x_j$, we have*

$$\# G/H = |\det(a_{ij})|$$

Proof. TODO!!! □

12 Definitions

Definition 12.0.1. *Let $K|\mathbb{Q}$ be an algebraic number field of degree n, and let $\alpha \in K$. Let $\sigma_i : K \to \mathbb{C}$ be the n embeddings. We call $\sigma_i(\alpha)$ the* ***K-conjugates*** *of α.*

We define the ***trace*** *to be $\mathrm{Tr}_{K|\mathbb{Q}}(\alpha) = \sum_{i=1}^n \sigma_i(\alpha)$ and the* ***norm*** *$\mathrm{Norm}_{K|\mathbb{Q}}(\alpha) = N_{K|\mathbb{Q}}(\alpha) = N(\alpha) = \prod_{i=1}^n \sigma_i(\alpha)$. When $K = \mathbb{Q}(\alpha)$, we call these the* ***absolute conjugates, trace,*** *and* ***norm****.*

Proposition 12.0.2. *We record the following properties :*

- *For any $K = \mathbb{Q}(\beta)$, suppose that β has minimal polynomial $m_\beta(X)$. If $\beta_1, \dots, \beta_n$ are the n roots of m_β in $\mathbb{C}$, then one can choose embeddings $\sigma_i : \beta \to \beta_i$.*
- $\mathrm{Norm}_{K|\mathbb{Q}}(\gamma\delta) = \mathrm{Norm}_{K|\mathbb{Q}}(\gamma)\mathrm{Norm}_{K|\mathbb{Q}}(\delta)$
- $\mathrm{Norm}_{K|\mathbb{Q}}(\gamma) = 0$ *if and only if* $\gamma = 0$.
- $\mathrm{Norm}_{K|\mathbb{Q}}(q) = q^n$ *for* $q \in \mathbb{Q}$.
- *If $K = \mathbb{Q}(\alpha)$ and $m_\alpha(X) = X^n + c_{n-1}X^{n-1} + \dots + c_0$, then we have $\mathrm{Norm}_{K|\mathbb{Q}}(\alpha) = (-1)^n c_0$ and $\mathrm{Norm}_{K|\mathbb{Q}}(\alpha) = -c_{n-1}$. In particular, the norm and trace are both in $\mathbb{Q}$. Generally speaking, for any $K = \mathbb{Q}(\beta)$, $\alpha \in K$, the norm and trace of α are symmetric functions of the conjugates of $\sigma_i(\alpha)$, thus in $\mathbb{Q}$.*

Proof. Immediate. The last line follows as a consequence of the Fundamental Theorem on the theory of symmetric functions. □

Definition 12.0.3. *Let $w = \{w_1, \dots, w_n\}$ be a n-tuple of elements of K, where $n = [K : \mathbb{Q}]$.*

- *The* ***determinant*** *is $\Delta(w) := \det(\sigma_i(w_j))$*
- *The* ***discriminant*** *of w is $\Delta(w)^2$*

Lemma 12.0.4. *$\Delta(w)^2 = \det(\mathrm{Tr}_{K|\mathbb{Q}}(w_i w_j))$ and consequently $\Delta(w)^2 \in \mathbb{Q}$.*

Proof. Let $A = (\sigma_i(w_j))$. Then,

$$\begin{aligned}\Delta(w)^2 = \det(A)^2 = \det(A^T A) &= \det\left(\sum_k \sigma_k(w_i)\sigma_k(w_j)\right)\\ &= \det\left(\sum_k \sigma_k(w_i w_j)\right) = \det(\mathrm{Tr}_{K|\mathbb{Q}}(w_i w_j))\end{aligned}$$

□

Lemma 12.0.5. *If $v = \{v_1, \dots, v_n\}$ is a basis for $K|\mathbb{Q}$ and $w = \{w_1, \dots, w_n\} \subseteq K$ with $w_i = \sum_j c_{ij} v_j$ and $c_{ij} \in \mathbb{Q}$, then*

$$\Delta(w) = \det(C)\Delta(v)$$

Proof. Write $A_v = (\sigma_i(v_j))$ and $A_w = (\sigma_i(w_j))$ such that $\Delta(v) = \det(A_v)$ and $\Delta(w) = \det(A_w)$. Now,

$$A_w = (\sigma_i(w_j)) = \left(\sigma_i\left(\sum_k c_{jk} v_k\right)\right) = \left(\sum_k c_{jk}\sigma_i(v_k)\right) = A_v C^T$$

The proof thus follows by taking det on both sides. □

Lemma 12.0.6. *If $K = \mathbb{Q}(\alpha)$ and $v = \{1, \alpha, \dots, \alpha^{n-1}\}$, then*

$$\Delta(v)^2 = \prod_{i<j}(\alpha_j - \alpha_i)^2$$

where α_i are the conjugates of α.

Proof. Note first that

$$\Delta(v) = \begin{vmatrix} 1 & \alpha_1 & \alpha_1^2 & \cdots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \alpha_2^2 & \cdots & \alpha_2^{n-1} \\ \vdots & & & & \vdots \\ 1 & \alpha_n & \alpha_n^2 & \cdots & \alpha_n^{n-1} \end{vmatrix}$$

which is the so-called van der Monde determinant. We note that this is a polynomial of degree $n(n-1)/2$ in $\alpha_1, \dots, \alpha_n$. As it vanishes when we set $\alpha_i = \alpha_j$, the polynomial is divisible by $\alpha_i - \alpha_j$ for all $i < j$. There are $n(n-1)/2$ such factors. By observing the diagonal, the coefficient of $\alpha_2\alpha_3^2 \cdots \alpha_n^{n-1}$ is 1, so we must have

$$\Delta(v) = \prod_{i<j}(\alpha_j - \alpha_i)$$

□

Corollary 12.0.7. *$\Delta(w_1, \dots, w_n) \neq 0$ if and only if $w_1, \dots, w_n$ is a basis for $K|\mathbb{Q}$.*

Proof. Suppose $K = \mathbb{Q}(\alpha)$ and let $v = \{1, \alpha, \dots, \alpha^{n-1}\}$. Noting the previous lemma, as α_i are distinct, we must have $\Delta(v) \neq 0$.

By Lemma 12.0.5, using C as a change of basis, $\Delta(w) \neq 0$ for any other basis w of $K|\mathbb{Q}$. If w is not a basis, then $\det(C) = 0$, giving $\Delta(w) = 0$. □

13 Specific Domains

13.1 Unique Factorization Domain

Definition 13.1.1. *R is a **unique factorisation domain** if R is an integral domain, and for all nonzero and nonunit $\alpha \in R$, there exists irreducible $\beta_1, \dots, \beta_n \in R$ such that*

1. *$\alpha = \beta_1, \dots, \beta_n$*
2. *If $\alpha = \gamma_1, \dots, \gamma_m$ with irreducible γ_i, then $m = n$ and there exists a permutation σ such that β_i and $\gamma_{\sigma(i)}$ are conjugates.*

Proposition 13.1.2. *Suppose that R is an integral domain in which factorisation into irreducibles is possible. Then the following are equivalent*

1. *Factorization is unique*
2. *Irreducible elements are prime*

Proof. Sketch. If the factorisation is unique and we have an irreducible p such that $p|xy$, $pc = xy$, by unique factorisation p is a factor of x or y.

If irreducible elements are prime, for any factorisation $\prod x_i$ and $\prod y_i$, taking x_i divides some y_j by primality, and by irreduciblity shows they are associates. We can inductively show factorisation is unique. □

14 Ring of Integers

14.1 Basic Definitions

Definition 14.1.1. *We say that $\alpha \in K$ is an **algebraic integer** if there exists a monic $g(x) \in \mathbb{Z}[x]$ such that $g(\alpha) = 0$. We define $\mathcal{O}_K$ as the set of all algebraic integers in $\mathcal{O}$.*

Proposition 14.1.2. *Some basic properties :*

- *Suppose $\alpha \in K$. Then $\alpha \in \mathcal{O}_K$ if and only if the minimal polynomial is in $\mathbb{Z}[x]$ by Gauss's lemma.*
- *Pick any $\alpha \in K$ such that there is a monic polynomial $\alpha^d + a_{d-1}\alpha^{d-1} + \cdots + a_0 = 0 \in \mathbb{Q}[x]$. Picking an n, we have*

$$(n\alpha)^d + na_{d-1}(n\alpha)^{d-1} + \cdots + n^d a_0 = 0$$

thus, picking an n to clear the denominators of all a_i, we get $n\alpha \in \mathcal{O}_K$.

- *The minimal polynomial of $r \in \mathbb{Q}$ is $x - r$ which is in $\mathbb{Z}[x]$ if and only if $r \in \mathbb{Z}$. Thus if $K = \mathbb{Q}$, then $\mathcal{O}_K = \mathbb{Z}$. Generally, $\mathbb{Z} \subseteq \mathcal{O}_K$.*

Proof. Immediate. □

Example 14.1.3 ($\mathcal{O}_K$ for $K = \mathbb{Q}(\sqrt{d})$ for $d \in \mathbb{Z}$)**.** Without loss of generality, we assume that $d \neq 1$ and is square-free. First note that $[K : \mathbb{Q}] = 2$, and K has a $\mathbb{Q}$-basis $\{1, \sqrt{d}\}$.

Taking any $a, b \in \mathbb{Q}$, $\alpha = a + b\sqrt{d} \in K$. Noting $\sigma_1(\alpha) = a + b\sqrt{d}$ and $\sigma_2(\alpha) = a - b\sqrt{d}$, we have $\mathrm{Tr}_{K|\mathbb{Q}}(\alpha) = 2a$ and $\mathrm{Norm}_{K|\mathbb{Q}}(\alpha) = a^2 - db^2$. Given $b \neq 0$, we have $m_\alpha(x) = x^2 - 2ax + (a^2 - db^2)$.

Thus $\alpha \in \mathcal{O}_K$ if and only if $2a, a^2 - db^2 \in \mathbb{Z}$. Suppose that $\alpha \in \mathcal{O}_K$. Then $(2a)^2 - d(2b)^2 \in \mathbb{Z}$, giving $d(2b)^2 \in \mathbb{Z}$. Writing $2b = u/v$, we have $du^2v^{-2} \in \mathbb{Z}$, such that $v^2 | du^2$. As d is square free, we have $v|u$, giving $2b \in \mathbb{Z}$. Write $2a = A$ and $2b = B$ with $A, B \in \mathbb{Z}$. Then we have $A^2 \equiv dB^2 \bmod 4$.

Now a case split,

- $d \equiv 2$ or $3 \bmod 4$. Then we must have A, B both even, giving $a, b \in \mathbb{Z}$
- $d \equiv 1 \bmod 4$. Then $A \equiv B \bmod 2$, so a, b are both in $\mathbb{Z}$ or both in $\mathbb{Z} + 1/2$.
- $d \equiv 0 \bmod 4$ does not occur as d is square free

Thus, we have

$$\mathcal{O}_K = \begin{cases} \langle 1, \sqrt{d} \rangle = \{m + n\sqrt{d} \mid m, n \in \mathbb{Z}\} & d \equiv 2, 3 \bmod 4 \\ \langle 1, \frac{1+\sqrt{d}}{2} \rangle = \{m + n\frac{1+\sqrt{d}}{2} \mid m, n \in \mathbb{Z}\} & d \equiv 1 \bmod 4 \end{cases}$$

Lemma 14.1.4. *$\alpha \in K$ is an algebraic integer if and only if there exists a non-zero finitely generated $\mathbb{Z}$-module $M \subseteq K$ such that $\alpha M \subseteq M$.*

Proof. Suppose that $\alpha \in \mathcal{O}_K$ such that $\alpha^d + a_{d-1}\alpha^{d-1} + \cdots + a_0 = 0$ with $a_i \in \mathbb{Z}$. Taking $M = \langle 1, \alpha, \ldots, \alpha^{d-1} \rangle$, we have $\alpha M \subseteq M$.

Conversely, suppose $M \subseteq K$ is a non-zero finitely generated $\mathbb{Z}$-module such that $\alpha M \subseteq M$. Take $w_1, \ldots, w_s$ to be a generating set for M, and write

$$\alpha w_i = \sum_j c_{ij} w_j$$

with $c_{ij} \in \mathbb{Z}$. Taking $C = (c_{ij})$, we have

$$(\alpha I - C) \begin{pmatrix} w_1 \\ w_2 \\ \vdots \\ w_s \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

such that α satisfies $\det(xI - C)$, a monic polynomial with integer coefficients. Thus $\alpha \in \mathcal{O}_K$. □

Theorem 14.1.5. *Let K be an algebraic number field. If $\alpha, \beta \in \mathcal{O}_K$, then $\alpha + \beta$, $\alpha\beta \in \mathcal{O}_K$.*

Proof. Suppose $\alpha, \beta \in \mathcal{O}_K$. By Lemma 14.1.4, we have finitely generated $\mathbb{Z}$-modules M, N such that $\alpha M \subseteq M$ and $\beta N \subseteq N$.

Now, MN is finitely generated, and

$$(\alpha + \beta)MN \subseteq (\alpha M)N + M(\beta N) \subseteq MN$$

$$(\alpha\beta)MN \subseteq (\alpha M)(\beta N) \subseteq MN$$

It follows again from Lemma 14.1.4 that $\alpha + \beta, \alpha\beta \in \mathcal{O}_K$. □

Remark 14.1.6. The above also follows as a direct consequence from the fact given any A that is a subring of B, elements of B that are integral over A form a subring.

Corollary 14.1.7. *If $\alpha \in \mathcal{O}_K$, then $\mathrm{Tr}_{K|\mathbb{Q}}(\alpha), \mathrm{Norm}_{K|\mathbb{Q}}(\alpha) \in \mathbb{Z}$.*

Proof. Let $\alpha \in \mathcal{O}_K$. Then all the $K|\mathbb{Q}$ conjugates $\alpha_1, \dots, \alpha_n$ belong to the splitting field of the minimal polynomial, $\mathcal{O}_L$. Now, $\mathrm{Tr}_{K|\mathbb{Q}}(\alpha) \in \mathcal{O}_L$ and $\mathrm{Norm}_{K|\mathbb{Q}}(\alpha) \in \mathcal{O}_L$ by Theorem 14.1.5. Now the trace and norm are both in $\mathbb{Q}$, and $\mathbb{Q} \cap \mathcal{O}_L = \mathbb{Z}$. □

Definition 14.1.8. *$\alpha \in \mathcal{O}_K$ is a **unit** if $\alpha^{-1} \in \mathcal{O}_K$.*

Lemma 14.1.9. *Let $\mathcal{O}_K$ be the ring of integers in a number field K, and let $\alpha, \beta \in \mathcal{O}_K$. Then,*

1. *α is a unit in $\mathcal{O}_K$ if and only if $\mathrm{Norm}_{K|\mathbb{Q}}(\alpha) = \pm 1$*
2. *If α and β are associates in $\mathcal{O}_K$, then $\mathrm{Norm}_{K|\mathbb{Q}}(\alpha) = \pm \mathrm{Norm}_{K|\mathbb{Q}}(\beta)$*
3. *If $\mathrm{Norm}_{K|\mathbb{Q}}(\alpha)$ is a rational prime (primes in $\mathbb{Z}$), then α is irreducible in $\mathcal{O}_K$.*

Proof. (i) Suppose that α is a unit. Then,

$$\mathrm{Norm}_{K|\mathbb{Q}}(\alpha)\mathrm{Norm}_{K|\mathbb{Q}}(\alpha^{-1}) = \mathrm{Norm}_{K|\mathbb{Q}}(\alpha\alpha^{-1}) = \mathrm{Norm}_{K|\mathbb{Q}}(1) = 1$$

which is a product of elements in $\mathbb{Z}$, so both are ± 1.

Conversely, if $\mathrm{Norm}_{K|\mathbb{Q}}(\alpha) = \pm 1$, let $\alpha_1, \dots, \alpha_n$ be the $K|\mathbb{Q}$ conjugates with $\alpha = \alpha_1$. Then, $\alpha_1 \dots \alpha_n = \pm 1$, such that $\alpha(\alpha_2 \dots \alpha_n) = \pm 1$. Hence, $\alpha^{-1} = \pm(\alpha_2 \dots \alpha_n)$, which is in $\mathcal{O}_L$ (the splitting field of the minimal polynomial) by Theorem 14.1.5. As K is a field, α^{-1} lies in K, giving $\alpha^{-1} \in \mathcal{O}_L \cap K = \mathcal{O}_K$.

(ii) We have $\alpha = u\beta$ for some unit u, so

$$\mathrm{Norm}_{K|\mathbb{Q}}(\alpha) = \mathrm{Norm}_{K|\mathbb{Q}}(u)\mathrm{Norm}_{K|\mathbb{Q}}(\beta) = \pm \mathrm{Norm}_{K|\mathbb{Q}}(\beta)$$

by (i)

(iii) Let $\alpha = \gamma\delta$. Then $\mathrm{Norm}_{K|\mathbb{Q}}(\alpha) = p = \mathrm{Norm}_{K|\mathbb{Q}}(\gamma)\mathrm{Norm}_{K|\mathbb{Q}}(\delta)$ for some prime $p \in \mathbb{Z}$. The result again follows from (i) □

Remark 14.1.10. The converse for (ii) and (iii) are false. Take $K = \mathbb{Q}(\sqrt{-5})$, where the ring $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$.

Note first we have a factorisation $6 = 2 \cdot 3 = (1 - \sqrt{-5}) \cdot (1 + \sqrt{-5})$ in $\mathcal{O}_K$. Now, $\mathrm{Norm}_{K|\mathbb{Q}}(a + b\sqrt{-5}) = a^2 + 5b^2$, so the norm in our factors are $4, 9, 6, 6$ respectively. If any of these elements are not irreducible, we should be able to find $\alpha = \beta\gamma$ such that the norm of β, γ lie in ± 2 or ± 3. Clearly, no such solutions exist. By Lemma 14.1.9 (ii), we see this factorisation is not unique.

Note that the norm for $1 + \sqrt{-5}$ and $1 - \sqrt{-5}$ are equal but are not associates (only units are ± 1) Also, we have clearly exhibited an α that is irreducible with non-prime norm.

Definition 14.1.11. *$w_1, \dots, w_n \in \mathcal{O}_K$ is said to be an **integral basis** for $\mathcal{O}_K$ if $\mathcal{O}_K = \{\sum_j c_j w_j \mid c_j \in \mathbb{Z}\}$.*

Equivalently, $w_1, \dots, w_n$ is a $\mathbb{Z}$-basis for $\mathcal{O}_K$. We sometimes call this set the integral basis for K.

Example 14.1.12. Taking $K = \mathbb{Q}(\sqrt{d})$, where d is a square-free integer such that $[K : \mathbb{Q}] = 2$, $\mathcal{O}_K$ has integral basis

$$\begin{cases} \{1, \sqrt{d}\} & d \equiv 2, 3 \bmod 4 \\ \{1, \frac{1+\sqrt{d}}{2}\} & d \equiv 1 \bmod 4 \end{cases}$$

Remark 14.1.13. Let $v = \{v_1, \ldots, v_n\}$ and $w = \{w_1, \ldots, w_n\}$ be any two $\mathbb{Q}$-bases of K. Define $M = \langle v_1, \ldots, v_n\rangle_{\mathbb{Z}}$ and $N = \langle w_1, \ldots, w_n\rangle_{\mathbb{Z}}$ be the $\mathbb{Z}$-submodules of K. Suppose that $v, w \subseteq \mathcal{O}_K$. Then $\Delta(v)^2$ and $\Delta(w)^2$ both lie in $\mathbb{Z}$, as $\Delta(v)^2 = \det(\mathrm{Tr}_{K|\mathbb{Q}}(v_i v_j))$.

Suppose now that $N \subseteq M$. Then we can find $c_{ij} \in \mathbb{Z}$ such that $w_i = \sum_{j=1}^{n} c_{ij} v_j$. Define $C = (c_{ij})$.

By Theorem 11.3.7, we have

$$|\det(C)| = [M : N] = \#M/N =: m$$

as additive groups. By Lemma 12.0.5, we have

$$\Delta(w)^2 = (\det(C))^2 \Delta(v)^2 = m^2 \Delta(v)^2$$

If $M = N$, then by Lemma 11.3.6, C is unimodular, thus $\Delta(w)^2 = \Delta(v)^2$.

Definition 14.1.14. *Let M be any subset of $\mathcal{O}_K$ which has a $\mathbb{Z}$-basis. Define $\Delta(M)^2 := \Delta(w)^2$ for any $\mathbb{Z}$-basis w of M.*

From the previous remark, if $N \subseteq M$, then $\Delta(N)^2 = m^2 \Delta(M)^2$, so we have that $\Delta(M)^2 | \Delta(N)^2$.

Theorem 14.1.15 (Integral Basis Theorem)**.** *The ring $\mathcal{O}_K$ has an integral basis.*

Proof. Let $v = \{v_1, \ldots, v_n\}$ be any $\mathbb{Q}$-basis for K. Multiplying v_i by a sufficiently large number, we can suppose $v \subseteq \mathcal{O}_K$.

Let $M = \langle v_1, \ldots, v_n\rangle_{\mathbb{Z}}$. Then $\Delta(M)^2 \neq 0$ and in $\mathbb{Z}$ as $\{v_1, \ldots, v_n\}$ are $\mathbb{Q}$-linearly independent. Choose the basis v such that $|\Delta(M)^2|$ is minimal.

We claim that $M = \mathcal{O}_K$, and hence that $\{v_1, \ldots, v_n\}$ is an integral basis. Suppose for a contradiction there is some $\alpha \in \mathcal{O}_K$ such that $\alpha \notin M$. Then $\alpha = \sum_{j=1}^{n} c_j v_j$ with $c_j \in \mathbb{Q}$. Then for any j and $m \in \mathbb{Z}$, $\alpha + m v_j \in \mathcal{O}_K$, but $\alpha + m v_j \notin M$. By adding suitable $\mathbb{Z}$-multiples of v_j to α, we may assume $|c_j| \leq 1/2$. Since $\alpha \notin M$, there exists j such that $c_j \neq 0$. Choose such j.

Let w be a new $\mathbb{Q}$-basis obtained from v by replacing v_j by α. We have $w \subseteq \mathcal{O}_K$. The change of basis matrix

$$C = \begin{pmatrix} 1 & 0 & \cdots & & 0 \\ 0 & 1 & \cdots & & 0 \\ \vdots & & & \vdots & \\ c_1 & \cdots & c_j & \cdots & c_n \\ \vdots & & & \vdots & \\ 0 & 0 & \cdots & 0 & 1 \end{pmatrix}$$

has determinant c_j. Thus

$$|\Delta(w)^2| = c_j^2 |\Delta(v)^2| < |\Delta(v)^2|$$

contradicting the minimality of $|\Delta(v)^2$. Hence, such an α does not exist, giving $M = \mathcal{O}_K$. □

Proposition 14.1.16. *Let $w = \{w_1, \ldots, w_n\}$ be any $\mathbb{Q}$-basis for K such that $w \subseteq \mathcal{O}_K$. Let $M = \langle w_1, \ldots, w_n\rangle_{\mathbb{Z}}$ and let $M \neq \mathcal{O}_K$. Then there exists a prime p such that $p^2 | \det(M)^2$ and $c_1, \ldots, c_n \in \mathbb{Z}$ not all divisible by p such that*

$$\frac{1}{p}(c_1 w_1 + \cdots + c_n w_n) \in \mathcal{O}_K$$

Proof. Let $m = [\mathcal{O}_K : M] > 1$ such that $|\Delta(M)^2| = m^2|\Delta(\mathcal{O}_K)^2|$. Since $m > 1$, there is a prime p dividing m, such that $p^2|\Delta(M)^2$. As $m = \#\mathcal{O}_K/M$, by Cauchy's Theorem on finite groups, $\mathcal{O}_K/M$ has an element of order p. Let $\alpha + M$ be such element. Then $\alpha = \sum d_j w_j$ with $d_j \in \mathbb{Q}$. By construction, $p\alpha \in M$ so that $pd_j \in \mathbb{Z}$. Thus, we can take $\alpha = 1/p \sum_j (pd_j)w_j \in \mathcal{O}_K$. □

Remark 14.1.17. The above shows a general method to find the integral basis for $\mathcal{O}_K$, where $[K : \mathbb{Q}] = n$.

- Let $w = \{w_1, \ldots, w_n\}$ be any $\mathbb{Q}$-basis for K such that $w \subseteq \mathcal{O}_K$. Calculate $\Delta(w)^2$. Taking $M = \langle w_1, \ldots, w_n\rangle_{\mathbb{Z}}$, we know $M \subseteq \mathcal{O}_K$.
- If $[\mathcal{O}_K : M] = m$, then we know $|\Delta(M)^2| = m^2|\Delta(\mathcal{O}_K)^2|$. If $\Delta(M)^2$ is squarefree, then $m = 1$, giving $\mathcal{O}_K = M$. Else, we can find a prime p such that $p^2|\Delta(M)^2$ and $c_i \in \mathbb{Z}$ not all divisible by p such that $1/p \sum c_i w_i \in \mathcal{O}_K$.
- Thus if $\Delta(M)^2$ is not squarefree, then for each prime p such that $p^2|\Delta(M)^2$, take $\alpha \in \mathcal{O}_K$ of the form $1/p \sum c_i w_i$ where p does not divide all c_j and $c_j \in \mathbb{Z}$. Suppose p does not divide c_j for $j = k$. Multiplying through by $r \in \mathbb{Z}$ such that $rc_k \equiv 1 \bmod p$, we may without loss of generality suppose that $c_k \equiv 1 \bmod p$. Subtracting integer multiples of w_i, we may further suppose that $0 \le c_i < p$ for all i, giving $c_k = 1$. Replacing w_k with the new α, we get another basis, spanning a $\mathbb{Z}$-module M'. The change of basis matrix has determinant $c_k/p = 1/p$, and in particular $\Delta(M')^2 = \frac{1}{p^2}\Delta(M)^2$
- Repeating the process with M' instead of M, if no such α exists (this requires finite checking as we only need to look for $0 \le c_i < p$), then p cannot divide m. Eventually we reach a basis where none of the avaialble primes divide m such that $m = 1$, giving the integral basis.

Example 14.1.18. Let $K = \mathbb{Q}(\sqrt{d})$ with d squarefree. Start with $\mathbb{Q}$-basis $\{1, \sqrt{d}\}$. Then we clearly have $\{1, \sqrt{d}\} \subseteq \mathcal{O}_K$ and

$$\Delta(\{1, \sqrt{d}\})^2 = \begin{vmatrix} 1 & -\sqrt{d} \\ 1 & +\sqrt{d} \end{vmatrix}^2 = 4d$$

As d is squarefree the only prime p such that $p^2|\Delta(\{1, \sqrt{d}\})^2$ is $p = 2$.

We have two cases,

- $d \equiv 1 \bmod 4$. We find $\frac{1}{2}(1 + \sqrt{d}) \in \mathcal{O}_K$. In this case we find

  $$\Delta(\{1, \frac{1}{2}(1 + \sqrt{-d})\})^2 = \frac{1}{2^2}4d = d$$

  and so we are done.
- $d \not\equiv 1 \bmod 4$. Then we see that $\frac{1}{2}(1 + \sqrt{d}) \notin \mathcal{O}_K$ as the minimal polynomial is not in $\mathbb{Z}[x]$. The other cases to check are $\frac{1}{2}$, $\frac{1}{2}\sqrt{d}$, neither are in $\mathcal{O}_K$. No such α was found, so 2 does not divide the index $m = [\mathcal{O}_K : \langle 1, \sqrt{d}\rangle_{\mathbb{Z}}]$. This shows $\{1, \sqrt{d}\}$ is an integral basis.

Definition 14.1.19. *Let K, L be fields with $K \subseteq L$. Let I be an ideal of $\mathcal{O}_K$. Then $I \cdot \mathcal{O}_L$ is defined to be the ideal of $\mathcal{O}_L$ generated by the products of the form $i\ell$ such that $i \in I$ and $\ell \in \mathcal{O}_L$.*

Proposition 14.1.20. *Given ideals I, J of $\mathcal{O}_K$, a principal ideal $(a) = a\mathcal{O}_K$ of $\mathcal{O}_K$,*

1. $(IJ) \cdot \mathcal{O}_L = (I \cdot \mathcal{O}_L)(J \cdot \mathcal{O}_L)$

2. $I^n \cdot \mathcal{O}_L = (I \cdot \mathcal{O}_L)^n$

3. $(a) \cdot \mathcal{O}_L = a\mathcal{O}_L$ *(principal ideals are generated by the same element)*

Proof. The first is simply an expansion of both sides, then double inclusion. The second follows by induction using the first statement. The third statement is straightforward from definitions. □

14.2 Cyclotomic Fields

Take the cyclotomic extension $\mathbb{Q}(\mu_p)$ for a prime p. Let ζ be a primitive p-th root. Let f be the minimal polynomial of ζ.

14.3 Class Number

Definition 14.3.1. *Let I and J be non-zero ideals of $\mathcal{O}_K$. Then we write $I \sim J$ if there exist $\alpha, \beta \in \mathcal{O}_K \setminus \{0\}$ such that $I(\alpha) = J(\beta)$.*

Proposition 14.3.2. *The relation $\sim$ gives an equivalence relation.*

Proof. Reflexivity and symmetry are immediate. For transitivity, if we have $I(\alpha) = J(\beta)$ and $J(\gamma) = K(\delta)$, we see that

$$I(\alpha\gamma) = I(\alpha)(\gamma) = J(\beta)(\gamma) = J(\gamma)(\beta) = K(\delta)(\beta) = K(\delta\gamma)$$

In particular, $I \sim K$. □

Definition 14.3.3. *The equivalence classes in $\mathcal{O}_K$ under $\sim$ are called **ideal classes**. We write C_K to denote the set of ideal classes. The cardinality $h_K = |C_k|$ is the **class number** of K.*

Proposition 14.3.4. *We have $h_K = 1$ if and only if $\mathcal{O}_K$ is a PID.*

Proof. ($\Rightarrow$) Suppose that $h_K = 1$. Then for all proper ideals I in $\mathcal{O}_K$, there exists $\alpha, \beta \in \mathcal{O}_K$ such that

$$I(\alpha) = \mathcal{O}_K(\beta)$$

The right side is (β). As $\beta \in (\beta)$, we have $\beta = i\alpha$ for some $i \in I$. Thus, $\beta/\alpha \in I$. We claim that $(\beta/\alpha) = I$. Clearly, $(\beta/\alpha) \subseteq I$. Given $a \in I$, we have $a\alpha \in I(\alpha) = (\beta)$, so $a\alpha = r\beta$ for some $r \in \mathcal{O}_K$, giving $a = r\beta/\alpha$. Thus $\alpha \in (\beta/\alpha)$ and $I \subseteq (\beta/\alpha)$.

($\Leftarrow$) Suppose that $\mathcal{O}_K$ is a PID. Then for any nonzero $I \subseteq \mathcal{O}_K$, there exists an $\alpha \in \mathcal{O}_K$ such that $I = (\alpha)$. In particular, $I(1) = \mathcal{O}_K(\alpha)$, so $I \sim \mathcal{O}_K$. □

Lemma 14.3.5. *Let $I \subseteq \mathcal{O}_K$ be a nonzero ideal. Then $I \cap \mathbb{Z} \neq \{0\}$.*

Proof. Choose any nonzero $\alpha \in I$. α is annihalated by some monic polynomial in $\mathbb{Z}[x]$, so write $\alpha^d + a_{d-1}\alpha^{d-1} + \cdots + a_0 = 0$. We can choose one such that $a_0 \neq 0$. In particular, $a_0 = -\alpha(a_1 + \cdots + \alpha^{d-1}) \in I \cap \mathbb{Z}$. □

Lemma 14.3.6. *Let $I \subseteq \mathcal{O}_K$ be a nonzero ideal. Then $\mathcal{O}_K/I$ is a finite ring.*

Proof. Choose any nonzero $a \in I \cap \mathbb{Z}$. We have $(a) \subseteq I \subseteq \mathcal{O}_K$. The map from $\mathcal{O}_K/(a)$ to $\mathcal{O}_K/I$ that takes $\alpha + (a)$ to $\alpha + I$ is well-defined and onto. Thus it suffices to show that $\mathcal{O}_K/(a)$ is finite.

Let $w = \{w_1, \ldots, w_n\}$ be an integral basis for $\mathcal{O}_K$. Then $\mathcal{O}_K/(a)$ is isomorphic as an additive group to $(\mathbb{Z}/a\mathbb{Z})^n$, where $n = [K : \mathbb{Q}]$. In particular, $\#\mathcal{O}_K/(a) = a^n < \infty$. □

Definition 14.3.7. *The norm of I is defined as $N(I) := \#\mathcal{O}_K/I$.*

Proposition 14.3.8. *Let $\sigma : K \to K$ be an automorphism. Then $I = (\alpha_1, \dots, \alpha_n)$ and $I^\sigma = (\alpha_1^\sigma, \dots, \alpha_n^\sigma) = (\sigma(\alpha_1), \dots, \sigma(\alpha_n))$ have an induced isomorphism. In particular, they have the same norm.*

Proof. The map is given by $x + I \to \sigma(x) + I^\sigma$. This is surjective as σ is surjective, and injective as every element of I^σ comes from I. □

Proposition 14.3.9. *If $I = (a)$, then $N(I) = |\mathrm{Norm}_{K|\mathbb{Q}}(\alpha)|$.*

Proof. Let $w = \{w_1, \dots, w_n\}$ be an integral basis for $\mathcal{O}_K$. Then αw is a $\mathbb{Z}$ basis for $I = (\alpha)$. By definition,

$$\Delta(\alpha w) = \det(\sigma_i(\alpha w_j)) = \det(\sigma_i(\alpha)\sigma_i(w_j)) = \left(\prod_{i=1}^n \sigma_i(\alpha)\right)\Delta(w) = \mathrm{Norm}_{K|\mathbb{Q}}(\alpha)\Delta(w)$$

Now I is an additive subgroup of $\mathcal{O}_K$ with index $N(I)$. Thus if $\alpha w_i = \sum c_{ij} w_j$ with $c_{ij} \in \mathbb{Z}$, then we have $N(I) = |\det(c_{ij})|$ by Theorem 11.3.7.

By Lemma 12.0.5, we have $\Delta(\alpha w) = \det(c_{ij})\Delta(w)$. In particular,

$$N(I) = |\Delta(\alpha w)/\Delta(w)| = |\mathrm{Norm}_{K|\mathbb{Q}}(\alpha)|$$

□

Lemma 14.3.10 (Hurwitz)**.** *Let K be a number field with $[K : \mathbb{Q}] = n$. Then there exists a positive integer M depending only on the choice of integral basis for $\mathcal{O}_K$ such that for any $\gamma \in K$, there exists a $w \in \mathcal{O}_K$ wand $1 \leq t \leq M$, $t \in \mathbb{Z}$ iwth*

$$|\mathrm{Norm}_{K|\mathbb{Q}}(t\gamma - w)| < 1$$

Proof. Let $\{w_1, \dots, w_n\}$ be an integral basis for $\mathcal{O}_K$. For any $\gamma \in K$, write

$$\gamma = \sum_{i=1}^n \gamma_i w_i$$

with $\gamma_i \in \mathbb{Q}$. Let $\gamma_i = a_i + b_i$ with $a_i \in \mathbb{Z}$ and $0 \leq b_i < 1$. As quick notation, write $[\gamma] = \sum_{i=1}^n a_i w_i$ and $\{\gamma\} = \sum_{i=1}^n b_i w_i$. Thus $\gamma = [\gamma] + \{\gamma\}$ and $[\gamma] \in \mathcal{O}_K$ for all $\gamma \in K$.

Let $w_i^{(1)}, \dots, w_i^{(n)}$ be the $K|\mathbb{Q}$ conjugates of w_i and set

$$C := \prod_{j=1}^n \left(\sum_{i=1}^n |w_i^{(j)}|\right)$$

Then, if $\gamma = \sum_{i=1}^n \gamma_i w_i$ and $\mu := \max_{1 \leq i \leq n} |\gamma_i|$, we have

$$|\mathrm{Norm}_{K|\mathbb{Q}}(\gamma)| = |\prod_{j=1}^n \left(\sum_{i=1}^n \gamma_i w_i^{(j)}\right)| \leq \prod_{j=1}^n \left(\sum_{i=1}^n \mu |w_i^{(j)}|\right) = C\mu^n$$

Choose m to be the first integer after $C^{1/n}$ and let $M = m^n$ such that M only depends on the choice of $w_1, \dots, w_n$.

Define a linear map $\phi : K \to \mathbb{R}^n$ by

$$\phi\left(\sum_{i=1}^{n} \gamma_i w_i\right) = (\gamma_1, \ldots, \gamma_n)$$

By construction, $\phi(\{\gamma\})$ lies in the n-dimensional unit cube, $B := \{(x_1, \ldots, x_n) \in \mathbb{R}^n \mid 0 \leq x_i < 1\}$. Partitioning B into m^n subcubes inside $1/m$ and consider the points $\phi(\{k\gamma\})$ for $0 \leq k \leq m^n$. There are $m^n + 1$ such points inside m^n subcubes, so there is some subcube with two points. Picking these k, say h, l with $h > l$ and taking $t = h - l$, we have $1 \leq t \leq m^n = M$.

By construction $t\gamma = w + \delta$ where $w := [h\gamma] - [l\gamma] \in \mathcal{O}_K$ and $\delta := \{h\gamma\} - \{l\gamma\}$ such that

$$\phi(\delta) \in [-1/m, 1/m]^n$$

By the inequality established previously,

$$|\mathrm{Norm}_{K|\mathbb{Q}}(\delta)| \leq C(1/m)^n < 1$$

as $m > C^{1/n}$. Now, as $\delta = t\gamma - w$, the lemma follows. □

Remark 14.3.11. If $M = 1$ in the above lemma, then we for any $\gamma \in K$, we can find a $w \in \mathcal{O}_K$ with $|\mathrm{Norm}_{K|\mathbb{Q}}(\gamma - w)| < 1$. Then, given any $\alpha, \beta \in \mathcal{O}_K$, let $\gamma = \alpha/\beta$. Thus, we have a $w \in \mathcal{O}_K$ such that

$$|\mathrm{Norm}_{K|\mathbb{Q}}(\alpha/\beta - w)| = |\mathrm{Norm}_{K|\mathbb{Q}}((\alpha - \beta w)/\beta)| < 1$$

In particular, by multiplicativity of the Norm, $|\mathrm{Norm}_{K|\mathbb{Q}}(\alpha - \beta w)| < |\mathrm{Norm}_{K|\mathbb{Q}}(\beta)|$. Thus, we can write $\alpha = \beta w + (\alpha - \beta w)$ such that the remainder has strictly smaller Norm. Thus $\mathcal{O}_K$ is a Euclidian domain (hence a PID, hence class number 1).

Theorem 14.3.12. *The class number $h_K = \# C_k$ is finite*

Proof. Let I be a nonzero ideal of $\mathcal{O}_K$. Choose $0 \neq \beta \in I$ such that $|\mathrm{Norm}(\beta)|$ is minimal, and let M be as in Hurwitz's Lemma. Applying Hurwitz with $\gamma := \alpha/\beta$, there is some t in the range $1 \leq t \leq M$ and $w \in \mathcal{O}_K$ such that $|\mathrm{Norm}(t(\alpha/\beta) - w)| < 1$. By construction, $t\alpha - \beta w \in I$ with $|\mathrm{Norm}(t\alpha - \beta w)| < |\mathrm{Norm}(\beta)|$. This contradicts the minimality of $|\mathrm{Norm}(\beta)|$ unless $t\alpha - w\beta = 0$. In particular, $t\alpha \in (\beta)$. Although t is based on α, as it lies between 1 and M, we know that $M!\alpha \in (\beta)$. As α was arbitrary,

$$(M!)I \subseteq (\beta)$$

Now let $J := \{1/\beta \times M! \times \alpha \mid \alpha \in I\}$. Then J is an ideal in $\mathcal{O}_K$, using the subset equation we established previously. Also, $(\beta)J = (M!)I$, so $I \sim J$. Also by construction, $\mathcal{O}_K \supseteq J \supseteq (M!)$. As we know $\mathcal{O}_K/(M!)$ is finite, there are only finitely many choices of J. Hence I is equivalent to one of finitely many ideals, and in particular there are finitely many equivalence classes. □

14.4 Unique Factorisation

Lemma 14.4.1. *If $I, J \subseteq \mathcal{O}_K$ are ideals with I nonzero with $JI = I$ then $J = \mathcal{O}_K$.*

Proof. Let $\alpha_1, \ldots, \alpha_n$ be a $\mathbb{Z}$ basis for I. As $I = JI$, we can find $b_{ij} \in J$ such that $\alpha_i = \sum_{j=1}^{n} b_{ij}\alpha_j$. Hence $\det(b_{ij} - \delta_{ij}) = 0$, and expanding this determinant, every term lies in J apart from the prodct of 1's in the identity. Thus, $1 \in J$, giving $J = (1) = \mathcal{O}_K$. □

Lemma 14.4.2. *If I is a nonzero ideal of $\mathcal{O}_K$ and $w \in K$ with $wI \subseteq I$, then $w \in \mathcal{O}_K$.*

Proof. Take $M = I$ with Lemma 14.1.4. □

Lemma 14.4.3. *If I, J are nonzero ideals in $\mathcal{O}_K$ and $w \in \mathcal{O}_K$ is such that $(w)I = JI$, then $(w) = J$.*

Proof. Choose any $\beta \in J$. Then we have $(w)I \supseteq (\beta)I$, such that $\{\beta/w\}I \subseteq I$. By Lemma 14.4.2, $\beta/w \in \mathcal{O}_K$, thus $\beta \in (w)$. As β was arbitrary, we see that $J \subseteq (w)$.

Thus $w^{-1}J$ is an ideal in $\mathcal{O}_K$. From assumption, we have $I = (w^{-1}J)I$, so by Lemma 14.4.1, $w^{-1}J = \mathcal{O}_K$, giving $J = (w)$. □

Proposition 14.4.4. *For any nonzero ideal $I \subseteq \mathcal{O}_K$, there exists a k such that $1 \leq k \leq h_K$ and I^k is principal.*

Proof. Among the $h_K + 1$ ideals $\{I^i \mid 1 \leq i \leq h_K + 1\}$, some two must be equivalent. Suppose $I^i \sim I^j$ with $j > i$. Thus $(\alpha)I^i = (\beta)I^j$ for some $\alpha, \beta \in \mathcal{O}_K$. Let $k = j - i$ and $J = I^k$. Then, $(\alpha)I^i = (\beta)I^iJ \subseteq (\beta)I^i$ such that $\{\alpha/\beta\}I^i \subseteq I^i$. By Lemma 14.4.2, we have $\alpha/\beta \in \mathcal{O}_K$. Also, $(\alpha/\beta)I^i = JI^i$, so by Lemma 14.4.3, $(\alpha/\beta) = J$. Thus $J = I^k$ is principal. □

Proposition 14.4.5. *The ideal classes form a group C_K. It is called the class group of K and its order is the class number h_K.*

Proof. Given two ideal classes $[I], [J]$, define the prodct by $[I] \cdot [J] := [IJ]$. This is clearly well-defined. The element $[O_k]$ acts as an identity, and associativity is derived from the ring structure of $\mathcal{O}_K$. Given $[I] \in C_K$, as I^k is principal for some I, $[I^{k-1}]$ clearly gives an inverse. □

Lemma 14.4.6 (Cancellation Lemma)**.** *Let $A, B, C \subseteq \mathcal{O}_K$ be nonzero ideals with $AB = AC$. Then $B = C$.*

Proof. Let k be such that $A^k = (\alpha)$ is principal. Multiplying by A^{k-1}, we get $(\alpha)B = (\alpha)C$, so $B = C$. □

Definition 14.4.7. *Let $A, B \subseteq \mathcal{O}_K$ be nonzero ideals. Write $B|A$ if there exists an ideal $C \subseteq \mathcal{O}_K$ such that $A = BC$.*

Proposition 14.4.8. *Let A, B be nonzero ideals in $\mathcal{O}_K$. Then $B \supseteq A$ if and only if there exists an ideal C such that $A = BC$ (equivalently, $B|A$).*

Proof. Let $k \geq 1$ be such that $B^k = (\beta)$ is principal. If $B \supseteq A$, then we have $B^{k-1}A \subseteq B^k = (\beta)$. Let $C := \{1/\beta\}B^{k-1}A$ such that $C \subseteq \mathcal{O}_K$ is an ideal. Then, $BC = B\{1/\beta\}B^{k-1}A = A$.

Conversely, if $B|A$ then $A = BC'$ for some C'. Immediately, $BC' \subseteq B$ as B is an ideal. Thus $A \subseteq B$. □

Lemma 14.4.9. *Let A, B be nonzero ideals and P be a prime ideal of $\mathcal{O}_K$ such that $P|AB$. Then either $P|A$ or $P|B$.*

Proof. Suppose that $P|AB$ and that P does not divide A. We have $P \supseteq AB$ but $P \not\supseteq A$, so we can find a $\alpha in A$ with $\alpha \notin P$. On the other hand, for any $\beta \in B$, we have $\alpha\beta \in P$. As P is a prime ideal, given $\alpha\beta \in P$, one of α or β belongs to P. Thus $\beta \in P$. This gives $P \supseteq B$, thus $P|B$. □

Remark 14.4.10. Nonzero prime ideals in $\mathcal{O}_K$ are maximal. This follows from the fact that if P is a nonzero prime ideal of $\mathcal{O}_K$, then $\mathcal{O}_K/P$ is a finite integral domain, thus a field.

Theorem 14.4.11 (Unique Factorisation Theorem for ideals of $\mathcal{O}_K$)**.** *Let A be any nonzero proper ideal of $\mathcal{O}_K$. Then there exist prime ideals $P_1, \ldots, P_r$ such that $A = P_1 \cdots P_r$. The factorisation is unique up to the order of factors.*

Proof. Suppose that there is some nonzero proper ideal A that has no prime factorisation. Let A be such an ideal with $N(A)$ minimal. There exists a maximal (thus prime) ideal P_1 containing A. In particular, we can find an ideal C with $A = P_1C$.

If $A = C$, then $P_1C = C$, which gives $P_1 = \mathcal{O}_K$, a contradiction. Thus $A \subsetneq C$. By the definition of Norm, we have $N(A) = N(C)[C : A] > N(C)$. By the minimality assumption, we can factor C into prime ideals $C = P_2 \cdots P_r$ (or trivially if $C = \mathcal{O}_K$). Then, $A = P_1 \cdots P_r$, a contradiction. Hence every nonzero proper ideal has a prime factorisation.

Suppose now that $A = P_1 \cdots P_r = Q_1 \cdots Q_s$. We know that $P_1 | Q_1 \cdots Q_s$. Take k minimal such that $P_1 | Q_1 \cdots Q_k$. If $k = 1$, $P_1 | Q_1$, and if $k > 1$, $P_1 | (Q_1 \cdots Q_{k-1})Q_k$, but P_1 does not divide $(Q_1 \cdots Q_{k-1})$, thus $P_1 | Q_k$. We therefore have $P_1 | Q_k$. As Q_k is maximal, $P_1 = Q_k$. Without loss of generality, take $k = 1$, and inductively repeat by applying the Cancellation Lemma.

In the end we get $\mathcal{O}_K = Q'_1 \cdots Q'_t$ unless $r = s$, but only one side clearly contains the identity. □

Remark 14.4.12. Prime ideals that appear in A are those which contain A. We don't have to worry about associates as for any unit u, $(u)I = I$. If $\mathcal{O}_K$ is a PID, this is a direct proof that it is a UFD.

Remark 14.4.13. Note that ideals A, B in $\mathcal{O}_K$ are coprime if and only if there is no shared maximal ideal P. In other words, they have no prime factor in common.

By observing the factorisation and applying the cancellation lemma, if A, B are coprime, we have

- $A|BC$, then $A|C$
- $A|I$ and $B|I$ implies $AB|I$

Lemma 14.4.14. *If A and B are coprime, then $AB = A \cap B$.*

Proof. Clearly, $AB \subseteq A \cap B$, thus $A \cap B | AB$. On the other hand, $A | A \cap B$ and $B | A \cap B$, by coprimality and unique factorisation, we have $AB | A \cap B$. □

Lemma 14.4.15. *If A, B are nonzero coprime ideals, then $N(AB) = N(A)N(B)$.*

Proof. By the Chinese Remainder Theorem, we have

$$\mathcal{O}_K/(A \cap B) \simeq \mathcal{O}_K/A \oplus \mathcal{O}_K/B$$

when A, B are coprime. By the previous lemma, we have $A \cap B = AB$. By considering the cardinality on both sides, the proof follows. □

Lemma 14.4.16. *If P is a nonzero prime ideal of $\mathcal{O}_K$ and $i \geq 0$, $\#P^i/P^{i+1} = \#\mathcal{O}_K/P$.*

Proof. We have $P^{i+1} \subseteq P^i$, but by the Cancellation Lemma, cannot have equality. Thus we can choose a $\pi \in P^i$ such that $\pi \notin P^{i+1}$. Then, $P^i \supseteq (\pi)$. Let $(\pi) = P^iB$, then we have that P does not divide B.

Define a homomorphism on additive groups by

$$\theta : \mathcal{O}_K \to P^i/P^{i+1}$$
$$\alpha \mapsto \bar{\alpha\pi}$$

by the map which multiplies α by π then reduces modulo P^{i+1}. Now we also have

$$\theta(\alpha)=0 \iff \alpha\pi \in P^{i+1} \iff (\alpha\pi)\subseteq P^{i+1} \iff (\alpha)P^iB \subseteq P^{i+1}$$
$$\iff P^{i+1}|(\alpha)P^iB \iff P|B(\alpha) \iff P|(\alpha)$$

Thus, $\ker(\theta)=P$.

Thus by the first isomorphism theorem, it suffices to show that θ is surjective. Now

$$(\pi)+P^{i+1}=P^iB+P^{i+1}=P^i$$

as $B+P=\mathcal{O}_K$. Thus, given any $\beta+P^{i+1}\in P^i/P^{i+1}$, there exists $\alpha\in\mathcal{O}_K$ and $\gamma\in P^{i+1}$ such that $\alpha\pi+\gamma=\beta$. Then $\theta(\alpha)=\beta+P^{i+1}$. □

Corollary 14.4.17. *If P is a nonzero prime ideal and $e\geq 1$, then $N(P^e)=N(P)^e$.*

Proof. Taking $\mathcal{O}_K$ and P^i as additive groups, we have

$$N(P^e)=\#\mathcal{O}_K/P^e=\#\mathcal{O}_K/P\cdot\#P/P^2\cdots\#P^{e-1}/P^e=(\#\mathcal{O}_K/P)^e=N(P)^e$$

where the second equality comes from the third isomorphism theorem used telecopically (or noting that $0\to P^{i-1}/P^i\to\mathcal{O}_K/P^i\to\mathcal{O}_K/P^{i-1}\to 0$ is a short exact sequence). □

Corollary 14.4.18. *If $A=\prod_i P_i^{e_i}$, then $N(A)=\prod N(P_i)^{e_i}$, where P_i are distinct nonzero prime ideals*

Proof. Using the proof above and Lemma 14.4.15. □

Corollary 14.4.19. *If A, B are nonzero ideals, then $N(AB)=N(A)N(B)$*

Proof. A consequence of Unique Factorisation and the previous corollary. □

Remark 14.4.20. If $N(I)=p$ for a rational prime, then I is automatically prime as $\mathcal{O}_K/I$ is a finite ring with p elements. Alternatively, consider the factorisation of I and note that any nontrivial prime ideal has norm at least 2.

On the other hand, if P is prime, it is maximal, thus $\mathcal{O}_K/P$ is a finite field with p^k elements for some prime p and integer k.

Alternatively, let K be a number field of degree $[K:\mathbb{Q}]=n$. Let P be a nonzero prime ideal of $\mathcal{O}_K$. Then $P\cap\mathbb{Z}$ is a prime ideal of $\mathbb{Z}$, so it is of the form $p\mathbb{Z}$ for some rational p. Thus $P\supseteq p\mathcal{O}_K=(p)$. We say that P **lies above** p. Suppose that

$$(p)=P_1^{e_1}\cdots P_r^{e_r}$$

where P_i are distict prime ideals in $\mathcal{O}_K$. Then they are all prime ideals lying above the rational prime p. Taking norms,

$$p^n=N(P_1)^{e_1}\cdots N(P_r)^{e_r}$$

such that $N(P_i)=p^{f_i}$ with $\sum_{i=1}^r e_if_i=n$. As P must be one of the P_i, we see that $N(P)$ is a power of p.

Definition 14.4.21. *The integer e_i is called the* ***ramification index*** *of P_i. If $e_i>1$, we say that P_i is* ***ramified****. If some $e_i>1$, we say that p ramifies in K. The integer f_i is called the degree of P_i.*

Note here that $p^{f_i} = \#\mathcal{O}_K/P_i$ and that $\mathcal{O}_K/P_i$ is isomorphic to the finite field with p^{f_i} elements.

Example 14.4.22. Considering $\mathbb{Z}[\sqrt{-5}]$, we have

$$(6) = (2)(3) = (1 - \sqrt{-5})(1 + \sqrt{-5})$$

Let $P_1 = (2, 1 + \sqrt{-5}), P_2 = (2, 1 - \sqrt{-5}), Q_1 = (3, 1 + \sqrt{-5}), Q_2 = (3, 1 - \sqrt{-5})$. Now,

$$(2) = (4, 6) \subseteq P_1P_2 \subseteq (2, 6) = (2)$$

Thus $P_1P_2 = (2)$. We have $N((2)) = \text{Norm}(2) = 4$, thus $N(P_1)N(P_2) = 4$. Also, $a \equiv b \bmod 2$ when $a + b\sqrt{-5} \in P_i$, giving $P_i \neq \mathcal{O}_K$. Thus $N(P_1) = N(P_2) = 2$.

By similar calculation, we have $(3) = (9, 6) \subseteq Q_1Q_2 \subseteq (3, 6) = (3)$, such that $Q_1Q_2 = (3)$, with $N(Q_1) = N(Q_2) = 3$. As these are prime, we see that P_1, P_2, Q_1, Q_2 are prime ideals.

Now, $P_1, Q_1 \supseteq (1 + \sqrt{-5})$ and $P_2, Q_2 \supseteq (1 - \sqrt{-5})$, so contains once of each, comparing norms gives $P_1Q_1 = (1 + \sqrt{-5})$ and $P_2Q_2 = (1 - \sqrt{-5})$.

Thus,

$$(2)(3) = (1 + \sqrt{-5})(1 - \sqrt{-5}) = P_1P2Q_1Q_2 = P_1Q_1P_2Q_2$$

giving unique factorisation, although the factorisation into irreducibles are different.

Theorem 14.4.23 (Dedekind)**.** *Suppose that $K = \mathbb{Q}(\alpha)$ with $\alpha \in \mathcal{O}_K$ with a minimal polynomial $m(x) \in \mathbb{Z}[x]$ with degree n. If p does not divide $[\mathcal{O}_K : \mathbb{Z}[\alpha]]$ and $\bar{m}(x) := m(x) \bmod p \in \mathbb{F}_p[x]$ factorises as*

$$\bar{m}(x) = \prod_{i=1}^{r} \bar{g}_i(x)^{e_i}$$

with $\bar{g}_i$ distict and irreducible, then

- *$P_i = (p, g_i(\alpha))$ is a prime ideal of $\mathcal{O}_K$ (where $g_i(x)$ is any polynomial such that $g_i(x) \equiv \bar{g}_i(x) \bmod p$)*
- *P_i are distinct*
- *The degree of P_i is the degree of $\bar{g}_i$*
- $(p) = \prod_{i=1}^{r} P_i^{e_i}$

Proof. Suppose that p does not divide the index $[\mathcal{O}_K : \mathbb{Z}[\alpha]]$. Consider the natural map $\mathbb{Z}[\alpha] \to \mathcal{O}_K/p\mathcal{O}_K$. An element γ of the kernel must have the form $p\beta$ for $\beta \in \mathcal{O}_K$. As p does not divide the index $[\mathcal{O}_K : \mathbb{Z}[\alpha]]$, we must have $\beta \in \mathbb{Z}[\alpha]$. Thus the kernel is precisely $p\mathbb{Z}[\alpha]$, which induces an injection $\mathbb{Z}[\alpha] \hookrightarrow \mathcal{O}_K/p\mathcal{O}_K$. This must be an isomorphism of rings as both sides have order p^n.

Now consider the ring homomorphism from $Z[x]$ to $Z[\alpha]/p\mathbb{Z}[\alpha]$ taking $g(x)$ to $g(\alpha) + p\mathbb{Z}[\alpha]$. This has kernel

$$\{g(x) \mid g(x) = m(x)h(x) + pj(x)\} = (p, m(x))$$

giving

$$\mathbb{Z}[\alpha]/p\mathbb{Z}[\alpha] \simeq \mathbb{Z}[x]/(p, m(x))$$

Finally, consider the homomorphism from $\mathbb{Z}[x]$ to $\mathbb{F}_p[x]/(\bar{m}(x))$ sending $g(x)$ to $\bar{g}(x) + (\bar{m}(x))$. The kernel of this map is

$$\{g(x) \mid \bar{m}(x)|\bar{g}(x)\} = \{g(x) = m(x)h(x) + pj(x)\} = (p, m(x))$$

Thus $\mathbb{Z}[x]/(p, m(x)) \simeq \mathbb{F}_p[x]/(\bar{m}(x))$, and composing maps, we get

$$\mathcal{O}_K/p\mathcal{O}_K \simeq \mathbb{Z}[\alpha]/p\mathbb{Z}[\alpha] \simeq \mathbb{Z}[x]/(p, m(x)) \simeq \mathbb{F}_p[x]/(\bar{m}(x))$$

There is a bijective correspondence between prime ideals of $\mathcal{O}_K$ containing (p) and the prime ideals of $\mathcal{O}_K/p\mathcal{O}_K$, and these have a correspondence to prime ideals of $\mathbb{F}_p[x]/(\bar{m}(x))$. However, these prime ideals are generated by irreducible factors $\bar{g}_i(x)$ of $\bar{m}(x)$. Tracing back with correspondence, these correspond to $P_i = (p, g_i(\alpha))$ in $\mathcal{O}_K$. This shows (i) and (ii). Also, the isomorphism shows $N(P_i) = \#\mathbb{F}_p[x]/(\bar{g}_i(x))$, which shows (iii).

Finally, we have

$$\prod_{i=1}^{r} P_i^{e_i} = \prod_{i=1}^{r} (p, g_i(\alpha))^{e_i} \subseteq \prod_{i=1}^{r} (p, g_i(\alpha)^{e_i}) \subseteq (p, \prod_{i=1}^{r} g_i(\alpha)^{e_i}) = (p)$$

On the other hand, $p^{f_i} = N(P_i) = p^{\deg(g_i)}$, such that

$$N\left(\prod_{i=1}^{r} P_i^{e_i}\right) = p^{\sum_{i=1}^{r} e_i f_i} = p^{\sum_{i=1}^{r} e_i \ \deg(g_i)} = p^n$$

On the other hand, $N((p)) = p^n$, so $(p) = \prod_{i=1}^{r} P_i^{e_i}$. □

Corollary 14.4.24. *If p ramifies, then $p|\Delta(\mathbb{Z}[\alpha])^2$.*

Proof. Note that if $p|[\mathcal{O}_K : \mathbb{Z}[\alpha]]$, then $p|\Delta(\mathbb{Z}[\alpha])^2$, so we may suppose that p does not divide $[\mathcal{O}_K : \mathbb{Z}[\alpha]]$. Then by Dedekind, if p ramifies with a factor P^2, then $\bar{m}(x)$ has a multiple irreducibl factor $\bar{g}(x)$ over $\mathbb{F}_p$, for which $g(\alpha) \in (p, g(\alpha)) = P$. We then have that $m(x) = g(x)^2 h(x) + pk(x)$ such that

$$m'(x) = g(x)(2g'(x)h(x) + g(x)h'(x)) + pk'(x) = g(x)j(x) + pl(x)$$

say. Thus $m'(\alpha) = g(\alpha)j(\alpha) + p\beta$ with $\beta \in \mathcal{O}_K$. It follows that

$$\text{Norm}_{K|\mathbb{Q}}(m'(\alpha)) = \prod_{\sigma} \sigma(m'(\alpha)) = \prod_{\sigma} \sigma(g(\alpha)j(\alpha)) + p\gamma$$

for some algebraic integer γ. In particular,

$$\text{Norm}_{K|\mathbb{Q}}(m'(\alpha)) = \text{Norm}_{K|\mathbb{Q}}(g(\alpha))\text{Norm}_{K|\mathbb{Q}}(j(\alpha)) + p\gamma$$

and as $P|(g(\alpha))$, we have $p|\text{Norm}_{K|\mathbb{Q}}(g(\alpha))$. Now this also gives that $\gamma \in \mathbb{Z}$. Thus $p|\text{Norm}_{K|\mathbb{Q}}(m'(\alpha))$, and now the result follows as $\Delta^2(\mathbb{Z}[\alpha]) = \pm\text{Norm}_{K|\mathbb{Q}}(m'(\alpha))$. □

Example 14.4.25. Let $K = \mathbb{Q}(\sqrt{-5})$ such that $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$ and $\Delta(\mathbb{Z}[\sqrt{-5}])^2 = 4(-5) = -20$. The possible ramified primes are 2 and 5. We have $m(x) = x^2 + 5$ and

- $x^2 + 5 \equiv (x+1)^2 \bmod 2$, such that $(2) = (2, \sqrt{-5} + 1)^2$
- $x^2 + 5 \equiv x^2 \bmod 5$, such that $(5, \sqrt{-5})^2 = (\sqrt{-5})^2$.

For all primes we have $\sum_{i=1}^{r} e_i f_i = 2$, so $r \leq 2$. Thus either $r = 1, e_1 = 2, f_1 = 1$ (ramified case), $r = 1, e_1 = 1, f_1 = 2$ (inert case),$r = 2, e_1 = e_2 = 1, f_1 = f_2 = 1$ (splitting case). We extend this notion to general algebraic number fields, saying that p is **inert** if (p) is prime in $\mathcal{O}_K$, and that p splits otherwise.

We have considered $p = 2, 5$, so consider $p \neq 2, 5$.

- $\left(\frac{-5}{p} = -1\right)$. Then x^2+5 is irreducible modulo p, and

  $$(p) = P := (p, \sqrt{-5}^2 + 5) = (p)$$

  is inert.

- $\left(\frac{-5}{p} = 1\right)$, then $x^2+5 \equiv (x-a)(x+a) \bmod p$, where $a \not\equiv -a \bmod p$. Thus, $(p) = P_1P_2$, where $P_1 = (p, \sqrt{-5}-a)$ and $P_2 = (p, \sqrt{-5}+a)$.

14.5 Computation of the Class Group

Definition 14.5.1. *Let $\{v_1, \ldots, v_n\}$ be any basis for $\mathbb{R}^n$. Let $L = \{\sum_{i=1}^n a_iv_i \mid a_i \in \mathbb{Z}\}$ be the lattice generated by v_i. This is an additive subgroup of $\mathbb{R}^n$. Let $D = \{\sum_{i=1}^n a_iv_i \mid a_i \in [0,1)\}$. We call D the* ***fundamental domain*** *for L.*

Note that any $v \in \mathbb{R}^n$ can be expressed uniquely as $v = u + w$ with $u \in L$ and $w \in D$.

Definition 14.5.2. *If $v_i = \sum_{j=1}^n a_{ij}e_j$ where $\{e_1, \ldots, e_n\}$ is the standard basis for $\mathbb{R}^n$, we define*

$$\mathrm{Vol}(D) := |\det(a_{ij})|$$

we also sometimes denote this $\mathrm{Vol}(L)$.

Note that $\mathrm{Vol}(D)^2 = \det(v_i \cdot v_j)$, being the determinant of the matrix $(a_{ij})(a_{ij})^T$. $\mathrm{Vol}(D)$ is independent of the choice of $\mathbb{Z}$-basis for L, as the change of basis for this is a unitary matrix with determinant ±1.

Lemma 14.5.3 (Blichfeldt)**.** *Let L be a lattice in $\mathbb{R}^n$, and let S be a bounded measurable subset of $\mathbb{R}^n$ such that $\mathrm{Vol}(S) > \mathrm{Vol}(L)$. Then there exist $x, y \in S$ with $x \neq y$ such that $x - y \in L$.*

Proof. OoSN. Lemma 8.1 of ANT. Slight measure theory bits. □

Definition 14.5.4. *We say that $S \subseteq \mathbb{R}^n$ is* ***convex*** *if*

$$x, y \in S, 0 \leq \lambda < 1 \implies \lambda x + (1-\lambda)y \in S$$

We say that S is ***symmetric*** *(about the origin), if*

$$x \in S \implies -x \in S$$

Theorem 14.5.5 (Minkowski's Convex Body Theorem)**.** *Let L be a lattice in $\mathbb{R}^n$. Let S be a bounded measurable subset of $\mathbb{R}^n$ which is convex and symmetric. If $\mathrm{Vol}(S) > 2^n\mathrm{Vol}(L)$ then there exists $v \in L - \{0\}$ with $v \in S$.*

Proof. OoSN. Theorem 8.3 of ANT. Need to clear what 'measurable' is first... □

Remark 14.5.6. If S is closed (thus compact), it is enough to have $\mathrm{Vol}(S) \geq 2^n\mathrm{Vol}(L)$.

Example 14.5.7. If $p \equiv 1 \bmod 4$, then there exists $x, y \in \mathbb{Z}$ such that $p = x^2 + y^2$. We first note from $(\frac{-1}{p}) = 1$ that there is an s with $s^2 \equiv -1 \bmod p$. If $p = x^2 + y^2$, then this equals 0 mod p, so $(x/y)^2 \equiv -1 \bmod p$. In particular, $x \equiv \pm sy \bmod p$. Note,

$$x \equiv sy \bmod p \iff x = sy + pz \text{ with } z \in \mathbb{Z} \iff (x,y) = y(s,1) + z(p,0)$$

In particular, $\{(s,1),(p,0)\}$ is a basis for L (solutions) in $\mathbb{R}^2$ with

$$\mathrm{Vol}(L) = \left|\det\begin{pmatrix} s & p \\ 1 & 0\end{pmatrix}\right| = p$$

Let C be the disc $x^2+y^2<2p$ with radius $\sqrt{2p}$. C is convex and symmetric about the origin, and we also have

$$\mathrm{Vol}(C) = \pi(\sqrt{2p})^2 = 2\pi p > 2^2 p = 2^2\mathrm{Vol}(L)$$

Thus, by Minkowski's Theorem, there exists a nonzero $v \in L$ such that $v \in C$. Suppose that $v=(x,y)$. As $v \in L$ we have $x \equiv sy \bmod p$, thus $x^2+y^2 \equiv 0 \bmod p$. On the other hand, $v \in C$ implies that $x^2+y^2<2p$, so we have $x^2+y^2=0$ or p. As v is nonzero, this gives a solution $x^2+y^2=p$.

Definition 14.5.8. *Let $[K:\mathbb{Q}] := n = r+2s$ where r is the number of real embeddings $\sigma_1,\dots,\sigma_r : K \to \mathbb{R}$ and s is the number of pairs of complex embeddings $\sigma_{r+1},\dots,\sigma_{r+s},\bar{\sigma}_{r+1},\dots,\bar{\sigma}_{r+s} : K \to \mathbb{C}$.*

Let $\sigma : K \to \mathbb{R}^r \times \mathbb{C}^s \simeq \mathbb{R}^n$ defined as

$$\sigma(x) := (\sigma_1(x),\dots,\sigma_r(x),\Re(\sigma_{r+1}(x)),\Im(\sigma_{r+1}(x)),\dots,\Re(\sigma_{r+s}(x)),\Im(\sigma_{r+s}(x)))$$

Now let $\mathcal{O}_K$ be the ring of integers of K and let $\{v_1,\dots,v_n\}$ be an integral basis for $\mathcal{O}_K$. Write A for the matrix whose ith row is $\sigma(v_i)$. By elementary column operations,

$$(-2i)^s\det(A) = \det(\sigma_j(v_i)) = \pm\sqrt{|\Delta^2(K)|} \neq 0$$

where the $(-2i)$ factor comes from the change of basis matrix from $(\Re(z),\Im(z))$ to $(z,\bar{z})$. In particular $\det(A)\neq 0$ and $\sigma(\mathcal{O}_K)$ is a lattice in $\mathbb{R}^n$ with volume $\sqrt{|\Delta^2(K)|}/2^s$.

If I is an ideal of $\mathcal{O}_K$ with basis $w=\{w_1,\dots,w_n\}$, then $w_i=\sum_j c_{ij}v_j$, and

$$N(I) = [\mathcal{O}_K : I] = \det(c_{ij})$$

by Theorem 11.3.7. Also, by Lemma 12.0.5, we have $\Delta^2(w) = \det^2(c_{ij})\Delta^2(v)$, so $\Delta^2(w) = N(I)^2\Delta^2(v)$, giving

$$\mathrm{Vol}(\sigma(I)) = \frac{\sqrt{|\Delta^2(w)|}}{2^s} = \frac{N(I)\sqrt{|\Delta^2(v)|^2}}{2^s}$$

Lemma 14.5.9. *For $t>0$, let*

$$R_t := \{(x_1,\dots,x_r,z_1,\dots,z_s)\in\mathbb{R}^r\times\mathbb{C}^s\} \mid \sum_{i=1}^r |x_i| + 2\sum_{i=1}^s |z_i| \leq t$$

Then

- *R_t is a compact, symmetric, and covnex subset of $\mathbb{R}^n$*
- $\mathrm{Vol}(R_t) = 2^r t^n(\pi/2)^s/n!$

Proof. OoSN. See Lang, ANT, page 116. □

Theorem 14.5.10. *Let $I \subseteq \mathcal{O}_K$ be a nonzero ideal. Then there exists a nonzero $\alpha\in I$ with*

$$|\mathrm{Norm}_{K|\mathbb{Q}}(\alpha)| \leq c_K(N(I))$$

where

$$c_K := \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n}\sqrt{|\Delta^2(K)|}$$

is the ***Minkowski's constant*** *for K.*

Proof. Choose $t \in \mathbb{R}$ such that $\pi^s t^n/n! = 4^s\sqrt{|\Delta^2(K)|}N(I)$. Then,

$$\mathrm{Vol}(R_t) = \frac{2^r t^n (\pi/2)^s}{n!} = \frac{2^n\sqrt{|\Delta^2(K)|}N(I)}{2^s} = 2^n \mathrm{Vol}(\sigma(I))$$

By Minkowski's Theorem, there exists a nonzero $\alpha \in I$ such that $\sigma(\alpha) \in R_t$. In particular,

$$\sum_{i=1}^{r} |\sigma_i(\alpha)| + 2\sum_{i=r+1}^{s} \sqrt{\Re(\sigma_i(\alpha)^2) + \Im(\sigma_i(\alpha))^2} \leq t$$

In particular, $\sum_{i=1}^n |\sigma_i(\alpha)| \leq t$, so by AM-GM inequality we get

$$\left(\prod_{i=1}^n |\sigma_i(\alpha)|\right)^{\frac{1}{n}} \leq \frac{1}{n}\left(\sum_{i=1}^n |\sigma_i(\alpha)|\right) \leq \frac{t}{n}$$

giving $|\mathrm{Norm}_{K|\mathbb{Q}}(\alpha)| \leq \left(\frac{t}{n}\right)^n = c_K(N(I))$. □

Theorem 14.5.11. *Any class ideal $c \in C_K$ contains an ideal J such that $N(J) \leq c_K$, that is*

$$N(J) \leq \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n}\sqrt{|\Delta^2(K)|}$$

Proof. Let I be any ideal in the inverse class c^{-1}. As we know there exists a nonzero $\alpha \in I$ such that $|\mathrm{Norm}_{K|\mathbb{Q}}(\alpha)| \leq c_K N(I)$. As $(\alpha) \subseteq I$, we have $I|(\alpha)$, we have an ideal J such that $IJ = (\alpha)$. Thus $[J] = c$ and $J \in c$. Taking Norms,

$$N(I)N(J) = N(IJ) = |\mathrm{Norm}_{K|\mathbb{Q}}(\alpha)| \leq c_K N(I)$$

giving $N(J) \leq c_K$. □

Remark 14.5.12. For a nonzero ideal $J \subseteq \mathcal{O}_K$, we have $N(J) = \#\mathcal{O}_K/J$ so that $N(J)(x+J) \in J$ for any $x \in \mathcal{O}_K$ by Langrange's Theorem, viewning $\mathcal{O}_K/J$ as an additive group. Taking $x = 1$, we see that $N(J) \in J$. Thus $J \supseteq (N(J))$ and that $J|(N(J))$. Thus, every class c contains an ideal J such that J has an element $m \in J \cap \mathbb{N}$ with $m \leq c_K$ $(m = N(J))$.

Corollary 14.5.13. *If $K \neq \mathbb{Q}$, then $|\Delta^2(K)| > 1$*

Proof. As $N(J) \geq 1$ for any ideal $J \subseteq \mathcal{O}_K$, we have

$$1 \leq \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n}\sqrt{|\Delta^2(K)|} \leq \left(\frac{4}{\pi}\right)^n \frac{n!}{n^n}\sqrt{|\Delta^2(K)|}$$

Define $b_n := \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n}$. It suffices to show that $b_n > 1$ for all $n \geq 2$. Now,

$$\frac{b_{n+1}}{b_n} = \frac{\pi}{4}\left(1 + \frac{1}{n}\right)^n = \frac{\pi}{4}\left(1 + n\frac{1}{n} + \cdots\right) \geq \frac{\pi}{2} > 1$$

Thus $b_n > 1$ for all $n \geq 2$. □

Let c be any ideal class. Then there exists some $J \in c$ such that $N(J) \leq c_K$. Writing J as a product of prime ideals, we have $J = P_1 \dots P_s$. By multiplicativity of the norm, we have $N(P_i) \leq c_K$ for each i. Moreover, as $c = [J] = [P_1 \dots P_s] = [P_1] \dots [P_s]$, c is in the group generated by ideal classes of prime ideals of norm at most c_K. Thus the class group itself is generated by classes of prime ideals in $\mathcal{O}_K$ of norm at most c_K.

To find a suitable set of generators, note that prime ideals of norm at most c_K are factors of ideals (p) where $p \leq c_K$. By Dedekind, p factorises into prime ideals to get a complete set of generators.

To determine the class group, it remains to find any relations satisfied by the classes of these prime ideals. Relations can be obtained by the prime fcatorisation of ideals (p), noting (p) is principal, and others can be obtained by factoring principal ideals (α) generated by elements $\alpha \in \mathcal{O}_K$ of smaller norm.

To then show that these relations is complete, one needs to show that appropriate combinations of these generators are not principal. For complex quadratic fields, we can see that I is non-principal by checking all $\alpha \in \mathcal{O}_K$ such that $\mathrm{Norm}_{K|\mathbb{Q}}(\alpha) = N(I)$ and checking whether $I = (\alpha)$. If K is complex quadratic there are only finitely many possible α to check (by explicitly considering the norm).

Example 14.5.14. Let $K = \mathbb{Q}(\sqrt{-5})$ such that $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$. As $\mathcal{O}_K$ is not a PID (as it is not a UFD), so $h_K > 1$. Also, $n = 2, s = 1, r = 0$, and $\Delta^2(K) = -20$, so

$$c_K = \frac{2!}{2^2}\left(\frac{4}{\pi}\right)\sqrt{20} = \frac{4\sqrt{5}}{\pi} < 3$$

Thus every ideal class contains an ideal of norm at most 2, and that C_K is generated by classes of prime ideals of norm at most 2.

Now, $(2) = P_2^2$, where $P_2 = (2, 1 + \sqrt{-5})$, with $N(P_2) = 2$, so $[P_2]$ generates C_K. Now as $[P_2]^2 = [(2)] = [\mathcal{O}_K]$, C_k is cyclic of order 2 and thus $h_K = 2$.

Example 14.5.15. Taking $K = \mathbb{Q}(\sqrt{-6})$ for $\mathcal{O}_K = \mathbb{Z}[\sqrt{-6}]$ with $n = 2$, $r = 0$, $s = 1$ and $\Delta^2(K) = -24$, we have

$$c_K = \frac{2!}{2^2}\left(\frac{4}{\pi}\right)\sqrt{24} = \frac{4\sqrt{6}}{\pi} \approx 3.1$$

The ideal class group C_K is generated by classes of prime ideals P such that $N(P) \leq c_K$, meaning that $N(P) = 2$ or 3.

By Dedekind, $(2) = P_2^2$ where $P_2 := (2, \sqrt{-6})$ and $(3) = P_3^2$ with $P_3 = (3, \sqrt{-6})$. We have $N(P_2) = 2$ and $N(P_3) = 3$. Thus C_K is generated by $[P_2]$ and $[P_3]$. Neither of these are principal as no $(x + y\sqrt{-6})$ can have norm 2 or 3. Now,

$$\sqrt{-6} = \sqrt{-6} \cdot 3 + 2 \cdot \sqrt{-6} \in P_2 P_3$$

And $\mathrm{Norm}_{K|\mathbb{Q}}(\sqrt{-6}) = 6$, giving $(\sqrt{-6}) = P_2 P_3$. It follows that $[P_2][P_3] = [\mathcal{O}_K]$, again showing that C_K must be cyclic of order 2, generated by $[P_2]$ and $h_K = 2$.

Example 14.5.16. We find all integer solutions of the equation $y^2 + 54 = x^3$. Let $x, y \in \mathbb{Z}$ be a solution. If y is even, $x^3 \equiv 2 \bmod 4$, which is impossible. If $3|y$, then $3|x$, and setting $x = 3x_1, y = 3y_1$, we get $y_1^2 + 6 = 3x_1^3$. Thus $3|y_1$, and writing $y_1 = 3y_2$, we get $3y_2^2 + 2 = x_1^3$. However, $3y_2^2 + 2 \equiv 2$ or $5 \bmod 9$, whereas $x_1^3 \equiv 0, 1$ or $8 \bmod 9$. This contradiction shows y is coprime to 3.

In particular, $\gcd(y,6) = 1$, and thus $\gcd(x,6) = 1$. We now use the ideal factorization $(y + 3\sqrt{-6})(y - 3\sqrt{-6}) = (x)^3$. We claim the factors on the left are coprime. If a prime ideal divides both factors, then $6\sqrt{-6} = \{y + 3\sqrt{-6}\} - \{y - 3\sqrt{-6}\} \in P$, so $P|(6\sqrt{-6}) = P_2^3 P_3^3$. Thus P is either P_2 or P_3. On the other hand, as $P|(y + 3\sqrt{-6})$ implies that $P|(x)^3$, taking norms gives $N(P)|x^6$, which is impossible as $\gcd(x,6) = 1$. Thus these are coprime ideals of $\mathcal{O}_K$, and by unique factorisation of ideals, we have

$$(y + 3\sqrt{-6}) = I^3$$

for some ideal I. As I^3 is principal we know $[I^3] = [\mathcal{O}_K]$, and as $h_K = 2$, $[I]^2 = [\mathcal{O}_K]$ (by Langrange), giving $[I] = [\mathcal{O}_K]$. As I is principal, we have $I = (\alpha)$ for some $\alpha \in \mathcal{O}_K$.

It follows that $(y + 3\sqrt{-6}) = (\alpha)^3 = (\alpha)^3$, giving $y + 3\sqrt{-6} = u\alpha^3$ for some unit u. Units in $\mathcal{O}_K$ are ± 1, so for both of these we have $u = u^3$. Thus,

$$y + 3\sqrt{-6} = \{u\alpha\}^3 = \{a + b\sqrt{-6}\}^3$$

by equating coefficients and solving gives $3 = b(3a^2 - 6b^2)$ thus $1 = b(a^2 - 2b^2)$. Thus $b = -1$ and $a^2 = 1$, giving $y = a^3 - 18b^2 a = a(a^2 - 18b^2) = \pm 17$. With these y the only possible x is 7, giving solutions $x = 7, y = \pm 17$.

Example 14.5.17. Let $K = \mathbb{Q}(\sqrt{-163})$ such that $\mathcal{O}_K = \mathbb{Z}(\frac{1}{2}(1 + \sqrt{-163}))$. Then,

$$c_K = \frac{2}{\pi}\sqrt{163} \approx 8.13 < 9$$

Thus the class group C_K is generated by classes of prime ideals dividing $(2), (3), (5), (7)$. Note that the minimal polynomial of the generator is $x^2 - x + 41$. Modulo 2, this is $x^2 + x + 1$, which is irreducible. In particular, the only prime above 2 is (2), which is principal (we are using the fact $\mathcal{O}_K \simeq \mathbb{Z}[x]/(x^2 - x + 41)$ and the third isomorphism here). For $p = 3, 5, 7$, we use Dedekind and note that all polynomials $x^2 + 163 \bmod p$ is irreducible thus (p) is inert. Thus the only relevant prime ideals are principal. In particular, C_K is trivial and $h_K = 1$. Thus $\mathcal{O}_K$ is a UFD.

Example 14.5.18. The fact $h_K = 1$ for $K = \mathbb{Q}(\sqrt{-163})$ implies that $n^2 + n + 41$ is prime for $0 \le n \le 39$.

Suppose for a contradiction that n^2+n+41 is not prime for some $n < 40$. Now $n^2+n+41 < 41^2$ and so $n^2 + n + 41$ must have a prime factor $q < 41$.

Now,

$$q|n^2 + n + 41 = \left\{n + \frac{1}{2}(1 + \sqrt{-163})\right\}\left\{n + \frac{1}{2}(1 - \sqrt{-163})\right\}$$

However q does not divide either factor in $\mathcal{O}_K$ and so q cannot be prime in $\mathcal{O}_K$. As we are in a UFD, it follows that q cannot be irreducible. Thus $q = \alpha\beta$ where $\mathrm{Norm}_{K|\mathbb{Q}}(\alpha) = \mathrm{Norm}_{K|\mathbb{Q}}(\beta) = q$. If

$$\alpha = x + y\frac{1 + \sqrt{-163}}{2}$$

then

$$q = \mathrm{Norm}_{K|\mathbb{Q}}(\alpha) = \left(x + \frac{y}{2}\right)^2 + 163\left(\frac{y}{2}\right)^2$$

As q is not square we have $y \neq 0$, giving $q \ge 163/4 > 40$, which gives a contradiction.

Remark 14.5.19. With similar logic,

- $n^2 + n + 17$ is prime for $0 \le n \le 15$ with $\mathbb{Q}(\sqrt{-67})$.

- $n^2 + n + 11$ is prime for $0 \leq n \leq 9$ with $\mathbb{Q}(\sqrt{-43})$
- $n^2 + n + 5$ is prime for $0 \leq n \leq 3$ with $\mathbb{Q}(\sqrt{-19})$
- $n^2 + n + 3$ is prime for $0 \leq n \leq 1$ with $\mathbb{Q}(\sqrt{-11})$

Example 14.5.20. Taking $K = \mathbb{Q}(\sqrt{-29})$, we have $\mathcal{O}_K = \mathbb{Z}[\sqrt{-29}]$ and $\Delta^2(K) = -116$. We have $n = 2$ and $s = 1$, so

$$c_K = \left(\frac{2}{\pi}\right)\sqrt{116} \approx 6.9 < 7$$

C_K is thus generated by classes of prime ideals dividing $(2), (3)$ and (5). To factor these, by Dedekind,

- $x^2 + 29 \equiv (x+1)^2 \bmod 2$, so $(2) = P_2^2$ where $P_2 := (2, \sqrt{-29} + 1)$ of norm 2.
- $x^2 + 29 \equiv x^2 - 1 \equiv (x+1)(x-1) \bmod 3$, so $(3) = P_3 P_3'$, where $P_3 := (3, \sqrt{-29} + 1)$ and $P_3' := (3, \sqrt{-29} - 1)$ are distinct prime ideals of norm 3.
- $x^2 + 29 \equiv x^2 - 1 \equiv (x+1)(x-1) \bmod 5$, so $(5) = P_5 P_5'$ with $P_5 := (5, \sqrt{29} + 1)$ and $P_5' := (5, \sqrt{29} - 1)$ are distinct prime ideals of norm 5.

In particular, $[P]^2 = [P_3][P_3'] = [P_5][P_5'] = [\mathcal{O}_K]$. Thus C_K is generated by $[P_2], [P_3], [P_5]$. Considering $\mathrm{Norm}_{K|\mathbb{Q}}(x + y\sqrt{-29}) = x^2 + 29y^2$, there are no elements in $\mathcal{O}_K$ with norms $\pm 2, \pm 3, \pm 5$, meaning P_2, P_3, P_5 are not principal, and $[P_2]$ must have order 2.

The only element $\alpha \in \mathcal{O}_K$ of norm ± 9 is ± 3. Thus if $P_3^2 = (\alpha)$, then we have $P_3^2 = (3) = P_3 P_3'$, which implies $P_3 = P_3'$, a contradiction. Thus the order of $[P_3]$ is at least 3. We also cannot have order 3 as there are no solutions to $x^2 + 29y^2 = \pm 27$.

Considering $[P_5]$, note that $3^2 + 29 \times 2^2 = 125$, so that $N(3 + 2(\sqrt{-29})) = 5^3$. Thus, $(3 + 2\sqrt{-29})$ must be one of $P_5^3, P_5^2 P_5', P_5 P_5'^2, P_5'^3$. However, $2 + 2\sqrt{-29} \in P_5$, giving $3 + 2\sqrt{-29} \notin P_5$. Thus P_5 does not divide this, giving $(3 + 2\sqrt{-29}) = P_5'^3$, and taking conjugates shows $(3 - 2\sqrt{-29}) = P_5^2$. Thus $[P_5]$ has order dividing 3. As P_5 is not principal, the order of P_5 is exactly 3.

Finally,

$$(30) = (2)(3)(5) = (1 + \sqrt{-29})(1 - \sqrt{-29})$$

And from $(2)(3)(5) = P_2^2 P_3 P_3' P_5 P_5'$, we can deduce that $(1 \pm \sqrt{-29})$ must be of the form $P_2 P_3^* P_5^*$, and in either case, $[P_3]$ is in the group generated by $[P_2]$ and $[P_5]$. Thus, C_K is an abelian group generated by an element of order 2 and an element order 3. This gives a cyclic group of order 6. We can use the arguemtn above to explicitly find that $(2 + 5\sqrt{-29}) = P_3^6$ and $(2 - 5\sqrt{-29}) = P_3'^6$.

Example 14.5.21. Let $K = \mathbb{Q}(\sqrt{-37})$. Given that $h_K = 2$, we show that there are no integral solutions of the equation $y^2 = x^3 + 37$.

Suppose that $x, y \in \mathbb{Z}$ such that $y^2 + 37 = x^3$. Then as ideals we have

$$(y + \sqrt{-37})(y - \sqrt{-37}) = (x)^3$$

We claim these two are coprime ideals. Suppose that a prime ideal P divides both. Then $y \pm \sqrt{-37} \in P$, so that the difference $2\sqrt{-37} \in P$. Thus $P|(2\sqrt{-37})$ and since P is prime we conclude that $P|(2)$ or $P|(\sqrt{-37})$. As $\mathcal{O}_K = \mathbb{Z}[\sqrt{-37}]$, we factor (2) and (37) using the decomposition of $x^2 + 37$ modulo p. We have

- $x^2 + 37 \equiv (x+1)^2 \bmod 2$, giving $(2) = P_2^2$ where $P_2 := (2, 1 + \sqrt{-37})$

- $x^2 + 37 \equiv x^2 \bmod 37$, so $(37) = (37, \sqrt{-37})^2 = P_{37}^2$, where $P_{37} := (\sqrt{-37})$ is a prime of norm 37.

It follows that if P is a common factor of $(y + \sqrt{-37})$ and $(y - \sqrt{-37})$, then $P = P_2$ or $P = P_{37}$. In either case, as $P|(y + \sqrt{-37})$, we have $P|(x)^3$, taking norms we get $2|x^6$ or $37|x^6$ respectively. Thus either $2|x$ or $37|x$.

If $37|x$, then from our original equation we have $37|y$. Thus 37^2 divides $x^3 - y^2 = 37$, a contradiction. If $2|x$, we have $8|x^3$, but then $y^2 + 1 \equiv 0 \bmod 4$, a contradiction.

Thus $(y + \sqrt{-37})$ and $(y - \sqrt{-37})$ are coprime ideals. Their products is a cube, thus by unique factorisation of ideals we have

$$(y + \sqrt{-37}) = I^3$$

for some ideal I. As I^3 is principal, the order of $[I]$ in C_K divides 3. As $h_K = 2$, I must be principal. Thus,

$$(y + \sqrt{-37}) = (a + b\sqrt{-37})^3$$

for some $a, b \in \mathbb{Z}$. In particular, $y + \sqrt{-37} = u(a + b\sqrt{-37})^3$ for some unit $u \in \mathcal{O}_K$. As the only such units are ± 1, we have $u = u^3$, so we may replacing a, b by $-a, -b$ if appropriate, we may assume that $u = 1$. Expanding, we get $y = a(a^2 - 111b^2)$ and $1 = b(3a^2 - 37b^2)$. The second equation implies that $b = \pm 1$ and $3a^2 - 37 = \pm 1$. No such a exists.

14.6 Fermat's Theorems

Definition 14.6.1. *Let p be prime and $m \in \mathbb{Z}$. m is a* ***quadratic residue*** *mod p if there exists a $x \in \mathbb{Z}$ such that $m \equiv x^2$ (mod p). Otherwise, m is a quadratic non-residue mod p.*

Lemma 14.6.2. *For any prime $p \neq 2$, define $\psi : \mathbb{Z}_p^* \to \mathbb{Z}_p^*$ by $x \mapsto x^2$. This is a 2-to-1 map. In particular, exactly half of $\{1, \ldots, p-1\}$ are quadratic residues mod p, and half are quadratic non-residues mod p.*

Proof. Follows by observing the kernel and also noting that $\psi(x) = \psi(p - x)$. □

Definition 14.6.3. *For a prime p and $p \not| m$, define the* ***Legendre symbol*** *by*

$$\left(\frac{m}{p}\right) = \begin{cases} 1 & \textit{if } m \textit{ is a quadratic residue mod } p \\ -1 & \text{otherwise} \end{cases}$$

When $p|m$, define $\left(\frac{m}{p}\right) = 0$.

Lemma 14.6.4. *Let p be an odd prime and $p \not| m, n, m_1, m_2$. Then,*

- *If $m_1 \equiv m_2$ mod p, then $\left(\frac{m_1}{p}\right) = \left(\frac{m_2}{p}\right)$*
- $\left(\frac{mn}{p}\right) = \left(\frac{m}{p}\right)\left(\frac{n}{p}\right)$
- $\left(\frac{-1}{p}\right) = 1 \iff p \equiv$ (mod 4) *or* $p = 2$. $\left(\frac{-1}{p}\right) = -1 \iff p \equiv 3$ (mod 4).
- $\left(\frac{2}{p}\right) = 1 \iff p \equiv \pm 1$ (mod 8). $\left(\frac{2}{p}\right) = -1 \iff p \equiv \pm 3$ (mod 8).

Theorem 14.6.5 (Gauss's Law of Quadratic Reciprocity)**.** *Let $p \neq 2$, $q \neq 2$ be distinct primes. If either $p \equiv 1$ or $q \equiv 1$ mod 4, then $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$. If both $p \equiv 3$ and $q \equiv 3$ mod 4, then $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$.*

Theorem 14.6.6. *If p is prime and $p \equiv 1 \bmod 4$, then there exists $a, b \in \mathbb{Z}$ such that $p = a^2 + b^2$ and this decomposition is unique.*

Proof. Assume that $p \equiv 1$ mod 4. Then we have $(frac{-1}p) = 1$, so there exists some $r \in \mathbb{Z}$ such that $p|1+r^2$. Extending to $\mathbb{Z}[i]$, we have $p|(1+ri)(1-ri)$. If p is irreducible in $\mathbb{Z}[i]$, then $p|(1+ri)$ or $p|(1-ri)$, as any irreducible is prime. However, p cannot divide $1+ri$ for example, as $\frac{1}{p} + \frac{r}{p}i \notin \mathcal{O}_K$. Thus we can write $p = (a+bi)(c+di)$ neither units. Taking norms,

$$p^2 = (a^2+b^2)(c^2+d^2)$$

As $\mathbb{Z}$ is a UFD and neither $a+bi$ or $c+di$ has norm ± 1, we have $p = a^2+b^2 = (a+bi)(a-bi)$. This shows existence. If $a+bi = \alpha\beta \in \mathbb{Z}[i]$, taking norms gives

$$p = \text{Norm}(\alpha)\text{Norm}(\beta)$$

Thus α or β must be a unit. Hence $a+bi$ is irreducible in $\mathbb{Z}[i]$ and similarly for $a-bi$. Hence $p = (a+bi)(a-bi)$ is the unique factorisation of p into irreducibles. If $p = e^2+f^2 = (e+fi)(e-fi)$, then $e+fi$ is an associate of $a+bi$ or $a-bi$, and in any case $\{a^2, b^2\} = \{e^2, f^2\}$. □

Theorem 14.6.7. *The only integer solutions of $y^2+2 = x^3$ are $x = 3, y = \pm 5$*

Proof. If y were even then x is also even, giving $8|y^2+2$ which is impossible since $4|y^2$. Thus y is odd. We can decompose $(y+\sqrt{-2})(y-\sqrt{-2}) = x^3$. Suppose that there is an irreducible element α which divides both $y+\sqrt{-2}$ and $y-\sqrt{-2}$. Then α divides the difference $2\sqrt{-2} = \sqrt{-2}^3$. However, $\sqrt{-2}$ is irreducible since its norm is 2, which is prime in $\mathbb{Z}$. Hence we must have $\alpha = \pm\sqrt{-2}$. Now,

$$\alpha|y+\sqrt{-2} \implies \sqrt{-2}|y \implies 2|y^2$$

which is a contradiction as y is odd. Hence $y+\sqrt{-2}$ and $y-\sqrt{-2}$ are coprime. Unique factorisation of $\mathbb{Z}[\sqrt{-2}]$ implies that $y+\sqrt{-2}$ and $y-\sqrt{-2}$ are associates of cubes. As the only units are ± 1. they are indeed both cubes. Now,

$$y+\sqrt{-2} = (a+b\sqrt{-2})^3$$

solving gives $(a^3-6ab^2)+(3a^2b-2b^3)\sqrt{-2}$. Thus $b(3a^2-2b^2) = 1$. Giving $b = \pm 1$ and $a = \pm 1$. Substituting these combinations, we get $y = \pm 5$, thus $x = 3$. □

15 Notes

In Lemma 12.0.5, we note the transpose is due to the fact that we order elements in the det on elements to be placed by row, whereas the change of basis works column-wise.

characteristic 0, separable -> min poly irreducible has no repeated roots -> has degree many embeddings

The $\mathbb{Z}$ basis for $\mathcal{O}_K$ generates K as a $\mathbb{Q}$ basis, as for any algebraic α, there is some $n\alpha \in \mathcal{O}_K$.

Ideals inside Ok are generated by n elements as they are submodules of Z^n

If $\mathcal{O}_K$ has integral basis $w_1, \ldots, w_n$, then we can view

$$\mathcal{O}_K \simeq \bigoplus_{i=1}^{n} \mathbb{Z}w_i$$

as an isomorphism of abelian groups. Also, $n := [K : \mathbb{Q}]$. Given any principal ideal (a) in $\mathcal{O}_K$, we have

$$(a) = a\mathcal{O}_K \simeq \bigoplus_{i=1}^{n} a\mathbb{Z}w_i$$

because $aw_1, \ldots, aw_n$ is an integral basis for (a). In particular,

$$O_K/(a) \simeq \bigoplus_{i=1}^{n} \mathbb{Z}w_i / \bigoplus_{i=1}^{n} a\mathbb{Z}w_i = \bigoplus_{i=1}^{n} (\mathbb{Z}/a\mathbb{Z})w_i \simeq (\mathbb{Z}/a\mathbb{Z})^n$$

Remark 15.0.1. Note first that every ideal in $\mathcal{O}_K$ can be written with at most 2 generators. (Proof. prime ideals height c over a noetherian ring can be generated by c elements, and the height of any maximal ideal in $\mathcal{O}_K$ is 2) Thus, write (α, β) for the ideal $(\alpha) + (\beta)$. Then the product

$$(\alpha, \beta)(\gamma, \delta) = \{\sum_{i=1}^{n} \mu_i\nu_i \mid \mu_i \in (\alpha, \beta), \nu_i \in (\gamma, \delta)\}$$

clearly contains $\alpha\gamma, \alpha\delta, \beta\gamma, \beta\delta$. On the other hand, $\mu_i\nu_i$ is of the shape $(\alpha a + \beta b)(\gamma c + \delta d) \in (\alpha\gamma, \alpha\delta, \beta\gamma, \beta\delta)$. Thus,

$$(\alpha, \beta)(\gamma, \delta) = (\alpha\gamma, \alpha\delta, \beta\gamma, \beta\delta)$$

Reducing generators explicitly can be done using ad-hoc methods (usually just expanding and double inclusion).

15.1 Fermat's Last Equation for the Cubic

We prove in this subsection that $x^3 + y^3 = z^3$ has no nontrivial solutions in $\mathbb{Z}$. We work in $K = \mathbb{Q}(\sqrt{-3})$, and we write

$$\omega = \frac{-1+\sqrt{-3}}{2}$$

such that $\mathcal{O}_K = \mathbb{Z}[\omega]$ for the rest of this subsection.

Lemma 15.1.1. *We have the following:*

- $\omega^3 = 1$. *The units of* $\mathcal{O}_K$ *are* $\pm 1, \pm\omega, \pm\omega^2$.
- *The ring* $\mathcal{O}_K$ *is a UFD.*
- *The element* $\lambda := \sqrt{-3}$ *is prime with norm 3. Moreover we have* $\lambda = \omega(1-\omega) = (-\omega^2)(1-\omega^2)$.

Proof. Note that to find the units, we look for $\mathrm{Norm}_{K|\mathbb{Q}}(a + b\omega) = a^2 - ab + b^2 = \pm 1$. The set of solutions that satisfy this gives exactly the above units. To show $\mathcal{O}_K$ is a UFD, it suffices to show that $\mathbb{Q}(\sqrt{-3})$ has class number 1. This is actually immediate as we have

$$c_K = \left(\frac{2}{\pi}\right)\sqrt{3} \approx 1.103 < 2$$

Thus every ideal class contains a prime ideal whose norm is at most 1, and in particular every ideal class contains a principal ideal, thus actually simply has class number 1. The last case follows by a simple check. □

Lemma 15.1.2. *If* $\alpha \in \mathbb{Z}[\omega]$ *and* λ *does not divide* α, *then* $\alpha^3 = \pm 1$ *mod* λ^4.

16 Preliminaries

16.0.1 Linear Maps

Definition 16.0.1. *Let* V *be a vector space over a field* k. *Define* $\mathrm{GL}(V)$ *to be the set of invertible linear maps, with group operation defined by composition.*

Proposition 16.0.2. *Let* $g \in \mathrm{GL}(V)$ *be an element of finite order and suppose that* k *is algebraically closed with 0 characteristic. Then* g *is diagonalizable.*

Proof. Let n be the order of $g \in \mathrm{GL}(V)$. Then $g^n = 1$, so g is annihlated by the polynomial $f(x) := x^n - 1$. The $m_g | f$, but as f splits in k and has no repeated roots, $m_g(x)$ splits into distinct linear factors. Hence g is diagonalizable by the Primary Decomposition Theorem. □

Remark 16.0.3. The converse does not hold in general. Consider $k = \overline{\mathbb{F}_2}$, $V = k\{e_1, e_2\}$ and $g \in \mathrm{GL}(V)$ be given by $g(e_1) = e_1, g(e_2) = e_1 + e_2$. Then $g^2 = 1$, and $m_g(x) = x^2 - 1 = (x-1)^2$. This has repeated roots, hence not diagonalizable.

16.0.2 Direct Sum

Definition 16.0.4. *Let V and W be vector spaces. The* ***external direct sum*** *is the vector space $V \oplus W := V \times W$.*

Remark 16.0.5. The external direct sum is consistent with the internal direct sum by identifying V and W with their images $\{(v,0) \mid v \in V\}$ and $\{(0,w) \mid w \in W\}$ inside $V \times W$. The sum of their images is all of $V \times W$ and the intersection is $\{(0,0)\}$.

Definition 16.0.6. *The* ***dual space*** *of a vector space V over $\mathbb{F}$ is $\mathrm{Hom}(V, \mathbb{F})$, where addition is defined pointwise and multiplication by composition.*

Remark 16.0.7. Idempotent actions decompose vector spaces. That is, if $P : V \to V$ with $P^2 = P$, then we can write

$$V = P(V) \oplus \ker P$$

noting that we can write $v = P(v) + (v - P(v))$.

16.0.3 Tensor Product

Definition 16.0.8. *Let V and W be two vectos spaces, with $\{v_1, \dots, v_m\}$ and $\{w_1, \dots, w_n\}$ as basis for V and W respectively. The* ***tensor product*** *of V and W, written $V \times W$ is the free vector space on the set of formal symbols*

$$\{v_i \otimes w_j \mid 1 \le i \le m, 1 \le j \le n\}$$

If $v = \sum_{i=1}^m \lambda_i v_i$ and $w = \sum_{j=1}^n \mu_j w_j$ are elements of V and W respectively, we define the elementary tensor

$$v \otimes w := \sum_{i=1}^m \sum_{j=1}^n \lambda_i \mu_j (v_i \otimes w_j) \in V \otimes W$$

Remark 16.0.9. We note the following results, which are immediate from definition.

- $\dim V \otimes W = (\dim V)(\dim W)$
- The elementary tensors span $V \otimes W$
- Not every element of $V \otimes W$ is an elementary tensor $v \otimes w$.

The free vector space does not depend on the choice of basis.

Lemma 16.0.10. *Let $\{v'_1, \dots, v'_m\}$ and $\{w'_1, \dots, w'_n\}$ be any choice of basis for V and W. Then,*

$$X' := \{v'_i \otimes w'_j \mid 1 \le i \le m, 1 \le j \le n\}$$

is a basis for $V \otimes W$.

Proof. We note that elementary tensors in $V \otimes W$ distribute, in the sense that

$$(v + v') \otimes (w + w') = (v \otimes w) + (v \otimes w') + (v' \otimes w) + (v' \otimes w')$$

for all $v, v' \in V$, $w, w' \in W$, and hence

$$(\lambda v) \otimes w = \lambda(v \otimes w) = v \otimes (\lambda w)$$

for all $v \in V, w \in W, \lambda \in k$. Hence, we can write each v_i as a linear combination of $\{v'_1, \dots, v'_m\}$ and each w_j as a linear combination of $\{w'_1, \dots, w'_n\}$, and see that the original basis vectors $v_i \otimes w_j$ of $V \otimes W$ all lie in the span of X'. As the size of this set is at most mn, it must be linearly independent, thus a basis. □

Remark 16.0.11. The above proof also shows that the canonical map $\otimes : V \times W \to V \otimes W$ by $(v, w) \mapsto v \otimes w$ is bilinear, such that

$$(\lambda v_1 + v_2) \otimes (\mu w_1 + w_2) = \lambda\mu(v_1 \otimes w_1) + \lambda(v_1 \otimes w) + \mu(v_2 \otimes w_1) + (v_2 \otimes w_2)$$

Lemma 16.0.12 (Universal Property of Tensor Product)**.** *Let V and W be vector spaces. Then for every blinear map $b : V \times W \to U$ for some third vector space U, we have a unique linear map $\tilde{b} : V \otimes W \to U$ such that the following commutes:*

$$\begin{tikzcd}
V \times W \arrow[r, "b"] \arrow[d] & U \\
V \otimes W \arrow[ur, "\tilde{b}"'] &
\end{tikzcd}$$

Proof. Fix bases $\{v_1, \dots, v_m\}$ for V and $\{w_1, \dots, w_n\}$ for W. Fixing a bilinear map $b : V \times W \to U$, this forces any $\tilde{b} : V \otimes W \to U$ to be the unique linear map that sends the basis vector $v_i \otimes w_j \in V \otimes W$ to $b(v_i, w_j)$, if it exists. It thus suffices to show this map commutes with any element in $V \times W$. Taking any $v = \sum_i \lambda_i v_i \in V$ and $w = \sum_j \mu_j w_j \in W$, $\tilde{b}$ sends the elementary tensor $v \otimes w = \sum_{i,j} \lambda_i \mu_j v_i \otimes w_j$ to

$$\sum_{i,j} \lambda_i \mu_j b(v_i, w_j) = b\left(\sum_i \lambda_i v_i, \sum_j \mu_j w_j\right) = b(v, w)$$

by using the bilinearity of b. □

16.0.4 Module Endomorphisms

Definition 16.0.13. *The **center** of the ring A is*

$$Z(A) := \{z \in A \mid az = za, \textit{for all } a \in A\}$$

The center is a commutative unital subring of A.

Definition 16.0.14. *Let A be a ring and V be an A-module. The **endomorphism ring** of V, denoted* $\mathrm{End}_A(V)$ *is the set of all A-module homomorphisms $\psi : V \to V$ equipped with pointwise addition of homomorphisms and composition as multiplication.*

Remark 16.0.15. When V is an A-module, it is an $\mathrm{End}_A(V)$-module via evaluation, $f \cdot v := f(v)$, for $f \in \mathrm{End}_A(V)$ and $v \in V$. The two actions of A and $\mathrm{End}_A(V)$ on V commute pointwise by definition. In particular, the action of any central element $z \in Z(A)$ on V is by an A-module endomorphism.

Definition 16.0.16. *A ring A is an **k-algebra** if it contains k as a central subfield. If A is a semisimple ring, we say that A is a **semisimple k-algebra**. A **homomorphism** of k-algebras is a k-linear ring homomorphism.*

k being inside the center allows it to 'act' like the scalar, making the definition of homomorphism the way we think of it naturally.

16.0.5 Group and Module Notations

Definition 16.0.17. *Let G be a finite group and let $g \in G$. Define*

- *g^G to denote the* ***conjugacy class*** *of g in G,*

$$g^G := \{g^x \mid x \in G\} where\ g^x := x^{-1}gx$$

- *$C_G(g)$ denotes the* ***centraliser*** *of g in G, with*

$$C_G(g) := \{x \in G \mid gx = xg\}$$

Remark 16.0.18. By The Orbit Stabilizer on the conjugation action, we have $|g^G| \cdot |C_G(g)| = |G|$ for any $g \in G$, where g^G is the conjugacy class, and the stabilizer of g is exactly the centraliser.

Definition 16.0.19. *Let V be a $\mathbb{C}G$-module. The* ***invariant submodule*** *of V is*

$$V^G := \{v \in V \mid g \cdot v = v, for\ all\ g \in G\}$$

16.0.6 Algebraic Numbers

Notation 16.0.20. We write $\mathbb{A}$ for the set of algebraic integers over $\mathbb{Q}$. Note that the set of algebraic numbers is the union of all subfields of $\mathbb{C}$ of finite dimension as a $\mathbb{Q}$-vector space.

Remark 16.0.21. Note the following:

- Any integer is an algebraic integer by the linear function
- Any root of unity is an algebraic integer
- If z is an algebraic number, then mz is an algebraic integer for some integer m
- $\mathbb{Q} \cap \mathbb{A} = \mathbb{Z}$ (by taking any element of the form r/s, taking it's monic polynomial, clearing denominators to show that s divides r).

Proposition 16.0.22. *Let M be a finitely generated subgroup of $(\mathbb{C}, +)$. Then*

$$\{z \in \mathbb{C} \mid zM \subseteq M\} \subseteq \mathbb{A}$$

17 Definitions and Examples

Definition 17.0.1. *Let G be a finite group and let V be a finite dimensional vector space over k. A* ***representation*** *of G on V is a group homomorphism*

$$\rho : G \to \mathrm{GL}(V)$$

The ***degree*** *of a representation is* $\dim V$.

Example 17.0.2. We record some examples of representations.

- The cyclic group $G = \langle g \rangle$ of order 2 acts on $V = k$ by negation taking $\rho(g) = -1$, giving a representation of G degree 1.

- If $G = D_6$ is the symmetry group of a triangle and $k = \mathbb{R}$, then G acts by $\mathbb{R}$-linear transformations on the plane $V = \mathbb{R}^2$, giving a representation. In general, the symmetry group of the regular n-gon $G = D_{2n}$ acts on $V = \mathbb{R}^2$ by $\mathbb{R}$-linear transformations, giving a natural representation of G of degree 2.

- Let $k = \mathbb{R}$ and let $X \subseteq \mathbb{R}^3$ be the se tof vertices of a cube centered at the origin, and let G be the stabilizer of X in the rotation group $SO_3(\mathbb{R})$. Then G is isomorphic to the symmetry group S_4, giving a degree 3 representation $S_4 \to \mathrm{GL}(\mathbb{R}^3)$.

Example 17.0.3. Ex 1.6 from RT, gal group into base field automorphisms

18 Representation of Finite Groups

Definition 18.0.1. *Let X be a finite set. The* ***free vector space on** X* *is the set*

$$kX := \left\{ \sum_{x \in X} a_x x \mid a_x \in k \right\}$$

of ***formal linear combinations*** *of members of X with coefficients a_x lying in k. Addition and scalar multiplication are taken as the natural ones.*

Remark 18.0.2. Note that X is naturally a basis for kX.

Let X be a finite set equipped with a left-action of the finite group G. Each $g \in G$ gives a permutation $\rho(g) : X \to X$ by $\rho(g)(x) = g \cdot x$. This permutation extends uniquely to an invertible linear map $\rho(g) : kX \to kX$ by

$$\rho(g) \left(\sum_{x \in X} a_x x \right) = \sum_{x \in X} a_x g \cdot x$$

Since $g \cdot (h \cdot x) = (gh) \cdot x$ for any $g, h \in G$ and $x \in X$, we have $\rho(g)\rho(h) = \rho(gh)$ in $\mathrm{GL}(kX)$ for all $g, h \in G$. Thus $\rho : G \to \mathrm{GL}(kX)$ is a representation.

Definition 18.0.3. *Noting the remark above, given X is a finite set equipped with a left action by a finite group G, $\rho : G \to \mathrm{GL}(kX)$ is a representation, called the* ***permutation representation associated with** X.*

Definition 18.0.4. *The representation $\rho : G \to \mathrm{GL}(V)$ is* ***faithful*** *if* $\ker \rho = \{1\}$.

Definition 18.0.5. *Let G be a finite group. A* ***matrix representation*** *is a group homomorphism $\rho : G \to \mathrm{GL}_n(k)$, where $\mathrm{GL}_n(k) = M_n(k)^\times$ is the group of invertible $n \times n$ matrices under matrix multiplication.*

Definition 18.0.6. *Let $\mathcal{B} := \{v_1, \ldots, v_n\}$ be a basis for V and let $\phi : V \to V$ be a linear map.The* ***matrix of ϕ with respect to $\mathcal{B}$*** *is ${}_{\mathcal{B}}[\phi]_{\mathcal{B}} = (a_{ij})_{i,j=1}^n$ where*

$$\phi(v_j) = \sum_{i=1}^n a_{ij} v_i$$

for all $j = 1, \ldots, n$.

Remark 18.0.7. Let V be a vector space V with basis $\mathcal{B}$. Then,

- The map $\phi \mapsto_{\mathcal{B}} [\phi]_{\mathcal{B}}$ gives an isomorphism of groups $\mathrm{GL}(V) \cong \mathrm{GL}_n(k)$.
- Every representation $\rho : G \to \mathrm{GL}(V)$ gives rise to a matrix representation

  $$\rho_{\mathcal{B}}(g) :=_{\mathcal{B}} [\rho(g)]_{\mathcal{B}}$$

  for all $g \in G$.
- Every matrix representation $\sigma : G \to \mathrm{GL}_n(k)$ defines a representation $\underline{\sigma} : G \to \mathrm{GL}(k^n)$ on the space k^n of column vectors, taking $\underline{\sigma} : k^n \to k^n$ be the k-linear map

  $$\underline{\sigma}(g)(v) = \sigma(g)v$$

  for all $g \in G, v \in k^n$ via matrix multiplication. By abuse of notation, the underline is sometimes omitted.

Example 18.0.8. Let $G = S_3$ act on $X = \{e_1, e_2, e_3\}$ by permutation of indices. This gives a degree 3 permutation representation $\rho : G \to \mathrm{GL}(kX)$ where for instance,

$$\rho_X((123)) = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

Definition 18.0.9. *Let $\rho : G \to \mathrm{GL}(V)$ and $\sigma : G \to \mathrm{GL}(W)$ be two representations. A **homomorphism**, also known as the **intertwining operator** is a linear map*

$$\psi : V \to W$$

such that

$$\sigma(g) \circ \psi = \psi \circ \rho(g)$$

*for all $g \in G$. We say that ψ is an **isomorphism** if it is bijective.*

Definition 18.0.10. *Two matrix representations $\rho_1 : G \to \mathrm{GL}_n(k)$ and $\rho_2 : G \to \mathrm{GL}_n(k)$ are said to be **equivalent** if there exists $A \in \mathrm{GL}_n(k)$ such that*

$$\rho_2(g) = A\rho_1(g)A^{-1}$$

for all $g \in G$.

Remark 18.0.11. If ρ_1 and ρ_2 are equivalent matrix representations, then the equality of products of matrices $\rho_2(g)A = A\rho_1(g)$ translates to an equality of linear maps

$$\underline{\rho_2(g)} \circ \underline{A} = \underline{A} \circ \underline{\rho_1(g)}$$

in $\mathrm{GL}(k^n)$, meaning that representations $\underline{\rho_1}$ and $\underline{\rho_2}$ are isomorphic. The converse is also true.

Definition 18.0.12. *Let $\rho : G \to \mathrm{GL}(V)$ be a representation, and let U be a linear subspace of V. Then,*

- *U is G-**stable** if $\rho(g)(u) \in U$ for all $g \in G$ and $u \in U$.*
- *Suppose that U is G-stable. Then the **subrepresentation of** ρ **afforded by** U is*

  $$\rho_U : G \to \mathrm{GL}(U)$$

  given by $\rho_U(g)(u) := \rho(g)(u)$ for all $g \in G$, $u \in U$.

- *Suppose that U is G-stable. The **quotient representation of ρ afforded by U** is*

$$\rho_{V/U} : G \to \mathrm{GL}(V/U)$$

given by $\rho_{V/U}(g)(v+U) := \rho(g)(v) + U$ for all $g \in G$ and $v + U \in V/U$.

Note that the maps are well defined when U is G-stable.

Lemma 18.0.13 (First Isomorphism For Representations)**.** *Let $\psi : V \to W$ be a homomorphism between representations $\rho : G \to \mathrm{GL}(V)$ and $\sigma : G \to \mathrm{GL}(W)$. Then,*

1. $\ker\psi$ *is a G-stable is a subspace of V.*
2. $\mathrm{Im}\ \psi$ *is a G-stable subspace of W*
3. *There is a natural isomorphism*
$$V/\ker\psi \cong \mathrm{Im}\ \psi$$
between G-representations $\rho_{V/\ker\psi}$ and $\sigma_{\mathrm{Im}\ \psi}$

Proof. We note the commutative diagram

$$\begin{tikzcd}
V \arrow[r, "\rho(g)"] \arrow[d, "\psi"'] & V \arrow[d, "\psi"] \\
W \arrow[r, "\sigma(g)"'] & W
\end{tikzcd}$$

Then the first two cases are clear. We note the quotient representation of ρ afforded by $\ker\psi$ and the subrepresentation of σ afforded by Im ψ induces a map $\Psi : V/\ker(\psi) \to \mathrm{Im}\ \psi$ with $v + \ker(\psi) \mapsto \psi(v)$ alongside a commutative diagram

$$\begin{tikzcd}
V/\mathrm{ker}\ \psi \arrow[r, "\rho_{V/\mathrm{ker}\ \psi}(g)"] \arrow[d, "\Psi"'] & V/\mathrm{ker}\ \psi \arrow[d, "\Psi"] \\
\mathrm{Im}\psi \arrow[r, "\sigma_{\mathrm{Im}\psi}(g)"'] & \mathrm{Im}\psi
\end{tikzcd}$$

In particular, $V/\ker\psi \cong \mathrm{Im}\ \psi$. □

Definition 18.0.14. *Let G be a group. The **trivial representation** of G on a vector space V, $\mathbb{1} : G \to \mathrm{GL}(V)$ given by*

$$\mathbb{1}(g)(v) = v$$

for all $g \in G$, $v \in V$.

Example 18.0.15. A representation need not be trivial, even if the subrepresentation and quotient representation are both trivial.

Let $k = \mathbb{F}_p$ and $G = \langle g \rangle$ be the cyclic group of order p. Let $\rho : G \to \mathrm{GL}_2(k)$ be the matrix representation given by

$$\rho(g^i) = \begin{pmatrix} 1 & i \\ 0 & 1 \end{pmatrix}$$

Let v_1, v_2 be the standard basis for $V = k^2$. Then $U := \langle v_1 \rangle$ is a G-stable subspace, as $\rho(g^i)(v_1) = v_1$ for all i. The subrepresentation $\rho_U : G \to \mathrm{GL}(U)$ and the quotient representation $\rho_{V/U} : G \to \mathrm{GL}(V/U)$ are both trivial, but ρ is clearly not trivial.

Definition 18.0.16. *the representation $\rho : G \to \mathrm{GL}(V)$ to a nonzero V is **irreducible** or **simple** if U being a G-stable subspace of V implies that either $U = \{0\}$ or $U = V$.*

Definition 18.0.17. *Let $\rho : G \to \mathrm{GL}(V)$ be a representation and U be a G-stable subspace. A **G-stable complement** for U in V is a G-stable subspace W such that $V = U \oplus W$.*

Example 18.0.18. Consider the permutation representation of $G = S_3$ afforded by kX, where $X = \{e_1, e_2, e_3\}$. Then

$$U := \langle e_1 + e_2 + e_3 \rangle$$

is a G-stable subspace, with G fixing every vector in U. So U is a trivial subrepresentation of V. Now let

$$W := \{a_1e_1 + a_2e_2 + a_3e_3 \mid a_1 + a_2 + a_3 = 0\}$$

This is a G-stable complement to U in V, provided $\mathrm{char}(k) \neq 3$. Let $\mathcal{B} = \{v_1, v_2\}$ be the basis for W, where $v_1 := e_1 - e_2$ and $v_2 = e_1 - e_3$. Then the degree 2 matrix representation $\sigma := (\rho_W)_{\mathcal{B}} : G \to \mathrm{GL}_2(k)$ afforded by W is determined by

$$\sigma((123)) = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix} \qquad \sigma((12)) = \begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix}$$

Proposition 18.0.19. *The nontrivial S_n-stable subspaces of the permutation representation $\rho : S_n \to \mathrm{GL}(kX)$ are $V = \langle \sum_{i=1}^n x_i \rangle, W = \{\sum_{i=1}^n a_i x_i \mid \sum_i a_i = 0\}$*

Proof. Sketch: $\dim V = 1$, so non nontrivial stable subspaces are contained in V. Taking any stable subspace U with nontrivial intersection with V, we show that this at least contains W. As $\dim W = n - 1$, either this is W or kX. □

Proposition 18.0.20. *Let X be a G-set and that the permutation representation $\rho : G \to \mathrm{GL}(kX)$ is irreducible. Then, the G-action on X is transitive. The converse need not hold.*

Proof. Suppose for a contradiction the G-action on X is not transitive. Then there is an $x \in X$ whose G-orbit $G \cdot x$ is a proper subset of X. In particular, $\emptyset \subsetneq \{x\} \subsetneq G \cdot x \subsetneq X$. Thus,

$$\{0\} \nleq k(G \cdot x) \nleq kX$$

Given any $g \in G$, $h \cdot x \in G \cdot x \subseteq k(G \cdot x)$,

$$\rho(g)(h \cdot x) = g \cdot (h \cdot x) = (gh) \cdot x \in G \cdot x \subseteq k(G \cdot x)$$

Thus as $G \cdot x$ is a natural basis for $k(G \cdot x)$, this is $\rho(g)$-invariant. This is a proper G-stable subspace, hence the permutation representation is reducible.

To see the converse is false, the permutation representation is reducible, but the S_n action on n elements is clearly transitive. □

Theorem 18.0.21 (Maschke)**.** *Let G be a finite group and suppose that $|G| \neq 0$ in k. Let U be a G-stable subspace of a finite dimensional G-representation V. Then U admits at least one G-stable complement W in V.*

Proof. Pick a basis for U and extend it to a basis for V such that we find some Z with $V = U \oplus Z$. Z is not G-stable in general, but we will replace this with a stable one. Let $\rho : G \to \mathrm{GL}(V)$ be our representation, writing $g \cdot v := \rho(g)(v)$ as ρ is a group homomorphism.

Let $\pi : V \to V$ be the projection map along the decomposition $V = U \oplus Z$ such that $\pi(u+z) = u$ for all $u \in U, z \in Z$. Now define a new linear map $\psi : V \to V$ by

$$\psi(v) := \frac{1}{|G|} \sum_{x \in G} \rho(x)\pi(\rho(x)^{-1}(v))$$

for all $v \in V$. Note that this is well-defined as $|G|$ is invertible in the field k. Fixing a $g \in G$ and $v \in V$, we have

$$|G|\psi(g \cdot v) = \sum_{x \in G} x \cdot \pi(x^{-1} \cdot (g \cdot v))$$

Writing $y^{-1} = x^{-1}g$, noting that x runs over the entire group in the sum, we get

$$|G|\psi(g \cdot v) = \sum_{y \in G} (gy) \cdot \pi(y^{-1} \cdot v) = g \cdot \sum_{y \in G} y \cdot \pi(y^{-1} \cdot v) = g \cdot |G|\psi(v)$$

Cancelling $|G|$, we deduce that ψ is a homomorphism of representations. Also, for any $u \in U$,

$$\psi(u) = \frac{1}{|G|} \sum_{x \in G} x \cdot \pi(x^{-1} \cdot u) = \frac{1}{|G|} \sum_{x \in G} x \cdot (x^{-1} \cdot u) = u$$

noting that as U is G-stable, $\pi(x^{-1} \cdot u) = x^{-1} \cdot u$ for all $x \in G$. So the restriction of ψ to U is the identity map. As U is G-stable and $\pi(V) = U$, we have $\psi(V) \subseteq U$. As $\psi(U) = U$, we have $\psi(V) = U$. With $\mathrm{Im}(\psi) = U$, taking $W := \ker \psi$ gives a G-stable subspace of V. Noting that $\dim W + \dim U = \dim V$ by Rank Nullity and for any $v \in W \cap V$, $0 = \psi(v) = v$, we have $V = U \oplus W$, showing that W is a G-stable complement to U in V. □

Remark 18.0.22. Maschke's Theorem fails if the characteristic of the ground field divides $|G|$, as in Example 18.0.15 (noting that the choice for W is $\langle v_2' \rangle$ where $v_2' = (a, b)$ for $b \neq 0$, which is never stable by ρ).

Definition 18.0.23. *Let $\rho : G \to \mathrm{GL}(V)$ be a representation. ρ is* ***completely reducible*** *if $V = \{0\}$, or there exist G-stable subspaces $U_1, \dots, U_m$ of V such that*

$$V = U_1 \oplus \cdots \oplus U_m$$

and the subrepresentation of G afforded by each U_i is irreducible.

Corollary 18.0.24. *Let G be a finite group and suppose that $\mathrm{char}(k) \nmid |G|$. Then every finite dimensional representation $\rho : G \to \mathrm{GL}(V)$ of G is completely reducible.*

Proof. We proceed by induction on $\dim V$, where the case $\dim V = 0$ is true by definition. Let U_1 be a G-stable non-zero subspace of V of smallest possible dimension (which exists, as V is one such space). By construction, U_1 is irreducible. Then U_1 admits a G-stable complement W by Maschke's Theorem. Now $\dim W < \dim V$, so by induction $W = U_2 \oplus \cdots \oplus U_m$ for some G-stable irreducible subspaces $U_2, \dots, U_m$.. Hence $V = U_1 \oplus U_2 \oplus \cdots \oplus U_m$ is also completely reducible. □

19 Decomposing Representations

Definition 19.0.1. *Let G be a finite group. The* ***group ring*** *of G (with coefficients in k) is the vector space kG with multiplication defined as*

$$\left(\sum_{x\in G} a_x x\right) \cdot \left(\sum_{y\in G} b_y y\right) = \sum_{g\in G}\left(\sum_{x\in G} a_x b_{x^{-1}g}\right) g$$

The identity element is the formal sum with identity coefficient on the identity of G.

Remark 19.0.2. The group G embeds into the group ring via the map $g \mapsto g$. This embedding respects multiplication, thus realises G as a subgroup of the group of units $kG^\times$ in the ring kG.

Example 19.0.3. Let $G = \langle x\rangle$ be a cyclic group of order n. Then kG has $G = \{1, x, \dots, x^{n-1}\}$ as a basis, so it is generated by k and x as a ring, and k commutes with x. Define a ring homomorphism $\psi : k[T] \to kG$ by $\psi(f(T)) = f(x)$ for each $f(T) \in k[T]$. Then ψ is surjective and $\ker\psi = \langle T^n - 1\rangle$. So, by the first isomorphism theorem for rings, we get

$$kG \cong k[T]/\langle T^n - 1\rangle$$

If k contains a primitive n-th root of unity ζ (such that T^n-1 splits), then it factors into a product of distinct linear factors $(T-1)(T-\zeta)\cdots(T-\zeta^{n-1})$. By the Chinese Remainder Theorem, this implies

$$kG \cong k[T]/\langle T^n - 1\rangle \cong \underbrace{k \times k \times \cdots \times k}_{n \text{ times}}$$

Proposition 19.0.4. *Let V be a vector space and G be a group.*

1. *Suppose that $\rho : G \to \mathrm{GL}(V)$ is a representation. Then V becomes a left kG-module via the action*

$$\left(\sum_{x\in G} a_x x\right) \cdot v = \sum_{x\in G} a_x \rho(x)(v)$$

for all $a_x \in k$, $v \in V$

2. *Suppose that V is a left kG-module. Then $\rho : G \to \mathrm{GL}(V)$ defined by*

$$\rho(g)(v) := g \cdot v$$

for all $g \in G$, $v \in V$ is a representation.

3. *This gives a bijection between the set of representations $\rho : G \to \mathrm{GL}(V)$ and the set of kG-module structures $kG \times V \to V$ on V.*

Remark 19.0.5. This correspondence of G-representations to kG-modules moves general theorems about modules into representations, including isomorphism theorems and correspondences.

Example 19.0.6. Let A be a ring. The **free A-module of rank 1** is the abelian group A equipped with the left-multiplication action of A by

$$a \cdot b = ab$$

for all $a, b \in A$. A-submodules of this A-module are called **left-ideals**.

Definition 19.0.7. *If $A = kG$, the representation $\rho : G \to \mathrm{GL}(kG)$ corresponding to the free kG-module of rank 1 is called the* ***left regular representation****.*

Remark 19.0.8. The left-regular representation coincides with the permutation representation of G on kG, where we extend from the natural action of G on G by left multiplication to kG.

Definition 19.0.9. *An A-module M is* ***irreducible*** *or* ***simple*** *if M is nonzero, and if N is an A-submodule of M, $N = \{0\}$ or $N = M$.*

An A-module V is ***completely reducible*** *if it is either the 0-module, or is equal to a direct sum of finitely many irreducible submodules.*

A homomorphism of representations is simply a map of kG-modules, known as a kG-linear map.

Definition 19.0.10. *Let A be a ring. We say that A is* ***semisimple*** *if the free A-module of rank 1 is completely reducible.*

Proposition 19.0.11. *Let G be a finite group such that $|G| \neq 0$ in k. Then the group ring kG is semisimple.*

Proof. Follows from correspondence and Maschke's Theorem. □

Definition 19.0.12. *Let V be an A-module. We say that V is* ***cyclic*** *if it can be generated by a single element $v : V = A \cdot v$. The* ***annihilator*** *of $v \in V$ is the left-ideal*

$$\mathrm{Ann}_A(v) := \{a \in A \mid av = 0\}$$

Example 19.0.13. Simple modules are cyclic. This is because any span of a single element produces a submodule which must be the entire thing.

Lemma 19.0.14. *Every cyclic A-module V is isomorphic to a quotient module of the free module of rank 1. If $V = A \cdot v$, then*

$$V \cong A/\mathrm{Ann}_A(v)$$

Proof. The map $\psi : A \to V$ given by $a \mapsto a \cdot v$ is an A-module homomorphism. This is surjective, so by the first isomorphism theorem, we have

$$V = \mathrm{Im}\ \psi \cong A/\ker\psi$$

Now this follows as $\ker\psi = \mathrm{Ann}_A(v)$. □

Lemma 19.0.15. *Let V, W be simple A-modules. Then every non-zero A-linear map $\psi : V \to W$ is an isomorphism.*

Proof. We know $\ker\psi$ is an A-submodule of V and that $\mathrm{Im}\ \psi$ is an A-submodule of W. As ψ is non-zero $\ker\psi$ is also not all of V and $\mathrm{Im}\ \psi$ is nonzero. As V and W are both simple, it must be the case that $\ker\psi = 0$ and $\mathrm{Im}\ \psi = W$. Hence ψ is bijective, and therefore is an isomorphism. □

Proposition 19.0.16. *Let A be a semisimple ring. Then A has only finitely many simple A-modules up to isomorphism.*

Proof. Write $A = V_1 \oplus \cdots \oplus V_r$ for some simple A-submodules V_i of A. Let V be a simple A-module, pick a nonzero vector $v \in V$ and consider the A-module map $\psi : A \to V$ by $a \mapsto a \cdot v$. Let $\psi_i : V_i \to V$ be the restriction of ψ to V_i such that if $a = a_1 + \cdots + a_r$ is the decomposition of $a \in A$ with $a_i \in V_i$ for each i, then

$$\psi(a) = \psi_1(a_1) + \cdots + \psi_r(a_r)$$

If ψ_i is the zero-map for all i, then ψ is the zero map. Hence ψ_i is nonzero for some i. In particular, V is isomorphic to one of the irreducible representations in the list $V_1, \ldots, V_r$. □

Theorem 19.0.17. *Let G be a finite group such that $|G| \neq 0$ in k. Then G has only finitely many irreducible representations up to isomorphism.*

Proof. The ring kG is semisimple by Maschke's Theorem. By Proposition 19.0.16 and correspondence, the proof follows. □

Definition 19.0.18. *For a finite group G, we write $r_k(G)$ to denote the number of isomorphism classes of irreducible k-representations of G.*

Theorem 19.0.19 (Schur's Lemma)**.** *Suppose that k is algebraically closed. Let V be a simple module over a finite dimensional k-algebra A. Then every A-submodule endomorphism of V is given by the action of some scalar $\lambda \in k$ such that*

$$\mathrm{End}_A(V) = k1_V$$

Proof. By Lemma 19.0.14, V is isomorphic to a quotient module of A, so V is itself finite dimensional as a k-vector space. Let $\psi : V \to V$ be an A-module endomorphism. Then it is a k-linear map, so has at least one eigenvalue $\lambda \in k$ (because the characteristic polynomial splits). Hence $\psi - \lambda 1_V : V \to V$ is a homomorphism with nonzero kernel, and as V is simple, is the zero map. Thus $\psi = \lambda 1_V$ is the action of $\lambda \in k$. □

Definition 19.0.20. *Let A be a k-algebra and V be an A-module with $\mathrm{End}_A(V) = k1_V$. Then by Schur's Lemma, every $z \in Z(A)$ acts on V by a scalar, which is denoted by z_V. The ring homomorphism $Z(A) \to k$ via $z \mapsto z_V$ is called the **central character** of V.*

19.1 Artin-Weddernburn

For this subsection, we fix A to be some semisimple ring, and $V_1, \ldots, V_r$ will denote the complete list of representatives for the isomorphism classes of simple A-modules. We also fix a decomposition

$$A = \bigoplus_{i=1}^{r} \bigoplus_{j=1}^{n_i} L_{i,j}$$

of the A-module A into a direct sum of simple left ideals $L_{i,j}$ where $L_{i,j} \cong V_i$ for each i and j.

Note that we must have $n_1, \ldots, n_r \geq 1$, as each V_i occurs as a direct summand of A at least once. Also, the left-ideals are not unique in general.

Proposition 19.1.1. *Let A be a finite dimensional semisimple k-algebra and suppose that k is algebraically closed. Then $\dim Z(A) \leq r$.*

Proof. By Schur's Lemma, we have $\mathrm{End}_A(V_i) = k1_{V_i}$ for all i, so we can define a k-linear map $\psi : Z(A) \to k^r$ by $\psi(z) := (z_{V_1}, \ldots, z_{V_r})$.

Suppose now that $\psi(z) = 0$ for some $z \in Z(A)$, such that $z_{V_i} = 0$ for all i. We show $z = 0$.

By the decomposition of $1 \in A$ along the decomposition, we have

$$1 = \sum_{i=1}^{r} \sum_{j=1}^{n_i} e_{i,j}$$

for some $e_{i,j} \in L_{i,j}$.

Then we must have

$$z = z1 = \sum_{i=1}^{r} \sum_{j=1}^{n_i} ze_{i,j} = \sum_{i=1}^{r} \sum_{j=1}^{n_i} z_{V_i} e_{i,j}$$

As $z_{V_i} = 0$ for all i, $z = 0$. Hence ψ is injective and so it follows that $\dim Z(A) \leq \dim k^r = r$. □

Lemma 19.1.2. *Each $B_i := \bigoplus_{j=1}^{n_i} L_{i,j}$ is a two-sided ideal of A, and $A = B_1 \oplus \cdots \oplus B_r$.*

Proof. The second part of the statement follows from definition, and each B_i is a left ideal of A. Hence it suffices to show it is a right ideal in A. Fix $a \in A$ and consider $L_{i,j} \subseteq B_i$. Let $i' \neq i$ and $1 \leq j' \leq n_{i'}$ be another pair of indices, and consider the projection $\psi \twoheadrightarrow L_{i',j'}$ along the decomposition.

The restriction of $\phi \circ r_a : A \to L_{i',j'}$ to $L_{i,j}$ by right multiplication is an A-module homomorphism from $L_{i,j}$ to $L_{i',j'}$. As $i' \neq i$, these modules are not isomorphic, so the restriction must be the zero map. Varying i' and j', the projection of $L_{i,j}$ onto each B_i' with $i' \neq i$ is zero. Hence $L_{i,j}a \subseteq B_i$. As B_i is equal to the sum of all $L_{i,j}$, we have $B_i a \subseteq B_i$ for all $a \in A$.

□

Lemma 19.1.3. *Let R be a k-algebra and suppose that $R = S_1 \oplus \cdots \oplus S_r$ for some non-zero two-sided ideals $S_1, \ldots, S_r$. Then $\dim Z(R) \geq r$.*

Proof. Write $1 = e_1 + \cdots + e_r$ for some $e_i \in S_i$. Let $a \in R$ and fix $i = 1, \ldots, r$. Since S_i is a left-ideal, $ae_i \in S_i$. As $a = ae_1 + \cdots + ae_r$, we see that ae_i is the component of a in S_i in the decomposition $R = S_1 \oplus \cdots \oplus S_r$. On the other hand, as S_i is a right ideal, $e_i a$ is the component of a in S_i by the same decomposition. Hence $ae_i = e_i a$ for all i and $a \in R$, thus e_i is central.

If $i \neq j$, then $e_i e_j \in S_i \cap S_j = \{0\}$, so $e_i e_j = 0$. Hence $e_i = e_i \cdot 1 = e_i \sum_{j=1}^{r} e_j = e_i^2$. In particular, the set $\{e_1, \ldots, e_r\}$ forms a set of pairwise orthogonal idempotents such that $e_i e_j = \delta_{i,j} e_i$.

Now suppose that $\sum_{i=1}^{r} \lambda_i e_i = 0$ for some $\lambda_i \in k$. Multiplying by e_j gives $\lambda_j e_j = 0$. If $e_j = 0$, then for all $a \in S_j$ we have $a = ae_j = 0$, contradicting the assumption that $S_j \neq \{0\}$. Thus $e_j \neq 0$ for all j, giving $\{e_1, \ldots, e_r\}$ to be a linearly independent set over k. Thus $r \leq \dim Z(R)$. □

Theorem 19.1.4. *Let A be a finite dimensional semisimple k-algebra and suppose that k is algebraically closed. Then $r = \dim Z(A)$.*

Proof. By Proposition 19.1.1, we have $r \geq \dim Z(A)$. By Lemma 19.1.2 $A = B_1 \oplus \cdots \oplus B_r$ for some two-sided ideals B_r, so by Lemma 19.1.3, $r \leq \dim Z(A)$, so the proof follows. □

Definition 19.1.5. *For a finite group G, let $s(G)$ denote the number of conjugacy classes of G. Now let $C_1, \ldots, C_s$ be the conjugacy classes of G. For each $i = 1, \ldots, s$, define the **conjugacy class sum** of C_i to be*

$$\widehat{C_i} := \sum_{x \in C_i} x \in kG$$

Proposition 19.1.6. *$\{\widehat{C_1}, \dots, \widehat{C_s}\}$ is a basis for $Z(kG)$ as a vector space, thus*

$$\dim Z(kG) = s(G)$$

Proof. Let C_a be the conjugacy class of $a \in G$. Fix a $x \in G$, and define $\phi_x : G \to G$ by $y \mapsto x^{-1}yx$. This is a bijective function closed under conjugacy classes, we have

$$\widehat{C_a} = \sum_{y \in C_a} y = \sum_{z \in C_a} \phi_x(z) = \sum_{z \in C_a} x^{-1}zx = x^{-1}\left(\sum_{z \in C_a} z\right) x = x^{-1}\widehat{C_a}x$$

In particular, $\widehat{C_a}$ commutes with any $x \in G$. Hence it commutes with any element in kG. Thus $\widehat{C} \in Z(kG)$ for any choice of conjugacy class.

Fix $z := \sum_{x \in G} a_x x \in Z(kG)$. We have

$$\sum_{x \in G} a_x x = z = g^{-1}zg = g^{-1}\left(\sum_{x \in G} a_x x\right) g = \sum_{x \in G} a_x(g^{-1}xg)$$

In particular, coefficients agree within any conjugacy class. Write λ_i for the coefficient in the conjugacy class C_i. Then, particular, we can write

$$z = \sum_{i=1}^{s} \sum_{x \in C_i} a_x x = \sum_{i=1}^{s} \lambda_i \sum_{x \in C_i} x = \sum_{i=1}^{s} \lambda_i \widehat{C_i}$$

Thus $Z(kG)$ is spanned by the sums of conjugacy classes.

If $0 = \sum_{i=1}^{s} \lambda_i \widehat{C_i} = \sum_{i=1}^{s} \sum_{x \in C_i} \lambda_i x$. As G is a linearly independent set in kG, we have $\lambda_i = 0$ for all i. Thus the conjugacy classes are linearly independent. □

Corollary 19.1.7. *Let G be a finite group and k be an algebraicaly closed field with $|G| \neq 0$ in k. Then $r_k(G) = s(G)$.*

Proof. By Maschke, kG is a semisimple k-algebra with $\dim Z(kG) = s(G)$ by Proposition 19.1.6. The proof follows from Theorem 19.1.4. □

Corollary 19.1.8. *Suppose that $|G| \neq 0$ in k and take $e := \frac{1}{|G|}\sum_{g \in G} g \in kG$. Then e is a central idempotent.*

Proof. e is a kG-linear combination of all conjugacy class sums, so $e \in Z(kG)$ by Proposition 19.1.6. Now,

$$e^2 = \frac{1}{|G|}\sum_{g \in G}\left(\frac{1}{|G|}\sum_{h \in H} gh\right) = \frac{1}{|G|}\sum_{g \in G}\left(\frac{1}{|G|}\sum_{h \in G} h\right) = \frac{1}{|G|}\sum_{g \in G} e = e$$

□

Lemma 19.1.9. *We note the following properties about the ring decomposition:*

1. *Each B_i is a ring with identity element e_i*
2. *A is isomorphic to the product of rings (B_i, e_i)*

$$A \cong B_1 \times \cdots \times B_r$$

3. *Each B_i is a semisimple ring with unique simple module V_i*

Proof. (i) Lemma 19.1.2 shows that B_i is an additive subgroup of A stable under multiplication. In the proof of Lemma 19.1.3 we saw that for any $a \in A$, $ae_i = e_i a$ is the B_i component of a along the decomposition $A = B_1 \oplus \cdots \oplus B_r$. In particular, $ae_i = e_i a = a$ for all $a \in B_i$

(ii) The isomorphism sends $a \in A$ to $(ae_1, \ldots, ae_r) \in B_1 \times \cdots \times B_r$.

(iii) Fix $\ell = 1, \ldots, n_i$ and suppose that U is a B_i-submodule of $L_{i,\ell}$. Then,

$$A \cdot U = \left(\bigoplus_{j=1}^{r} B_j \right) \cdot U \leq U$$

where the last equality follows from the fact $B_j \cdot U \leq B_j \cdot B_i = B_j e_j \cdot e_i B_i = 0$ if $j \neq i$, and $B_i \cdot U \leq U$ as U is a B_i-submodule. In particular, U is an A-submodule of $L_{i,\ell}$, thus U is either zero of all of $L_{i,\ell}$ as it is a simple A-module. Thus $L_{i,\ell}$ hence V_i are all simple B_i-moduoes. As $B_i = \bigoplus_{j=1}^{n_i} L_{i,j}$, it is a semisimple ring. In particular, by Proposition 19.0.16, V_i is the only simple B_i-module up to isomorphism. □

Remark 19.1.10. Note that B_i is an additive subgroup of A stable under multiplication, but it is not a unital subring when $r \geq 2$, as the identity element e_i is not the identity element 1 in A.

Definition 19.1.11. *Let A be a ring. The* ***opposite ring*** *to A, written A^{op} has the same abelian group as A, but multiplication defined as*

$$a \star b = ba$$

for all $a, b \in A^{\mathrm{op}}$

Proposition 19.1.12. *For each $a \in A$, write $r_a : A \to A$ to be the left A-linear map given by $r_a(b) = ba$ for each $b \in A$. The map*

$$r : A^{\mathrm{op}} \to \mathrm{End}_A(A) \qquad a \mapsto r_a$$

is an isomorphism of rings.

Proof. We note that r is a ring homomorphism, taking the structure from A.

For $a \in A$, if $r_a = 0$, then we have $a = 1_A a = r_a(1_A) = 0(1_A) = 0$, so the kernel of r is trivial. Take any $\psi \in \mathrm{End}_A(A)$. For every $b \in A$, we have by A-linearity of ψ,

$$\psi(b) = \psi(b1) = b\psi(1) = r_{\psi(1)}(b)$$

In particular $\psi = r_{\psi(1)}$. So we have an isomorphism of rings. □

Proposition 19.1.13. *Let V be an A-module. Suppose $D := \mathrm{End}_A(V)$ and let $n \geq 1$.*

1. *The inclusion maps and projection maps to each coordinate give a ring homomorphism $M_n(D) \cong \mathrm{End}_A(V^n)$*

2. *For any ring S, $M_n(S)^{\mathrm{op}} \cong M_n(S^{\mathrm{op}})$.*

Proof. (i) Let $\sigma_j : V \to V^n$ be the inclusion maps and $\pi_j : V^n \to V$ be the projection maps. Define $\alpha : M_n(D) \to \operatorname{End}_A(V^n)$ by

$$(\phi_{i,j}) \mapsto \sum_{i=1}^{n}\sum_{j=1}^{n} \sigma_i \circ \phi_{i,j} \circ \pi_j$$

and $\beta : \operatorname{End}_A(V^n) \to M_n(D)$ by

$$\phi \mapsto (\pi_i \circ \psi \circ \sigma_j)$$

Now,

$$(\beta \circ \alpha)(\phi_{i,j}) = \beta\left(\sum_i \sum_j \sigma_i \circ \phi_{i,j}\pi_j\right)$$

And the i', j'-th coordinate of the evaluation is

$$\pi_{i'} \circ \left(\sum_i \sum_j \sigma_i \circ \phi_{i,j}\pi_j\right)\sigma_{j'} = \sum_i \sum_j (\pi_{i'} \circ \sigma_i) \circ \phi_{i,j} \circ (\pi_j \circ \sigma_{j'}) = \phi_{i',j'}$$

Noting that $\pi_i \circ \sigma_j = \delta_{i,j}$, thus α is injective.

Also,

$$(\alpha \circ \beta)(\phi) = \alpha((\pi_1 \circ \phi \circ \sigma_j)) = \sum_i \sum_j \sigma_i \circ (\pi_i \circ \phi \circ \sigma_j) \circ \pi_j = \left(\sum_i \sigma_i \circ \pi_i\right) \circ \phi \circ \left(\sum_j \sigma_j \circ \pi_j\right) = \psi$$

Noting that $\sum_k \sigma_k \circ \pi_k = 1_{\operatorname{End}_A(V^n)}$. Finally, this is a unital ring homomorphism, induced by the linear structure of matrix multiplication and projection / inclusions.

(ii) This follows from the fact there is a natural isomorphism by transposing. □

Proposition 19.1.14. *Let B be a semisimple ring with exactly one simple module V up to isomorphism. Suppose that $B \cong \underbrace{V \oplus \cdots \oplus V}_{n \text{ times}}$ as a left B-module, and let $D := \operatorname{End}_B(V)$. Then there is a ring isomorphism*

$$B \cong M_n(D^{\mathrm{op}})$$

Proof. We know from Proposition 19.1.12 that $B \cong \operatorname{End}_B(B)^{\mathrm{op}}$. Since $B = V^n$ as a left B-module, we have $\operatorname{End}_B(B) \cong M_n(D)$. Hence

$$B \cong \operatorname{End}_B(B)^{\mathrm{op}} \cong M_n(D)^{\mathrm{op}} \cong M_n(D^{\mathrm{op}})$$

Noting Proposition 19.1.13. □

Theorem 19.1.15 (Artin-Weddernburn)**.** *Suppose that k is an algebraically closed field and that A is a finite dimensional semisimple k-algebra. Then there exist positive integers $n_1, \ldots, n_r$ and a k-algebra isomorphism*

$$A \cong M_{n_1}(k) \times \cdots \times M_{n_r}(k)$$

Proof. By Lemma 19.1.9, without loss of generality, we may assume that $r = 1$, such that A has exactly one simple module V up to isomorphism. Then $A \cong M_n(D^{\mathrm{op}})$ where $D := \operatorname{End}_A(V)$ by Lemma 19.1.14. On the other hand, $D \cong k$ by Schur's Lemma. □

Proposition 19.1.16. *Suppose that $A = M_n(k)$ be the ring of $n \times n$ matrices with entires in k and let $V := k^n$ be the natural left A-module of $n \times 1$ column vectors. Then,*

1. *V is a simple A-module*
2. *A has no nonzero proper two sided ideals*
3. *$A = L_1 \oplus \cdots \oplus L_n$, where $L_j := M_n(k) \cdot E_{i,i}$ is a decomposition into simple left ideals.*

Proof. (i) First note that V is nonzero. Let W be an A-submodule of V and assume that $W \neq \{0\}$. Taking a nonzero $w \in W$, extend this to a basis for V. Consider the matrix that sends w to e_i a standard basis vector, and all other basis vectors to 0. Then we have $T(v) = e_i \in W$, so this forces $W = V$.

(ii) Pick any two-sided nonzero ideal $I \subseteq M_n(k)$. As I is nonzero, choose $A = (a_{i,j}) \in I$ that is nonzero. Let $a_{i,j} \neq 0$. Then,

$$E_{ri} A E_{js} = a_{ij} E_{rs} \in I$$

as I is two sided. Scaling, $E_{rs} \in I$. Hence every elementary matrix E_{rs} belongs in I, forcing $I = M_n(k)$.

(iii) Note first that the set $E_{i,i}$ over i is a pairwise orthogonal idempotent. The span of $E_{i,i}$ by left-multiplication gives elements of the form $E_{j,i}$. In particular, as $1 = \sum_i E_{i,i}$,

$$A = A \cdot 1 = A \sum_i E_{i,i} = \sum_i (A E_{i,i}) \in \sum_i I_i$$

If $\sum_i A_i E_{i,i} = 0$, then right multiplication by $E_{j,j}$ forces $A_j E_{j,j} = 0$, hence direct. Finally, $I_i \simeq k^n$, so is simple. □

Remark 19.1.17. Note that the decomposition above need not be unique. We can pick $E'_{i,i} = P E_{i,i} P^{-1}$ for some invertible matrix P (not diagonal, to change the matrix), then this is again a complete set of primitive orthogonal idempotent with a new decomposition $M_n(k) = \bigoplus_i M_n(k) E'_{i,i}$.

The main point is that $M_n(k)$ is semisimple, and the decomposition is unique up to isomorphism. Hence, permuting or conjugating maintains isomorphism.

Corollary 19.1.18. *Suppose that k is algebraically closed. Let G be a finite group such that $|G| \neq 0$ in k and let $V_1, \ldots, V_r$ be a complete list of pairwise non-isomorphic simple kG-modules. Then we have*

1. *$kG \simeq V_1^{\dim V_1} \oplus \cdots \oplus V_r^{\dim V_r}$ as a kG-module*
2. *$|G| = \sum_{i=1}^r (\dim V_i)^2$*

Proof. We know that kG is a semisimple ring by Maschke's Theorem, so by Artin Weddernburn, we can decompose

$$kG \cong M_{n_1}(k) \times \cdots \times M_{n_r}(k)$$

The matrix algebra $M_n(k)$ acts on the space of column vectors k^n by left-multiplication, and this forces k^n to be a simple $M_n(k)$-module. On the other hand, $M_n(k)$ is isomorphic to a direct sum of n copies of k^n, so $n_i = \dim V_i$ for each $i = 1, \ldots, r$.

The second statement is then immediate from the first. □

Proposition 19.1.19. *Every representation $\rho : G \to \mathrm{GL}(V)$ extends to a k-algebra homomorphism $\tilde{\rho} : kG \to \mathrm{End}_k(V)$*

Proof. As $\mathrm{End}_k(V)$ is a k-vector space and G is a basis for kG, $\rho : G \to \mathrm{GL}(V) \subseteq \mathrm{End}_k(V)$ extends uniquely to a k-linear map $\tilde{\rho} : kG \to \mathrm{End}_k(V)$. Now this acts like a homomorphism for elements in G, so it follows that

$$\tilde{\rho}(xy) = \tilde{\rho}\left(\sum_{g\in G}\sum_{h\in H} a_g b_h gh\right) = \sum_{g\in G}\sum_{h\in H} a_g b_h \tilde{\rho}(gh) = \tilde{\rho}(g)\tilde{\rho}(h) = \left(\sum_{g\in G} a_g \tilde{\rho}(g)\right)\left(\sum_{h\in H} b_h \tilde{\rho}(h)\right)$$

Also, $\tilde{\rho}(1_{kG}) = \rho(1_G) = 1_{\mathrm{End}_k(V)}$. □

20 Constructing representations

Lemma 20.0.1. *Let V be a vector space and let $G \times V \to V$ be a G-action on the set V. This extends to a kG-module structure on V if and only if the G-action on V is linear, such that*

$$g \cdot (v + \lambda w) = (g \cdot v) + \lambda(g \cdot w)$$

for all $g \in G$, $v, w \in V$, $\lambda \in k$.

Definition 20.0.2. *Let V and W be G-repreesntations. The external direct sum $V \oplus W$ is a G-representation via*

$$g \cdot (v \cdot w) = (g \cdot v, g \cdot w)$$

for all $g \in G$, $v \in V$, $w \in W$.

Definition 20.0.3. *Let V be a G-representation. This induces a representation on the dual space V^* via*

$$(g \cdot f)(v) := f(g^{-1} \cdot v)$$

*for all $g \in G$, $f \in V^*$, $v \in V$. We call this the **dual representation**.*

Definition 20.0.4. *Let V, W be G-representations. The vector space $\mathrm{Hom}(V, W)$ of all linear maps from V to W admits a linear G-action by*

$$(g \cdot f)(v) = g \cdot f(g^{-1} \cdot v)$$

for all $g \in G$, $f \in \mathrm{Hom}(V, W)$, $v \in V$. When W is the trivial 1-dimensional representation, we recover the dual space $\mathrm{Hom}(V, k) = V^*$.

Lemma 20.0.5. *Let V be a finite dimensional G-representation. The biduality isomorphism between vector spaces by*

$$\tau : V \to (V^*)^* \qquad \tau(v)(f) := f(v)$$

for all $f \in V^*, v \in V$ is an isomorphism of G-representations.

Proof. Noting that the map is a bijection, it suffices to check that this is indeed a homomorphism by the induced dual representations. Now,

$$(g \cdot \tau(v))(\psi) = \tau(v)(g^{-1} \cdot \psi) = (g^{-1} \cdot \psi)v = \psi(g \cdot v) = (\tau(g \cdot v))(\psi)$$

□

20.0.1 Actions on Tensor

Definition 20.0.6. *Let V and W be finite dimensional kG-modules. Define a G-action on $V \otimes W$ by setting*

$$g \cdot (v \otimes w) := (g \cdot v) \otimes (g \cdot w)$$

for all $g \in G$, $v \in V$, $w \in W$. This is called the ***tensor product representation*** *$V \otimes W$.*

This gives a well-defined G-representation as it is a linear G-action on $V \otimes W$.

Lemma 20.0.7. *Let V and W be finite dimensional kG-modules. Then there is an isomorphism of kG-modules*

$$V^* \otimes W \cong \mathrm{Hom}(V, W)$$

Proof. For every $f \in V^*$ and $w \in W$, we have a linear map $b(f, w) : V \to W$ given by $b(f, w)(v) := f(v)w$. The resulting map $b : V^* \times W \to \mathrm{Hom}(V, W)$ is blinear, so by the Universal Property on Tensors, extends to a linear map

$$\alpha : V^* \otimes W \to \mathrm{Hom}(V, W)$$

given by $\alpha(f \otimes w)(v) := f(v)w$ for all $f \in V^*, w \in W, v \in V$. Let $\{v_1, \ldots, v_n\}$ be a basis for V and let $\{v_1^*, \ldots, v_n^*\}$ be the corresponding dual basis for V^*. We define a linear map $\beta : \mathrm{Hom}(V, W) \to V^* \otimes W$ by

$$f \mapsto \sum_{i=1}^{n} v_i^* \otimes f(v_i)$$

We first show that these maps are mutual inverses.

Let $f \in \mathrm{Hom}(V, W)$ and $v \in V$. Then,

$$(\alpha \circ \beta)(f)(v) = \alpha(\beta(f))(v) = \sum_{i=1}^{n} \alpha(v_i^* \otimes f(v_i))(v) = \sum_{i=1}^{n} v_i^*(v) f(v_i) = f\left(\sum_{i=1}^{n} v_i^*(v) v_i\right) = f(v)$$

In particular, $\alpha \circ \beta = 1_{\mathrm{Hom}(V,W)}$. Also, for any $v \in V$,

$$(\beta \circ \alpha)(v_i^* \otimes w_j) = \beta(\alpha(v_i^* \otimes w_j)) = \sum_{k=1}^{n} v_k^* \otimes \alpha(v_i^* \otimes w_j)(v_k) = \sum_{k=1}^{n} v_k^* \otimes v_i^*(v_k) w_j = v_i^* \otimes w_j$$

So $\beta \circ \alpha = 1_{V^* \otimes W}$ as each basis element is sent to the identity. Finally, to show that α is a homomorphism of kG-modules, as we know α is k-linear, it suffices to show G-equivariance. Taking any $g \in G, f \in V^*, w \in W$, we have

$$\begin{aligned}
\alpha(g \cdot (f \otimes w))(v) &= \alpha((g \cdot f) \otimes (g \cdot w))(v) \\
&= (g \cdot f)(v)(g \cdot w) \\
&= f(g^{-1} \cdot v)(g \cdot w) \\
&= g \cdot (f(g^{-1} \cdot v)w) \\
&= g \cdot \alpha(f \otimes w)(g^{-1} \cdot v) \\
&= (g \cdot \alpha(f \otimes w))(v)
\end{aligned}$$

where the last line is an equality based on the homomorphism action induced by kG module actions on V and W. □

Definition 20.0.8. *Suppose that* $\operatorname{char}(k) \neq 2$ *and let* V *be a finite dimensional vector space.*

- *For each* $v, w \in V$*, define*

$$vw := \frac{1}{2}(v \otimes w + w \otimes v) \in V \otimes V$$

Then, the ***symmetric square*** *of* V *is the subspace of* $V \otimes V$ *given by*

$$S^2V := \langle \{vw \mid v, w \in V\} \rangle$$

- *For each* $v, w \in V$*, define*

$$v \wedge w := \frac{1}{2}(v \otimes w - w \otimes v) \in V \otimes V$$

The ***alternating square*** *of* V *is the subspace of* $V \otimes V$ *defined by*

$$\bigwedge^2 V := \langle \{v \wedge w \mid v, w \in V\} \rangle$$

Note that $vw = wv$ in S^2V and that $v \wedge w = -w \wedge v$ in $\bigwedge^2 V$ for all $v, w \in V$.

Lemma 20.0.9. *Let* $\dim V = n$ *and suppose that* $\operatorname{char}(k) \neq 2$*. Then,*

1. $V \otimes V = S^2V \oplus \bigwedge^2 V$
2. $\dim S^2V = \frac{n(n+1)}{2}$ *and* $\dim \bigwedge^2 V = \frac{n(n-1)}{2}$
3. *If* V *is a* G*-representation, then so are* S^2V *and* $\bigwedge^2 V$ *via the actions*

$$g \cdot (vw) = (g \cdot v)(g \cdot w) g \cdot (v \wedge w) = (g \cdot v) \wedge (g \cdot w)$$

for all $g \in G, v, w \in V$.

Proof. (i) Let $S_2 := \langle \sigma \rangle$ be the cyclic group of order 2. Since $\operatorname{char}(k) \neq 2$, the group ring kS_2 admits orthogonal idempotents $e_1 := \frac{1+\sigma}{2} \in kS_2$ and $e_2 := \frac{1-\sigma}{2} \in kS_2$, which gives rise to the decomposition

$$kS_2 = kS_2e_1 \oplus kS_2e_2 = ke_1 \oplus ke_2$$

by Lemma 19.1.2, where the last equality then follows from the fact $\sigma e_1 = e_1$ and $\sigma e_2 = -e_2$. Thus, every kS_2-module M admits an even-odd decomposition

$$M = e_1M \oplus e_2M = \{m \in M \mid \sigma m = m\} \oplus \{m \in M \mid \sigma m = -m\}$$

Now, S_2 acts linearly on $V \otimes V$ by

$$\sigma \cdot (v \otimes w) = w \otimes v$$

Then $S^2V = e_1 \cdot (V \otimes V)$ is the even part of $V \otimes V$ and $\bigwedge^2 V = e_2 \cdot (V \otimes V)$ is the odd part of $V \otimes V$. Then the even-odd decomposition gives $V \otimes V = S^2V \oplus \bigwedge^2 V$.

(ii) If $\{v_1, \dots, v_n\}$ is a basis for V, then $\{v_i \otimes v_j \mid 1 \leq i, j \leq n\}$ spans $V \otimes V$, so $\{e_1 \cdot (v_i \otimes v_j)\}$ spans S^2V. Now, $e_1 \cdot (v_i \otimes v_j) = v_iv_j = v_jv_i$, so $\{v_iv_j\}$ span S^2V. Hence,

$$\dim S^2V \leq \frac{n(n+1)}{2}$$

Similarly, $e_2 \cdot (v_i \otimes v_j) = v_i \wedge v_j$ spans $\bigwedge^2 V$, and therefore

$$\dim \bigwedge^2 V \leq \frac{n(n-1)}{2}$$

On the other hand, $\dim V \otimes V = n^2$, so decomposition implies the result.

(*iii*) We have two groups G and S_2 acting on $V \otimes V$. Now,

$$\sigma \cdot (g \cdot (v \otimes w)) = \sigma(g \cdot v \otimes g \cdot w) = g \cdot w \otimes g \cdot v = g \cdot (w \otimes v) = g \cdot (\sigma \cdot (v \otimes w))$$

for any $v, w \in V$ and $g \in G$. Hence, these actions commute pointwise, and so the actions preserve $S^2 V$ and $\bigwedge^2 V$. Hence these submodules inherit a linear G-action from $V \otimes V$ as claimed. □

Remark 20.0.10. This idea extends to finding proper kG-submodules to the tensor $V^{\otimes n}$ as a direct sum of kG-submodules $S^\lambda(V)$, one for each irreducible representation λ of the symmetric group S_n. This construction $V \mapsto S^\lambda(V)$ is called the **Schur Functor**.

Corollary 20.0.11. *Suppose* $\operatorname{char}(k) \neq 2$ *and V be a G-representation. The square tensor $V \otimes V$ is reducible when* $\dim V \geq 2$.

Proof. By Lemma 20.0.9, $V \otimes V$ decomposes as $S^2 V \oplus \bigwedge^2 V$, and these are both nontrivial by part (*ii*) of the Lemma. $S^2 V$ and $\bigwedge^2 V$ are both G-representations by (*iii*). □

Lemma 20.0.12. *Let V be a finite dimensional kG-module. Let W be a one-dimensional kG-module. Then, $V \otimes W$ is simple if and only if V is simple.*

Proof. First note that $W \otimes W^* \cong k$, as

$$g \cdot (w \otimes w^*) = (g \cdot w) \otimes (g \cdot w^*) = \chi(g) w \otimes \chi(g)^{-1} w^* = 1 \cdot (w \otimes w^*)$$

Hence the group elements act trivially, and so in particular $W \otimes W^* \cong k$.

Hence it suffices to show one direction, as then we can use the congruence $V \cong V \otimes (W \otimes W^*)$.

Suppose that $V \otimes W$ is simple. Suppose for a contradiction that V is not simple. Then we have a nonzero proper kG-module U of V. Let $\mathcal{B}_U = \{u_1, \ldots, u_k\}$ be a basis for U and extend it to a basis $\mathcal{B}_V$ of V. Let $\{w\}$ be a basis for the one dimensional space W. Then,

$$g \cdot (u \otimes w) = \underbrace{g \cdot u}_{\in U} \otimes \underbrace{g \cdot w}_{\in U} \in U \otimes W$$

Hence $U \otimes W$ is a proper G-stable subspace of $V \otimes W$, hence a kG module, a contradiction. Thus V is simple. □

Proposition 20.0.13. *Let V be a finite dimensional kG-module. Then, V is simple if and only if V^* is simple.*

Proof. Note that it suffices to show $\Rightarrow$, as $V^{**} \cong V$. Suppose that V is simple. Take $U \subseteq V^*$ be a nonzero kG-module. Tqking the annihilator of U, this is a G-stable subspace of V. As V is simple, noting $\operatorname{Ann}(U) = V$, we have $U = 0$ or $\operatorname{Ann}(U) = 0$. The first case is ruled out by the fact $U \neq 0$, so $\operatorname{Ann}(U) = 0$.

Now, the proof follows from the fact

$$U \cong \operatorname{Hom}_k(V/\operatorname{Ann}(U), k) \cong \operatorname{Hom}_k(V, k) \cong V^*$$

□

21 Character Theory

21.1 Definitions and Basic Properties

Definition 21.1.1. *Let $\rho : G \to \mathrm{GL}(V)$ be a complex representation of G. The* ***character*** *of ρ is the function*

$$\chi_\rho : G \to \mathbb{C} \qquad g \mapsto \mathrm{tr}(\rho(g))$$

The ***degree*** *of a character χ_ρ is the degree of the representation ρ.*

We write χ_V to denote the character of the representation afforded by a $\mathbb{C}G$-module V, when the $\mathbb{C}G$-module structure on V is understood.

Remark 21.1.2. Note that the character χ_V only depends on the isomorphism class of the $\mathbb{C}G$-module V, and the isomorphism class of the representation ρ. TODO!! more?

Definition 21.1.3. *A function $f : G \to \mathbb{C}$ is said to be a* ***class function*** *if it is constant on the conjugacy classes of G. That is,*

$$f(xgx^{-1}) = f(g)$$

for all $g, x \in G$. We denote the space of all class functions on G by $\mathcal{C}(G)$.

Note that $\mathcal{C}(G)$ is a commutative ring via pointwise multiplication of functions.

Lemma 21.1.4. *The character χ_V of any finite dimensional kG-module V is a class function.*

Proof. If $\rho : G \to \mathrm{GL}(V)$ is the corresponding representation, then the linear endomorphism $\rho(g)$ of V is conjugate to $\rho(xgx^{-1})$ in $\mathrm{GL}(V)$. But the conjugate linear maps have the same trace, as

$$\mathrm{tr}(ABA^{-1}) = \mathrm{tr}((AB)A^{-1}) = \mathrm{tr}(A^{-1}(AB)) = \mathrm{tr}(B)$$

for any $A, B \in \mathrm{GL}(V)$. □

Proposition 21.1.5. *Let G be a finite group and let V, W be finite dimensional $\mathbb{C}G$-modules. Then we have the following equalities in $\mathcal{C}(G)$:*

1. $\chi_{V^*} = \overline{\chi_V}$
2. $\chi_{V \oplus W} = \chi_V + \chi_W$
3. $\chi_{V \otimes W} = \chi_V \chi_W$
4. $\chi_{\mathrm{Hom}(V,W)} = \overline{\chi_V}\chi_W$
5. $\chi_{S^2 V}(g) = \frac{1}{2}(\chi_V(g)^2 + \chi_V(g^2))$ *for all $g \in G$*
6. $\chi_{\bigwedge^2 V}(g) = \frac{1}{2}(\chi_V(g)^2 - \chi_V(g^2))$ *for all $g \in G$.*

Proof. Fix $g \in G$. The action $g_V \in \mathrm{GL}(V)$ of g on V is diagonalizable. Fix a basis of g_V-eigenvectors $\{v_1, \ldots, v_n\}$ for V with corresponding eigenvalues $\lambda_1, \ldots, \lambda_n$, and fix a basis of g_W-eigenvectors $\{w_1, \ldots, w_m\}$ for W with eigenvalues $\mu_1, \ldots, \mu_m$. Then,

$$\chi_V(g) = \mathrm{tr}(g_V) = \sum_{i=1}^n \lambda_i \qquad \chi_W(g) = \mathrm{tr}(g_W) = \sum_{j=1}^m \mu_j$$

(i) Let $\{v_1^*, \dots, v_n^*\}$ be the dual basis for V^* relative to $\{v_1, \dots, v_n\}$. Then,

$$(g \cdot v_i^*)(v_j) = v_i^*(g^{-1} \cdot v_j) = v_i^*(\lambda_j^{-1} v_j) = \lambda_j^{-1} \delta_{ij} = (\lambda_i^{-1} v_i^*)(v_j)$$

where the last line equality follows from the fact tht given equation is 0 unless $i = j$. Hence,

$$g \cdot v_i^* = \lambda_i^{-1} v_i^*$$

for all $i = 1, \dots, n$. On the other hand, as λ_i is a root of unity, we have $g \cdot v_i^* = \overline{\lambda_i} v_i^*$, thus

$$\chi_{V^*}(g) = \operatorname{tr}(g_{V^*}) = \sum_{i=1}^{n} \overline{\lambda_i} = \overline{\operatorname{tr}(g_V)} = \overline{\chi_V(g)}$$

(ii) The action is defined by

$$g_{V \oplus W} = \begin{pmatrix} g_V & 0 \\ 0 & g_W \end{pmatrix}$$

so the trace is exactly the sum of traces.

(iii) By definition, the elementary tensors form a basis for $V \otimes W$. We note

$$g \cdot (v_i \otimes w_j) = (g \cdot v_i) \otimes (g \cdot w_j) = (\lambda_i v_i) \otimes (\mu_j w_j) = \lambda_i \mu_j (v_i \otimes w_j)$$

In particular, the elementary tensors form a basis of eigenvectors for the g-action on $V \otimes W$ with eigenvalue $\lambda_i \mu_j$. Hence,

$$\chi_{V \otimes W}(g) = \sum_{i=1}^{n} \sum_{j=1}^{m} \lambda_i \mu_j = \left(\sum_{i=1}^{n} \lambda_i \right) \left(\sum_{j=1}^{m} \mu_j \right) = \chi_V(g) \chi_W(g)$$

(iv) We note the isomorphism $V^* \otimes W \cong \operatorname{Hom}(V, W)$, hence

$$\chi_{\operatorname{Hom}(V,W)} = \chi_{V^* \otimes W} = \chi_{V^*} \chi_W = \overline{\chi_V} \chi_W$$

(v) Noting that $v_i v_j$ is a basis for $S^2 V$, we compute

$$g \cdot (v_i v_j) = (g \cdot v_i)(g \cdot v_j) = (\lambda_i v_i)(\lambda_j v_j) = \frac{1}{2}(\lambda_i v_i \otimes \lambda_j v_j + \lambda_j v_j \otimes \lambda_i v_i) = \lambda_i \lambda_j v_i v_j$$

In particular, the set $\{v_i v_j \mid 1 \leq i \leq j \leq n\}$ form an eigenbasis for $S^2 V$, thus

$$\chi_{S^2 V}(g) = \sum_{1 \leq i \leq j \leq n} \lambda_i \lambda_j = \sum_{1 \leq i < j \leq n} \lambda_i \lambda_j + \sum_i \lambda_i^2 = \frac{1}{2} \left(\sum_i \lambda_i \right)^2 + \frac{1}{2} \sum_i \lambda_i^2 = \frac{1}{2} \chi_V(g)^2 + \frac{1}{2} \chi_V(g^2)$$

(vi) By the same reasoning from (v), the set $\{v_i \wedge v_j \mid 1 \leq i < j \leq n\}$ form an eigenbasis for $\bigwedge^2 V$. Expanding,

$$\chi_{\bigwedge^2 V}(g) = \sum_{1 \leq i < j \leq n} \lambda_i \lambda_j = \frac{1}{2} \left(\sum_i \lambda_i \right)^2 - \frac{1}{2} \sum_i \lambda_i^2 = \chi_V(g)^2 - \chi_V(g^2)$$

□

Definition 21.1.6. *Let G be a finite group and let $\{g_1, \dots, g_s\}$ be a set of representatives for the conjugacy classes of G. Let $V_1, \dots, V_r$ be a complete list of representatives for the isomorphism classes of simple $\mathbb{C}G$-modules.*

*The **character table** of G is the $r \times s$ array with the (i,j)-th entry given by $\chi_{V_i}(g_j)$*

Remark 21.1.7. As $r = r_{\mathbb{C}}(G)$ and $s = s(G)$, the character table is always square. Also, $\chi(1) = \operatorname{tr}(\mathrm{Id}_V) = \dim V$.

Proposition 21.1.8. *Let $\rho : G \to \mathrm{GL}(V)$ be a finite dimensional representation. Then,*

- *$\chi_V(g) = \chi_V(1)$ if and only if $\rho(g) = 1$*
- *If $\dim V = 1$ then χ is a group homomorphism.*

Proof. $(i) \Rightarrow$ If $\chi_V(g) = \chi_V(1) = \dim V$, then we note by the finite order of G that $\rho(g)^m = \rho(g^m) = \rho(1) = I_V$ for some m. Hence $\rho(g)$ satisfies the polynomial $X^m - I = 0$, hence the eigenvalues of $\rho(g)$ satisfy $\lambda^m = 1$. In particular, $|\lambda| = 1$. As the trace is then the sum of these eigenvalues which equals $\dim V$, by the triangle inequality we must have $\lambda = 1$ for any eigenvalue. In particular, $\rho(g) = I_V$.

$\Leftarrow$ If $\rho(g) = 1$, then we have

$$\chi_V(g) = \operatorname{tr}(1) = \dim V = \chi_V(1)$$

(ii) If $\dim V = 1$, then $\chi(g) = \rho(g)$, so the proof follows immediately from the fact ρ is a group homomorphism. □

Lemma 21.1.9. *Suppose that k is algebraically closed.*

1. *Suppose further that G is abelian. Every smiple kG-module is one-dimensional.*
2. *The converse of the above holds provided that $|G| \neq 0$ in k.*

Proposition 21.1.10. *Let χ be a character of G. Then $\chi(g^{-1}) = \overline{\chi(g)}$ for all $g \in G$.*

Proposition 21.1.11. *Let $g \in G$. Then the following are equivalent:*

1. *g is conjugate to g^{-1}*
2. *for every character χ of G, we have $\chi(g) \in \mathbb{R}$.*

Definition 21.1.12. *Characters of degree 1 are called **linear characters**.*

Proposition 21.1.13. *Let $\chi_1, \dots, \chi_r$ be the complete list of characters of the irreducible complex representations of the finite group G. Then,*

$$\chi_1(1)^2 + \cdots + \chi_r(1)^2 = |G|$$

Proof. Suppose that the simple kG-module V_i affords the character χ_i. Then, $\chi_i(1) = \dim V_i$, thus the proof follows by Artin Weddernburn. □

Definition 21.1.14. *Let N be a normal subgroup of the finite group G and let $\rho : G/N \to \mathrm{GL}(V)$ be a representation. The **inflated representation** of G,*

$$\dot{\rho} : G \to \mathrm{GL}(V)$$

is defined by $\dot{\rho} := \rho(gN)$ for all $g \in G$.

Definition 21.1.15. *Let G be a finite group. The **derived subgroup** G' is the subgroup of G generated by all **commutators** $[x, y] := xyx^{-1}y^{-1}$ in G, such that*

$$G' := \langle xyx^{-1}y^{-1} \mid x, y \in G\rangle$$

Remark 21.1.16. The derived subgroup is a normal subgroup of G. The commutator also satisfies $[g, h]^{-1} = [g^{-1}, h^{-1}]$ and $\phi([g, h]) = [\phi(g), \phi(h)]$ where $\phi : G \to H$ is a group homomorphism.

Proposition 21.1.17. *Suppose that N is a normal subgroup of G, and suppose further that G/N is abelian. Then G' is a normal subgroup of N.*

Proof. If G/N is abelian, then we know that for any $x, y \in G$, we have $xyN = (xN) \cdot (yN) = (yN) \cdot (xN) = yxN$. In particular, $xyx^{-1}y^{-1} \in N$. Hence we have $G' \subseteq N$, and as G' is normal in G, it is normal in N. □

Proposition 21.1.18. *Every group homomorphism from G to an abelian group A is trivial on the commutator subgroup G' and hence factors through G/G'*

Proof. Let $\phi : G \to A$ be a group homomorphism where A is abelian. Then every commutator in A is equal to the identity, so every commutator $[g, h]$ of G lies in $\ker\phi$. In particular, $G' \leq \ker\phi$. Hence there is an induced map $\tilde{\phi} : G/G' \to A$ by sending $gG' \mapsto \phi(g)$, such that ϕ factors as $\tilde{\phi} \circ q_{G'}$ where $q_{G'}$ is the canonical quotient map. □

Proposition 21.1.19. *Suppose that G is abelian. Then every simple kG-module is one-dimensional. The converse holds provided that $|G| \neq 0$ in k.*

Proof. Let V be a simple kG-module. Then we can find a nonzero vector $v \in V$. As k and G are abelian, so is kG.

The action of every $z \in Z(kG) = kG$ on V lies in $\mathrm{End}_{kG}(V)$. As k is algebraically closed and V is simple, by Schur's Lemma, we have $\mathrm{End}_{kG}(V) = k1_V$. As $k \cdot v \subseteq V$ is closed under actions by scalars, it follows that $k \cdot v$ is a nonzero kG-submodule of V. As V is simple, we must have $V = k \cdot v$, which is one dimensional over k.

If $|G| \neq 0$ in k, by Maschke's Theorem, kG is semisimple, and there is a complete list $V_1, \ldots, V_r$ of representatives for the isomorphism classes of simple kG-modules. Hence by Artin Weddernburn, we have $kG \simeq M_{\dim V_1}(k) \times \cdots \times M_{\dim V_r(k)}$ as k-algebras. By assumption $\dim V_i = 1$ for all i, so we have $kG \simeq k^n$ as a commutative ring. In particular $G \leq kG^\times \simeq (k^n)^\times$ is abelian. □

Lemma 21.1.20. *Let G be a finite group. There is a bijective correspondence between complex linear characters of G and irreducible complex characters of G/G'. Hence G has precisely $|G : G'|$ distinct complex linear characters.*

Proof. Let χ be a complex linear character of G afforded by the complex representation $\rho : G \to \mathrm{GL}(V)$. Then $\mathrm{GL}(V) \cong \mathrm{GL}_1(\mathbb{C}) \cong \mathbb{C}^\times$, which is abelian, thus ρ induces a representation $\tilde{\rho} : G/G' \to \mathrm{GL}(V)$, such that $\tilde{\rho} \circ q_{G'} = \rho$. As $\dim V = 1$, we have $\tilde{\rho}$ is irreducible, and thus χ descends to an irreducible character $\tilde{\chi}$ of G/G' afforded by $\tilde{r}ho$ with $\tilde{\rho} \circ q_{G'} = \chi$.

On the other hand, suppose that ϕ is an irreducible complex character of G/G' afforded by the representation $\tau : G/G' \to \mathrm{GL}(V)$. As G/G' is abelian and $\mathbb{C}$ is algebraically closed, the simple $\mathbb{C}(G/G')$-module is 1-dimensional. Hence, the inflated representation $\dot{\tau} : G \to \mathrm{GL}(V)$ is also of degree 1, thus ϕ lifts to a linear character $\dot{\phi}$ of G afforded by $\cdot\tau$.

The bijection comes from the fact $\chi = \tilde{\chi} \circ \pi = \dot{\tilde{\chi}}$

As G/G' is abelian, $|G/G'| = |G : G'|$ is the number of conjugacy classes of G/G', which is the number of isomorphism classes of simple $\mathbb{C}(G/G')$-modules, which is the number of complex linear characters of G by correspondence.

□

Example 21.1.21. Let $G = A_4$ be the alternating group of order 12. We know that V_4 is a normal subgroup of order 4, written

$$V_4 := \{1, (12)(34), (14)(23), (13)(24)\}$$

Since A_4/V_4 has order 3, it must be a cyclic group of order 3, hence abelian. In particular, $A_4' \leq V_4$, forcing $|A_4'| \in \{1, 2, 4\}$. No subgroup of order 2 in V_4 is normal in A_4, and A_4' is nontrivial as it is not abelian, so it must be the case that $A_4' = V_4$. In particular, by Lemma 21.1.20, A_4 admits 3 distinct linear characters inflated from $A_4/V_4 \cong C_3$.

Definition 21.1.22. *Let G be a finite group. The **inner product on class functions***

$$\langle -, - \rangle : \mathcal{C}(G) \times \mathcal{C}(G) \to \mathbb{C}$$

is defined as

$$\langle \phi, \psi \rangle := \frac{1}{|G|} \sum_{g \in G} \overline{\phi(g)} \psi(g)$$

Remark 21.1.23. It is routine to verify that this is a complex inner product on $\mathcal{C}(G)$, satisfying our usual notions of sesquilinear, positive definite, and conjugate symmetry.

Proposition 21.1.24 (Fixed Point Formula)**.** *Let G be a finite group and let V be a finite dimensional $\mathbb{C}G$-module. Then*

$$\dim V^G = \frac{1}{|G|} \sum_{g \in G} \chi_V(g) = \langle \mathbb{1}, \chi_V \rangle$$

Proof. Let $e := \frac{1}{|G|} \sum_{g \in G} g \in \mathbb{C}G$ Then $ge = eg = e$ fora all $g \in G$, so we have $e^2 = e$. We call e to be the **principal idempotent of** $\mathbb{C}G$.

Now we have a decomposition

$$V = e \cdot V \oplus (1 - e) \cdot V$$

If $g \in G$, then $g \cdot (e \cdot v) = (ge) \cdot v = e \cdot v$ so $e \cdot V \leq V^G$. On the other hand, if $v \in V^G$, then $g \cdot v = v$ for all $g \in G$, so $|G| e \cdot v = \sum_{g \in G} g \cdot v = |G| v$, giving $v = e \cdot v$, hence $v \in e \cdot V$. In particular, $e \cdot V = V^G$.

The action of $e \in \mathbb{C}G$ on V is a linear map $e_V : V \to V$ which is an idempotent with image $e \cdot V$. So, writing $\rho : G \to \mathrm{GL}(V)$ for the representation afforded by V, we have

$$\dim V^G = \dim e \cdot V = \mathrm{tr}(e_V) = \frac{1}{|G|} \sum_{g \in G} \mathrm{tr} \rho(g) = \frac{1}{|G|} \sum_{g \in G} \chi_V(g)$$

□

Proposition 21.1.25. *Let V and W be finite dimensional $\mathbb{C}G$-modules. Then,*

1. $\mathrm{Hom}_{\mathbb{C}G}(V, W) = \mathrm{Hom}(V, W)^G$

2. $\langle \chi_V, \chi_W \rangle = \dim \mathrm{Hom}_{\mathbb{C}G}(V, W)$

Proof. (i) Let $f \in \mathrm{Hom}(V, W)$. Then f is fixed by the G-action if and only if

$$g \cdot f(g^{-1} \cdot v) = f(v)$$

for all $g \in G$ and $v \in V$. In particular, we rewrite that

$$g_W \circ f = f \circ g_V$$

for all $g \in G$. By definition, this is exactly the functions $finHom_{\mathbb{C}G}(V, W)$.

(ii) Noting the Fixed Point Formula, we have

$$\dim \mathrm{Hom}(V, W)^G = \frac{1}{|G|} \sum_{g \in G} \chi_{\mathrm{Hom}(V,W)}(g) = \frac{1}{|G|} \sum_{g \in G} \overline{\chi_V(g)} \chi_W(g) = \langle \chi_V, \chi_W \rangle$$

□

Theorem 21.1.26 (Row Orthogonality)**.** *Let ϕ and ψ be irreducible characters of the finite group G. Then,*

$$\langle \phi, \psi \rangle = \begin{cases} 1 & \text{if } \phi = \psi \\ 0 & \text{if } \phi \neq \psi \end{cases}$$

Proof. Let V and W be the simple $\mathbb{C}G$-modules whose characters are $\phi = \chi_V$ and $\psi = \chi_W$. As V and W are simple, if they are not isomorphic, the only map is the 0 map. If the two are isomorphic, by Schur's Lemma we have

$$\dim \mathrm{Hom}_{\mathbb{C}G}(V, W) = \dim \mathrm{End}_{\mathbb{C}G}(V) = 1$$

Hence,

$$\dim \mathrm{Hom}_{\mathbb{C}G}(V, W) = \begin{cases} 1 & \text{if } V \cong W \\ 0 & \text{if } V \ncong W \end{cases}$$

Hence by Proposition 21.1.25,

$$\langle \phi, \psi \rangle = \langle \chi_V, \chi_W \rangle = \dim_{\mathbb{C}G} \mathrm{Hom}(V, W) \in \{0, 1\}$$

Suppose that $\chi_V = \chi_W$. Then,

$$\langle \chi_V, \chi_W \rangle = ||\chi_V||^2 = \frac{1}{|G|} \sum_{g \in G} |\chi_V(g)|^2 \geq \frac{(\dim V)^2}{|G|} > 0$$

as $\chi_V(1) = \dim V$. Hence $\langle \chi_V, \chi_V \rangle = 1$. If $\chi_V \neq \chi_W$, then V cannot be isomorphic to W as isomorphic representations have the same characters, hence $\langle \phi, \psi \rangle = \dim \mathrm{Hom}_{\mathbb{C}G}(V, W) = 0$. □

Remark 21.1.27. Let V be a finite dimensional kG-module,$\chi_1, \ldots, \chi_r$ be the complete list of characters of the irreducible complex representations of G, and suppose that V_i is the simple kG-module with character χ_i. By Maschke's Theorem, we know that V is a direct sum of simple kG-modules. Since $V_1, \ldots, V_r$ are the only possible simple kG-modules up to isomorphism, we can find non-negative integers $a_1, \ldots, a_r$ such that

$$V \cong V_1^{a_1} \oplus \cdots \oplus V_r^{a_r}$$

We call a_i the **multiplicity** of V_i in V.

Corollary 21.1.28. *Let V and W be two finite dimensional kG-modules. Then V is isomorphic to W if and only if $\chi_V = \chi_W$.*

Proof. Decompose V into simple kG-modules, such that

$$V \cong V_1^{a_1} \oplus \cdots \oplus V_r^{a_r}$$

Passing to characters, we have

$$\chi_V = a_1\chi_1 + \cdots + a_r\chi_r$$

Thus by row orthogonality, we can recover a_i from χ_V by

$$\langle \chi_i, \chi_V \rangle = \langle \chi_i, \sum_{j=}^{r} a_j\chi_j \rangle = \sum_{j=1}^{r} a_j\delta_{ij} = a_i$$

If $\chi_V = \chi_W$, decomposing $W = V_1^{b_1} \oplus \cdots \oplus V_r^{b_r}$ as a kG-module, then for any i, $a_i = \langle \chi_i, \chi_V \rangle = \langle \chi_i, \chi_W \rangle = b_i$. Hence $V \cong W$. The converse is straightforward. □

Corollary 21.1.29. *The irreducible characters of G form an orthonormal basis for $\mathcal{C}(G)$.*

Proof. By row orthogonality, the characters are pairwise orthogonal elements in the inner product space $\mathcal{C}(G)$. On the other hand, $\dim \mathcal{C}(G) = s(G) = r_{\mathbb{C}} = r$, so $\{\chi_1, \ldots, \chi_r\}$ form a basis for $\mathcal{C}(G)$. □

Theorem 21.1.30 (Column Orthogonality)**.** *Let G be a finite group. Let $\chi_1, \ldots, \chi_r$ be the irreducible characters of G and let $g, h \in G$. Then,*

$$\sum_{i=1}^{r} \overline{\chi_i(g)}\chi_i(h) = \begin{cases} |C_G(g)| & \text{if } g \text{ is conjugate to } h \\ 0 & \text{otherwise} \end{cases}$$

Proof. Let $\{g_1, \ldots, g_r\}$ be a complete list of representatives for the conjugacy classes of G. Suppose that $g \in g_j^G$ and $h \in g_k^G$ for some j, k. As the characters χ_i are class functions, we will assume without loss of generality that $g = g_j$ and $h = g_k$.

Define

$$x_{i,j} = \chi_i(g_j) \cdot c_j \qquad \text{where } c_j := \sqrt{|g_j^G|/|G|}$$

Then we can compute,

$$\begin{aligned} \sum_{j=1}^{r} \overline{x_{i,j}} x_{k,j} &= \sum_{j=1}^{r} \overline{\chi_i(g_j)} c_j \chi_k(g_j) c_j \\ &= \sum_{j=1}^{r} \overline{\chi_i(g_j)} \chi_k(g_j) c_j^2 \\ &= \frac{1}{|G|} \sum_{j=1}^{r} |g_j^G| \overline{\chi_i(g_j)} \chi_k(g_j) \\ &= \frac{1}{|G|} \sum_{g \in G} \overline{\chi_i(x)} \chi_k(x) \\ &= \langle \chi_i, \chi_k \rangle = \delta_{i,k} \end{aligned}$$

Where the last line comes from row orthogonality. Hence the $r \times r$ matrix $X := (x_{i,j})$ is unitary:

$$\overline{X} \cdot X^T = I$$

So $\overline{X}$ is the left-inverse (and the right-inverse) of X^T in $\mathrm{GL}_r(\mathbb{C})$. Applying complex conjugation, we have

$$\overline{X}^T \cdot X = I$$

In particular,

$$(\overline{X}^T \cdot X)_{j,k} = \sum_{i=1}^{r} \overline{x_{i,j}} x_{i,k} = \sum_{i=1}^{r} \overline{\chi_i(g_j)} c_j \chi_i(g_k) c_k = \delta_{j,k}$$

Dividing both sides by $c_j c_k$ and taking $j = k$, we have $1/c_j^2 = |G|/|g_j^G| = |C_G(g_j)|$. □

21.2 Examples of Character Table Computation

When the explicit representations are known, computing the character tends to be straightforward.

Example 21.2.1. The character table for the cyclic group of order 3, $G = \{1, x, x^2\}$ is where $\omega :=$ $\exp(2\pi i/3)$ is a primitive cube root of unity. To see explicitly where these choices of representations came from, note that we have $\rho(g)^3 = \rho(g^3) = \rho(e) = 1$, so we must have $\rho(g)$ be sent to a primitive cube root of unity, and this determines all possible representations.

	1	x	x^2
$\mathbb{1}$	1	1	1
χ	1	ω	ω^2
χ^2	1	ω^2	ω

Example 21.2.2. Let $G = S_3$. Alongside the trivial character, we have a sign character $\epsilon : S_3 \to \{\pm 1\} \subseteq \mathbb{C}^\times$ by

$$\epsilon(\sigma) = \begin{cases} 1 & \text{if } \sigma \text{ is even} \\ -1 & \text{if } \sigma \text{ is odd} \end{cases}$$

We also have the two-dimensional irreducible representation W of S_3 from Example 18.0.18, we get the character table of S_3 as

	1	(123)	(12)
$\mathbb{1}$	1	1	1
ϵ	1	1	-1
χ_W	2	-1	0

We can use inflation to find character tables as well.

Example 21.2.3. Let $G = A_4$. Then $A_4' = V_4$, and G has 3 distinct linear characters. The representatives for the conjugacy classes in A_4 are 1, $g_2 := (12)(34)$, $g_3 := (123)$ and $g_4 := (132)$. Hence noting there are 4 conjugacy classes, our character table for A_4 looks as follows: where ω is a primitive third root of unity. As the sum of squares on the identity class is $|G| = 12$, we deduce that $d^2 = 3$. This equals $\dim V \in \mathbb{N}$, so we get $d = 3$.

g	1	g_2	g_3	g_4
$\lvert g^G\rvert$	1	3	4	4
$\lvert C_G(g)\rvert$	12	4	3	3
χ_1	1	1	1	1
χ_2	1	1	ω	ω^2
χ_3	1	1	ω^2	ω
χ_4	d	a	b	c

Now by row orthogonality, we get

$$\begin{aligned}
0 &= |G|\langle \chi_1, \chi_4\rangle = \sum_{g\in G} \overline{\chi_1(g)}\chi_4(g) = 1\cdot 1\cdot 3 + 3\cdot 1\cdot a + 4\cdot 1\cdot b + 4\cdot 1\cdot c = 3 + 3a + 4b + 4c \\
0 &= |G|\langle \chi_2, \chi_4\rangle = 3 + 3a + 4b\omega + 4c\omega^2 \\
0 &= |G|\langle \chi_3, \chi_4\rangle = 3 + 3a + 4b\omega^2 + 4c\omega
\end{aligned}$$

Solving this gives $a = -1$, $b = c = 0$, so the full character table follows by substituting these values.

Example 21.2.4. Let G be the symmetric group S_4. The conjugacy class representatives are $g_1 = 1$, $g_2 = (12)(34)$, $g_3 = (123)$, $g_4 = (12)$, $g_5 = (1234)$, with conjugacy classes of sizes 1, 3, 8, 6, 6 respectively. We know that $V_4 \leq S_4$ and $S_4/V_4 \cong S_3$. Hence, this gives irreducible characters $\tilde{\mathbb{1}}, \tilde{\epsilon}, \tilde{\chi_W}$ obtained by inflation from S_3.

This gives a partial table:

g	1	g_2	g_3	g_4	g_5
$\lvert g^G\rvert$	1	3	8	6	6
$\lvert C_G(g)\rvert$	24	8	3	4	4
$\tilde{\mathbb{1}}$	1	1	1	1	1
$\tilde{\epsilon}$	1	1	1	-1	-1
$\tilde{\chi_W}$	2	2	-1	0	0
χ_4	d_4	α_4	β_4	γ_4	δ_4
χ_5	d_5	α_5	β_5	γ_5	δ_5

Now noting that $d_4^2 + d_5^2 = 24 - 1^2 - 1^2 - 2^2 = 18$, the only solutions with positive integers to this is $d_4 = d_5 = 3$ by column orthogonality. By applying this again to the first pair of columns and the second column, we obtain

$$1 + 1 + 4 + 3\alpha_4 + 3\alpha_5 = 0 \qquad 1^2 + 1^2 + 2^2 + |\alpha_4|^2 + |\alpha_5|^2 = 8$$

Hence $\alpha_4 + \alpha_5 = -2$ and $|\alpha_4|^2 + |\alpha_5|^2 = 2$, which solves to $\alpha_4 = \alpha_5 = -1$.

Applying this to the third column we get

$$1^2 + 1^2 + (-1)^2 + |\beta_4|^2 + |\beta_5|^2 = 3$$

Thus $\beta_4 = \beta_5 = 0$.

Similar considerations give $\gamma_5 = -\gamma_4$ and that $|\gamma_4| = 1$. As $g_4 = (12)$ has order 2, it acts with eigenvalues ±1 in any representation. Hence γ_4 is the sum of these eigenvalues, and is a real number, so the choices are $\gamma_4 = \{1, -1\}$. Without loss of generality, we may assume that $\gamma_4 = 1$, otherwise swapping χ_4 with χ_5. Row orthogonality gives $\delta_4 = -1$ and $\delta_5 = 1$, completing our table.

21.3 Burnside's Theorem

Proposition 21.3.1. *$\chi(g)$ is an algebraic integer for all $g \in G$.*

Proof. $\chi(g)$ is a sum of ord-g-th roots of unity, why are all algebraic integers. These form a subring of $\mathbb{C}$ □

Lemma 21.3.2. *Let G be a finite group and let $C_1, \dots, C_r$ be the conjugacy classes in G. Let S be the additive subgroup of $\mathbb{C}G$ generated by the conjugacy class sums. Then S is a subring of $\mathbb{Z}(\mathbb{C}G)$.*

Proof. Sketch. Show stability under multiplication (as we know it is stable under addition.) (show coef is the same in the same conjugacy class) □

Theorem 21.3.3. *Let V a simple $\mathbb{C}G$-module with $g \in G$.*

1. *The conjugacy class sum $\widehat{g^G}$ acts on V by the scalar $\frac{|g^G|\chi_V(g)}{\chi_V(1)} \in \mathbb{C}$*
2. *The scalar above is an algebraic integer*

Proof. As V is a simple $\mathbb{C}G$-module and the conjugacy class sum $z := \widehat{g^G}$ is central in $\mathbb{C}G$, it acts by a scalar $z_V \in \mathbb{C}$ on every simple $\mathbb{C}G$-module by Schur's Lemma. Taking the trace of this action, we get

$$z_V \dim V = |g^G|\chi_V(g)$$

Hence (i) follows from the fact $\dim V = \chi(1)$.

Now let $\rho : G \to \mathrm{GL}(V)$ be the representation afforded by V. Then ρ extends to a $\mathbb{C}$-algebra homomorphism $\tilde{\rho} : \mathbb{C}G \to \mathrm{End}(V)$. The restriction of this homomorphism to the center is the central character of V, so $\tilde{\rho}(\mathbb{C}G) \subseteq \mathbb{C}$. Hence $\tilde{\rho}(S)$ is a finitely generated abelian subgroup of $\mathbb{C}$. It is also a subring of $\mathbb{C}$ as $\tilde{\rho}$ is a ring homomorphism and S is a subring of $Z(\mathbb{C}G)$. Hence $z_V \cdot \tilde{\rho}(S) \subseteq \tilde{\rho}(S)$. □

Corollary 21.3.4. *If V is a simple $\mathbb{C}G$-module, then* $\dim V$ *divides* $|G|$.

Proof. By row orthogonality,

$$\sum_i \chi_V(g^{-1})\frac{|g_i^G|\chi_V(g_i)}{\chi_V(1)} = \frac{|G|}{\chi_V(1)}$$

Now the left side is an algebraic integer, and the right side shows it is a rational number. Hence this is an integer. □

Definition 21.3.5. *Let G be a finite group and let p be a prime. Write $|G| = p^\alpha m$ where $p \nmid m$ A **sylow p-subgroup** of G is a subgroup P of G order p^α.*

Theorem 21.3.6 (Sylow)**.** *Let G be a finite group.*

1. *G contains at least one Sylow p-subgroup.*
2. *Any two sylow p-subgroups are conjugate in G*
3. *The number of Sylow p-subgroups of G is congruent to 1 mod p, and this number divides $m = |G|/p^\alpha$.*

Lemma 21.3.7. *Let G be a group of order $p^\alpha q^\beta$ where p and q are distinct primes with $\alpha, \beta \geq 1$. Let g be a central element of a Sylow p-subgroup P of G. Then $|g^G|$ is a power of q.*

Proof. As P centralises g, we have $P \leq C_G(g)$. Hence $|G : C_G(g)|$ divides $|G|/|P| = q^\beta$. However, this index equals $|g^G|$. □

Lemma 21.3.8. *Let $\alpha = \frac{\zeta_1 + \cdots + \zeta_n}{n}$ be sums of roots of unity, and α is an algebraic integer. Then either $\alpha = 0$ or $\alpha = \zeta_1 = \cdots = \zeta_n$.*

Theorem 21.3.9. *Let G be a finite group and suppose that the size of a conjugacy class of a non central element $g \in g$ is a power of q. Then G is not a simple group.*

Corollary 21.3.10 (Burnside)**.** *Let G be a non-abelian group of order $p^\alpha q^\beta$ where p, q are primes. Then G is not a simple group.*

21.4 Module vs Representation

Example 21.4.1. Consider the representation $\rho : \mathbb{Z} \to \mathrm{GL}(V)$ via the extension of $n \mapsto (M \mapsto M^n)$. Then,

$$k\mathbb{Z} = \oplus_{n \in \mathbb{Z}} kT^n = k[T, T^{-1}]$$

- $\rho : G \to \mathrm{GL}(V) \leftrightarrow kG$-module V
- ρ completely reducible $\leftrightarrow$ kG is completely reducible
- subrepresentations correspond exactly to submodules
- If $V = U \oplus W$ (subreps) correspond
- semisimple (kG as a kG module is completely reducible)
- Noting that $V^* \otimes V \cong \mathrm{End}(V)$, the left ideals of $\mathrm{End}(V)$ (are of the form $U \otimes V$, $U \subseteq V^*$) correspond to subspaces of V^*.

Example 21.4.2. Let $G = C_3 = \langle x \rangle$. Suppose that $\mathrm{char}(k) \neq 3$ and that k contains a primitive cube root of unity.

Then, kG is generated by kx, with the two commuting with each other. Thus, we have a surjective evaluation homomorphism from $k[t] \twoheadrightarrow kG$ sending $t \mapsto x$. Now by the first isomorphism theorem, $\ker \phi = (t^3 - 1)$. This induces an isomorphism

$$kC_3 \cong k[t]/(t^3 - 1) \cong k[t]/(t - 1) \times k[t]/(t - \omega) \times k[t]/(t - \omega^2)$$

by the chinese remainder theorem.

Lemma 21.4.3. *Let χ be a character of G. The set $N := \{g \in G \mid \chi(g) = \chi(1)\}$ is a normal subgroup of G, and is exactly the kernel of the representation.*

Proof. Let χ be a character of the complex representation $\rho : G \to \mathrm{GL}(V)$. If $g \in N$, $\rho(g)$ is diagonalizable, so we can find a basis of $\rho(g)$-eigenvectors $\{v_1, \ldots, v_n\}$ for V with eigenvalues $\lambda_1, \ldots, \lambda_n$ where each λ_i is a order-g-th root of unity. Now,

$$\chi(g) = \mathrm{tr}\rho(g) = \lambda_1 + \cdots + \lambda_n = n$$

The argument then follows by Cauchy-Schwarz. □

Proposition 21.4.4. *G is simple if and only if $\chi(g) \neq \chi(1)$ for all $g \neq 1$ and every irreducible $\chi \neq \mathbb{1}$.*

Proof. $\Rightarrow$ □

Proposition 21.4.5. *Let χ be a character of G. $\chi(g^{-1}) = \overline{\chi(g)}$ for all $g \in G$.*

Proof. Sketch. Take the eigenvalues, these are on roots of unity, the inverse forms a set of $\chi(g^{-1})$, the inverse is the conjugate. □

Proposition 21.4.6. *$g \in G$ is conjugate to g^{-1} if and only if $\chi(g) \in \mathbb{R}$ for every character χ of G.*

Proof. ($\Rightarrow$) Characters are class functions so $\chi(g^{-1}) = \chi(g) = \overline{\chi(g)} \in \mathbb{R}$.

($\Leftarrow$) If all $\chi_i \in \mathbb{R}$ for irreducible characters but g is not conjugate to g^{-1}, by column orthogonality, we have

$$0 = \sum_i \overline{\chi_i(g^{-1})}\chi_i(g) = \sum_i \chi_i(g)^2$$

As each component is real, this forces $\chi_i(g) = 0$. On the other hand by column orthogonality on itself,

$$0 = \sum_i \overline{\chi_i(g)}\chi_i(g) = |C_G(g)| \geq 1$$

Hence a contradiction, showing that g is conjugate to g^{-1}. □

Proposition 21.4.7. *The following things can be found from the character table:*

- $|G|$
- $|G : G'|$ *thus also* $|G'|$
- $|Z(G)|$

Proof. Note first that $|G| = \sum_i \chi_i(1)^2$ and that $|G : G'| = |\{i \mid \chi_i(1) = 1\}|$, and we use these to find $|G'| = |G|/|G : G'|$.

Finally, elements in the center are exactly those with trivial conjugacy classes, hence g is in the center if and only if $C_G(g) = G$. By column orthogonality, this is exactly when $\sum_i |\chi_i(g)|^2 = |C_G(g)| = |G|$ by column orthogonality. This gives an explicit method to compute the size of the center. □

22 Techniques

22.0.1 Computing Conjugacy Classes

1. By the orbit stabilizer, we always have $|g^G||C_G(g)| = |G|$
2. The elements in the center each form their own conjugacy class. Then we can use the fact $|G| = |Z(G)| + \sum |C_i|$
3. For S_n, use cycle-type analysis
4. Normal subgroups are unions of conjugacy classes

22.0.2 Finding Characters

1.

22.1 Definitions

Definition 22.1.1. *Let X be a space and let u and v be paths such that $u(1) = v(0)$. The* ***composite path*** *$u.v$ is given by*

$$u.v(t) = \begin{cases} u(2t) & \text{if } 0 \le t \le \frac{1}{2} \\ v(2t-1) & \text{if } \frac{1}{2} \le t \le 1 \end{cases}$$

23 Graph

Note to self: we only contain notes about graphs that are important from a topological perspective, and less from a number theory / algorithm perspective.

23.1 Definitions

Definition 23.1.1. *A* ***countable graph*** *Γ is specified by*

- *A finite or countable set V of* ***vertices***
- *A finite or countable set E of* ***edges***
- *A function δ which sends an edge e to a subset of V with either 1 or 2 elements. $\delta(e)$ is known as* ***endpoints*** *of e.*

We can construct an associated topological space, or the **graph** Γ as follows. Take a disjoint union of points corresponding to vertices, and a disjoint union of copies of the interval I corresponding to edges. For each $e \in E$, identity 0 in the associated copy of I with one vertex in $\delta(e)$ and 1 with the other vertex of $\delta(e)$.

Definition 23.1.2. *An* ***orientation*** *on the graph Γ is a choice of functions $\iota : E \to V$ and $\pi : E \to V$ such that for each $e \in E$, $\delta(e) = \{\iota(e), \pi(e)\}$. We say that $\iota(e)$ and $\pi(e)$ are* ***intial*** *and* ***terminal*** *vertices of the edge e, and we view the edge as running from the intial vertex to the terminal vertex (in a directed sense).*

Definition 23.1.3. *Let Γ be a graph with vertex set V, edge set E, and endpoint function δ. A* ***subgraph*** *of Γ is the vertex set $V' \subseteq V$ and edge set $E' \subseteq E$ with the endpoint function being the restriction of δ. To be well-defined, we need for each $e \in E'$, $\delta(e) \subseteq V'$. If Γ is oriented, then the subgraph inherits the orientation.*

Definition 23.1.4. *An* **edge path** *in a graph Γ is a concatenation $u_1 \dots u_n$ where each u_i is either a path running along a single edge at unit speed, or a constant path based at a vertex.*

A **edge loop** *is an edge path $u : I \to \Gamma$ where $u(0) = u(1)$.*

An edge path (respectively, edge loop) is said to be **embedded** *if u is injective (respectively, if the only points in I with the same image under u are 0 and 1).*

23.2 Tree

Definition 23.2.1. *A* ***tree*** *is a connected graph that contains no embedded edge loops.*

Lemma 23.2.2. *In a tree, there is a unique embedded edge path between distinct vertices.*

Proof. Any two distinct vertices are connected by an edge path, since the tree is connected. A shortest such path is embedded. We wish to show that this is unique.

Suppose for a contradiction there are two distinct embedded edge paths $p = u_1 \dots u_n$ and $p' = u'_1 \dots u'_n$, between a distinct pair of vertices. Let $u_i(0)$ be the point on p where the paths first diverge. Let $u_j(1)$ be the next point on p which lies in the image of p'. Then the concatenation of $u_i \dots u_j$ with the sub-arc of p' between $u_j(1)$ and $u_i(0)$ form an embedded edge loop, a contradiction on the assumption that we have a tree. □

Definition 23.2.3. *A* ***maximal tree*** *in a connected graph* Γ *is a subgraph* T *that is a tree, but any addition of any edge* $E(\Gamma) \setminus E(T)$ *to* T *gives a graph that is not a tree.*

Lemma 23.2.4. *Let* Γ *be a connected graph and let* T *be a subgraph that is a tree. Then the following are equivalent :*

1. $V(T) = V(\Gamma)$

2. *T is maximal*

Proof. $(i) \Rightarrow (ii)$ Let e be an edge of $E(\Gamma) \setminus E(T)$. If the endpoints of e are the same vertex, then adding e to T gives a subgraph that is not a tree, as it contains an embedded edge loop. Without loss of generality, assume the endpoints of d are distinct. They lie in T, as $V(T) = V(\Gamma)$. They are connected by an embedded edge path p in T by Lemma 23.2.2. Now, $p \cup e$ is an embedded loop in $T \cup e$, thus is not a tree.

$(ii) \Rightarrow (i)$ Suppose that T is a maximal tree and there is a vertex v of Γ that is not in $V(T)$. Pick a shortest edge path from T to v, which exists as Γ is connected. The first edge of this path starts in $V(T)$ but cannot end in $V(T)$. We can therefore add this to T to create a larger tree, which contradicts maximality. □

Lemma 23.2.5. *Any connected graph* Γ *contains a maximal tree.*

Proof. By definition, $V(\Gamma)$ is finite or countable. We can therefore choose a total ordering on $V(\Gamma)$. Without loss of generality, we may assume that for each $i \geq 2$, the i-th vertex shares an edge with an earlier vertex. We construct a nested sequence of subgraphs $T_1 \subsetneq T_2 \subsetneq \cdots$ of trees where $V(T_i)$ is the first i vertices up to the ordering.

Set T_1 to be the first vertex. By assumption, there is an edge e joining the i-th vertex to one of the previous vertices, so we can set $T_i = T_{i-1} \cup e$. There are no new embedded edge loops, so inductively any T_i is a tree.

We claim that $T = \bigcup_i T_i$ is a tree. Suppose that it contains an embedded edge loop ℓ. Then, as ℓ consists of finitely many edges, they must all appear in T_i, but then T_i is not a tree, a contradiction. As T contains all the vertices of Γ, it is maximal by Lemma 23.2.4. □

23.3 Cayley Graphs

Definition 23.3.1. *Let* G *be a group and let* S *be a set of generators for* G*. The associated* ***Cayley Graph*** *is an oriented graph with vertex set* G *and edge set* $G \times S$*. Eah edge is associated with a pair* (g, s) *where* $g \in G$ *and* $s \in S$*. The functions* ι *and* π *are specified by* $\iota(g, s) = g$ *and* $\pi(g, s) = gs$*. We say that this edge is* ***labelled*** *by the generator* s*.*

The Cayley graph of a group depends on a choice of generators. We also note that any two points in a Cayley graph can be joined by a path. Conversely, given any path from the identity to the g vertex, we can write g as a product of generators and their inverses. We therefore have a correspondence between closed loops starting at the identity and ways of writing the identity.

24 Topological Structures

24.1 Simplicial Complexes

Definition 24.1.1. *The **standard** n**-simplex** is the set*

$$\Delta^n = \{(x_0, \ldots, x_n) \in \mathbb{R}^{n+1} \mid x_i \geq 0, \forall i \sum_i x_i = 1\}$$

*The non-negative integer n is the **dimension** of the simplex. The vertices denoted $V(\Delta^n)$ are points $(x_0, \ldots, x_n)$ in Δ^n such that $x_i = 1$ for some i. For each non-empty subset A of $\{0, \ldots, n\}$, there is a **face** of Δ^n which is*

$$\{(x_0, \ldots, x_n) \in \Delta^n \mid x_i = 0 \ \forall i \notin A\}$$

*Note that Δ^n is a face of itself. The **inside** of Δ^n is*

$$\text{inside}(\Delta^n) = \{(x_0, \ldots, x_n) \in \Delta^n \mid x_i > 0 \forall i\}$$

Note that the inside of Δ^0 is Δ^0.

We note that $V(\Delta^n)$ is a basis for $\mathbb{R}^{n+1}$. Thus any function $f : V(\Delta^n) \to \mathbb{R}^m$ extends to a unique linear map $\mathbb{R}^{n+1} \to \mathbb{R}^m$. The restriction of this to Δ^n is known as the **affine extension** of f, or just called affine.

Definition 24.1.2. *A **face inclusion** of a standard m-simplex into a standard n-simplex where $m < n$ is the affine extension of an injection $V(\Delta^m) \to V(\Delta^n)$.*

Definition 24.1.3. *An **abstract simplicial complex** is a pair (V, Σ) where V is a set of vertices and Σ is a set of non-empty finite subsets of V called simplices such that*

- *For each $v \in V$, $\{v\} \in \Sigma$*
- *If $\sigma \in \Sigma$, any nonempty subset of σ is also in Σ.*

*We say that (V, Σ) is **finite** if V is a finite set.*

Definition 24.1.4. *The **topological realisation** $|K|$ of an abstract simplicial complex $K = (V, \Sigma)$ is the space obtained by the following procedure:*

1. *For each $\sigma \in \Sigma$, take a copy of the standard n-simplex, where $n + 1$ is the number of elements of σ. Denote this simplex Δ_σ, labelling its vertices with elements of σ*
2. *Whenever $\sigma \subsetneq \pi \in \Sigma$, identify Δ_σ with a subset of Δ_π via face inclusion that sends elements of σ to corresponding elements of π.*

Equivalently, it is the quotient space obtained by a disjoint union of simplices in (i) and imposing the equivalence in (ii).

Any point $x \in |K|$ lies inside a unique simplex $\sigma = (v_0, \ldots, v_n)$. Thus it can be expressed as

$$x = \sum_{i=0}^{n} \lambda_i v_i$$

for unique positive numbers $\lambda_0, \ldots, \lambda_n$ that sum to 1. If $V = \{w_0, \ldots, w_m\}$, we write $x = \sum \mu_i w_i$ taking $\mu_i = 0$ if $w_i \notin \{v_0, \ldots, v_n\}$. If $|K|$ is the topological realisation of an abstract simplicial complex K, we denote the images of the vertices in $|K|$ by $V(|K|)$.

Note that when we refer to a **simplicial complex**, we mean either the abstract simplicial complex or its topological realisation.

Definition 24.1.5. *A **triangulation** of a space X is a simplicial complex K with a choice of homeomorphism $|K| \to X$.*

Example 24.1.6. The torus $S^1 \times S^1$ has a triangulation using nine vertices, using the standard grid.

Definition 24.1.7. *A **subcomplex** of a simplicial complex (V, Σ) is a simplicial complex (V', Σ') such that $V' \subseteq V$ and $\Sigma' \subseteq \Sigma$.*

Definition 24.1.8. *A **simplicial map** between abstract simplicial complexes between (V_1, Σ_1) and (V_2, Σ_2) is a function $f : V_1 \to V_2$ such that for all $\sigma_1 \in \Sigma_1$, $f(\sigma_1) = \sigma_2$ for some $\sigma_2 \in \Sigma_2$. It is a **simplicial isomorphism** if it has a simplicial inverse.*

Note that this map need not be injective, thus may decrease the dimension of a simplex.

Proposition 24.1.9. *A simplicial map f between abstract simplicial complexes K_1 and K_2 induces a continuous map $|f| : |K_1| \to |K_2|$.*

Proof. Define $|f|$ on $V(|K_1|)$ according to f, extending to each simplex using the unique affine extension. □

This map is also called a simplicial map. Note also that this map is determined by the image of its vertices, and is uniquely determined from there.

Definition 24.1.10. *A **subdivision** of a simplicial complex K is a simplicial complex K' with a homeomorphism $h : |K'| \to |K|$ such that for any simplex σ' of K', $h(\sigma')$ lies entirely in a simplex of $|K|$ and the restriction of h to σ' is affine (linearity on convex combinations).*

Example 24.1.11. Let K be the triangulation of $I \times I$ with a single diagonal from the top left to bottom right. For any positive integer r, let K' be the triangulation of $I \times I$ by dividing $I \times I$ tinto a lattice of r^2 congruent squares, dividing each along the diagonal that runs from top left to bottom right. Then K' is a subdivision of K. We write $(I \times I)_{(r)}$ for this.

Definition 24.1.12. *Let K be a simplicial complex. An **edge path** is a finite sequence $(a_0, \ldots, a_n)$ of vertices of K such that for each i, $\{a_{i-1}, a_i\}$ spans a simplex of K. The length of the path is n.*

*An **edge loop** is an edge path with $a_n = a_0$. We define concatenation of edge paths in the standard way.*

24.2 Cell complexes

Definition 24.2.1. *Let X be a space, and $f : S^{n-1} \to X$ be a map. The space obtained by attaching an n-cell to X along f is defined to be the quotient of the disjoint union $X \sqcup D^n$ such that for each point $x \in X$, $f^{-1}(x)$ and x are all identified to a point. We denote this by $X \cup_f D^n$.*

Remark 24.2.2. There is a homeomorphic image of both X and the interior of D^n in $X \cup_f D^n$ by the natural map. There is an induced map from $D^n \to X \cup_f D^n$ but this need not be injective, as the points in the boundary of D^n may be identified.

Definition 24.2.3. *A (finite) **cell complex** is a space X decomposed as*

$$K^0 \subsetneq K^1 \subsetneq \cdots \subsetneq K^n = X$$

where

1. K^0 is a finite set of points

2. K^i is obtained from K^{i-1} by attaching a finite collection of i-cells.

Example 24.2.4. A finite graph is precisely a finite cell complex that consists only of 0-cells and 1-cells.

Remark 24.2.5. Any finite simplicial complex is a finite cell complex by letting each n simplex be an n-cell.

Example 24.2.6. The torus $S^1 \times S^1$ has a cell structure with one 0-cell, two 1-cells and a single 2-cell. Viewing K^1 as a graph, give its two edges an orientation, labelling them a and b. The attaching map $f : S^1 \to K^1$ of the 2-cell sends the circle along the path $aba^{-1}b^{-1}$.

25 Homotopy

25.1 Basic Definitions and Properties

Definition 25.1.1. *A **homotopy** between two maps $f, g : X \to Y$ is a map $H : X \times I \to Y$ such that $H(x, 0) = f(x)$ and $H(x, 1) = g(x)$ for all $x \in X$. We say that f, g are **homotopic** and write $f \simeq g$ or $H : f \simeq g$, or $f \overset{H}{\simeq} g$.*

Example 25.1.2. Suppose that Y is a subset of $\mathbb{R}^n$ that is convex. Then for any two maps $f, g : X \to Y$ are homotopic by

$$(x, t) \mapsto (1 - t)f(x) + tg(x)$$

This is known as the straight-line homotopy.

Lemma 25.1.3 (Gluing Lemma). *If $\{C_1, \ldots, C_n\}$ is a finite covering of a space X by closed subsets and $f : X \to Y$ is a function whose restriction to each C_i is continuous, then f is continuous.*

Proof. The map f is continuous if and only if $f^{-1}(C)$ is closed for each closed subset of Y. But $f^{-1}(C) = \bigcup_{i=1}^{n} f^{-1}(C) \cap C_i$, which is a finite union of closed sets, thus closed. □

Lemma 25.1.4. *For any two spaces X and Y, homotopy is an equivalence relation of continuous maps $X \to Y$.*

Proof. Reflexive: for any $f : X \to Y$, $H : f \simeq f$ by $H(x, t) = f(x)$.

Symmetric: if $H : f \simeq g$, then $\bar{H} : g \simeq f$ where $\bar{H}(x, t) = H(x, 1 - t)$.

Transitive: if $H : f \simeq g$ and $K : g \simeq h$, then $L : f \simeq h$ via

$$L(x, t) = \begin{cases} H(x, 2t) & \text{if } 0 \leq t \leq \frac{1}{2} \\ K(x, 2t - 1) & \text{if } \frac{1}{2} \leq t \leq 1 \end{cases}$$

L is continuous by the gluing lemma. □

Remark 25.1.5. If we take X to be a single point, the continuous maps $X \to Y$ are points of Y, thus homotopies between them are paths. So the relation of being connected by a path is an equivalence relation on Y. These equivalence classes are called **path-components** of Y. If Y has a single path-component, we call is **path-connected**.

Lemma 25.1.6. *Given the following continuous maps :*

$$\begin{tikzcd} W \arrow[r, "f"] & X \arrow[r, shift left, "g"] \arrow[r, shift right, "h"'] & Y \arrow[r, "k"] & Z \end{tikzcd}$$

If $g \simeq h$, then $gf \simeq hf$ and $kg \simeq kh$.

Proof. Let H be the homotopy between g and h. Then $k \circ H : X \times I \to Z$ is a homotopy between kg and kh.

Similarly, $H \circ (f \times \mathrm{id}_I) : W \times I \to Y$ is a homotopy between gf and hf. □

Definition 25.1.7. *Two spaces X and Y are* ***homotopy equivalent*** *written $X \simeq Y$ if there are maps*

$$\begin{tikzcd} X \arrow[r, shift left, "f"] & Y \arrow[l, shift left, "g"] \end{tikzcd}$$

such that $gf \simeq \mathrm{id}_X$ and $fg \simeq \mathrm{id}_Y$.

Lemma 25.1.8. *Homotopy equivalence is an equivalence relation on spaces.*

Proof. Reflexivity and symmetry are straightforward. For transitivity, consider the following maps:

$$\begin{tikzcd} X \arrow[r, shift left, "f"] & Y \arrow[l, shift left, "g"] \arrow[r, shift left, "h"] & Z \arrow[l, shift left, "k"] \end{tikzcd}$$

where fg, gf, hk, kh are all homotopic to the relavant identity map. Then by Lemma 25.1.6, $gkhf \simeq g(\mathrm{id}_Y)f = gf \simeq \mathrm{id}_X$. So, $(gk)(hf) \simeq \mathrm{id}_X$, and similarly $(hf)(gk) \simeq \mathrm{id}_Z$. □

Definition 25.1.9. *A space X is* ***contractible*** *if it is homotopy equivalent to the space with one point.*

There is a unique map $X \to \{*\}$ and any map $\{*\} \to X$ sends $*$ to some point $x \in X$. Then $\{*\} \to X \to \{*\}$ is the identity, and $X \to \{*\} \to X$ is the constant map c_x. Hence X is contractible if and only if $\mathrm{id}_X \simeq c_x$ for some $x \in X$.

Example 25.1.10. If X is a convex subspace of $\mathbb{R}^n$, then for any $x \in X$, $c_x \simeq \mathrm{id}_X$ by the straight-line homotopy. Hence X is contractible. In particular, $\mathbb{R}^n$ and D^n are both contractible.

Definition 25.1.11. *When A is a subspace of a space X and $\iota : A \to X$ is the inclusion map, we say that a map $r : X \to A$ such that $ri = \mathrm{id}_A$ and $ir \simeq \mathrm{id}_X$ is a* ***homotopy retract****. In these circumstances, A and X are homotopy equivalent.*

Example 25.1.12. Let $\iota : S^{n-1} \to \mathbb{R}^n \backslash \{0\}$ be the inclusion map, and define

$$r(x) = x/|x|$$

Then $ri = \mathrm{id}_{S^{n-1}}$ and $H : ir \simeq \mathrm{id}_{\mathbb{R}^n \backslash \{0\}}$ by

$$H(x,t) = tx + (1-t)x/|x|$$

This is well-defined as the straight line between x and $x/|x|$ does not go through the origin. Thus r is a homotopy retract and our equivalence follows.

Example 25.1.13. Let M denote the Möbius band. There is an inclusion map $\iota : S^1 \to M$ sending $e^{2\pi ix}$ to $(x, \frac{1}{2})$. There is a retraction map sending $(x, y) \mapsto (x, \frac{1}{2})$. Then r is a homotopy retract via the straight-line homotopy.

Similarly, $S^1 \times \{\frac{1}{2}\}$ is a homotopy retract of $S^1 \times I$. Hence $M \simeq S^1 \simeq S^1 \times I$.

Definition 25.1.14. *let X and Y be spaces and let A be a subspaces of X. Then two maps $f, g : X \to Y$ are* ***homotopic relative*** *to A if $f|_A = g|_A$ and there is a homotopy $H : f \simeq g$ such that $H(x, t) = f(x) = g(x)$ for all $x \in A$ and $t \in I$.*

Remark 25.1.15. With a similar notion to homotopy equivalence, there is closure under composition and is an equivalence relation. (Proof is similar.)

25.2 The Simplicial Approximation Theorem

Definition 25.2.1. *Let K be a simplicial complex, and let x be a point in $|K|$. The* ***star*** *of x in $|K|$ is the following subset of $|K|$,*

$$\mathrm{st}_K(x) = \bigcup\{\mathrm{inside}(\sigma) \mid \sigma \textit{ is a simplex of } |K| \textit{ and } x \in \sigma\}$$

Lemma 25.2.2. *For any $x \in |K|$, $\mathrm{st}_K(x)$ is open in $|K|$.*

Proof. Consider

$$\begin{aligned}|K| - \mathrm{st}_K(x) &= \bigcup\{\mathrm{inside}(\sigma) \mid \sigma \text{ is a simplex of } |K| \text{ and } x \notin \sigma\} \\ &= \bigcup\{\sigma \mid \sigma \text{ is a simplex of } |K| \text{ and } x \notin \sigma\}\end{aligned}$$

The second equality holds as any point lies in a simplex lies in the inside of some face τ of σ, and $x \notin \sigma$ implies $x \notin \tau$. Now the latter is a subcomplex of K. This is closed, thus $\mathrm{st}_K(x)$ is open. □

Proposition 25.2.3. *Let K and L be simplicial complexes, and let $f : |K| \to |L|$ be a continuous map. Suppose that for each vertex v of K, there is a vertex $g(v)$ of L such that $f(\mathrm{st}_K(v)) \subseteq \mathrm{st}_L(g(v))$. Then g is a simplicial map $V(K) \to V(L)$ and $|g| \simeq f$.*

Proof. First we claim the following. Let $\sigma = (v_0, \ldots, v_n)$ be a simplex of K and let $x \in \mathrm{inside}(\sigma)$. Let τ be the simplex of L such that $f(x)$ lies in the inside of τ. Then $g(v_0), \ldots, g(v_n)$ are vertices of τ.

Since x lies in the inside of τ, it is in $\mathrm{st}_K(v_i)$ for each i. So $f(x) \in f(\mathrm{st}_K(v_i)) \subseteq \mathrm{st}_L(g(v_i))$. Therefore the inside of τ lies in $\mathrm{st}_L(g(v_i))$. Thus $g(v_i)$ is a vertex of τ.

Now, as $g(v_0), \ldots, g(v_n)$ are vertices of τ, they span a simplex which is a face of τ and hence a member of L. Thus g is a simplicial map.

We show homotopy between f and $|g|$ as follows. First consider any $x \in K$. Let τ be a simplex of L that contains $f(x)$ in its inside. Write $x = \sum_{i=0}^n \lambda_i v_i$ where $v_0, \ldots, v_n$ are vertices of the same simplex with $\lambda_i \geq 0$, summing to 1. In particular, $|g|(x) = \sum_{i=0}^n \lambda_i g(v_i)$. The vertices $g(v_0), \ldots, g(v_n)$ are all vertices of τ. Thus, we may define a straight-line homotopy in τ that interpolates between $f(x)$ and $|g|(x)$. This is well-defined, as even though x may lie in several simplices, they all give the same point $H(x, t)$ for all $t \in I$.

H is continuous, as the map agrees on overlapping starts of simplices, and thus follows from the gluing lemma. □

Proposition 25.2.4. *Let K, L, f, g be as in the previous proposition. Let A be any subcomplex of K and let B be a subcomplex of L such that $f(|A|) \subseteq |B|$. Then g also maps A into B and the homotopy between $|g|$ and f sends $|A|$ to $|B|$ throughout.*

Proof. Let v be any vertex of A. Let τ be the simplex of L such that $f(v)$ lies in the inside of τ. Then by the claim above, $g(v)$ is a vertex of τ. Since $f(v) \in |B|$, we deduce that τ lies in $|B|$, and hence $g(v)$ is a vertex of B.

Now consider any point x in $|A|$. Let $(v_0, \dots, v_n)$ be the simplex of K containing x in its inside. Let τ' be the simplex of L such that $f(x)$ lies in the inside of τ'. Then τ' lies in B as $f(x)$ lies in $|B|$. By the first claim in Proposition 25.2.3, $g(v_0), \dots, g(v_n)$ must all be vertices of τ', and hence vertices of B. The straight-line homotopy between f and $|g|$ sends x into τ' throughout, and hence the image of x remains in $|B|$. □

Definition 25.2.5. *The* ***standard metric*** d *on a finite simplicial complex* $|K|$ *is defined to be*

$$d(\sum_i \lambda_i v_i, \sum_i \lambda_i' v_i) = \sum_i |\lambda_i - \lambda_i'|$$

Note this is an actual metric on $|K|$.

Definition 25.2.6. *Let* K' *be the subdivision on* K*, and let* d *be the standard metric on* $|K|$*. The* ***coarseness*** *of the subdivision is*

$$\sup\{d(x,y) \mid x \textit{ and } y \textit{ belong to the star of the same vertex of } K'\}$$

Example 25.2.7. The subdivision $(I \times I)_{(r)}$ has coarseness $4/r$ (by the standard metric).

Theorem 25.2.8 (Lebesgue Covering Theorem)**.** *Let* X *be a complact metric space, and let* $\mathcal{U}$ *be an open covering of* X*. Then there is a constant* $\delta > 0$ *such that every subset of* X *with diameter less than* δ *is entirely contained within some member of* $\mathcal{U}$*.*

Proof. For each $x \in X$, we can find an open $\mathcal{U}_x$ such that $x \in \mathcal{U}_x$. By openness of this, we can find a r_x such that $x \in B(x, r_x) \subseteq \mathcal{U}_x$.

Take the set $B(x, r_x/2)$, which covers X. By compactness, a finite set of balls with x_i that covers X. Take the minimum $r_{x_i}/2$ of this set and set it as δ.

Now, take any subset A of X with diameter less than δ. Pick any $a \in A$ and find the corresponding $B(x_i, r_{x_i}/2)$ such that $a \in B(x_i, r_{x_i}/2)$. By the triangle inequality, any $a' \in A$ is contained in $B(x_i, r_{x_i}) \subseteq \mathcal{U}_{x_i}$. □

Theorem 25.2.9 (Simplicial Approximation Theorem (Variant 1))**.** *Let* K *and* L *be simplicial complexes where* K *is finite, and let* $f : |K| \to |L|$ *be a continuous map. Then, there is a constant* $\delta > 0$ *with the following property. If* K' *is a subdivision of* K *with coarseness less than* δ*, then there is a simplicial map* $g : K' \to L$ *such that* $|g| \simeq f$*.*

Proof. The sets $\{\mathrm{st}_L(w) \mid w \text{ is a vetex of } L\}$ form an open covering of $|L|$, and so the sets $\{f^{-1}(\mathrm{st}_L(w))\}$ form an open covering of $|K|$. Let $\delta > 0$ be the constant from the Lebesgue Covering Theorem for this covering, and let K' be a subdivision of K with coarseness less than δ.

Then, for any vertex v of K', $\mathrm{diam}(\mathrm{st}'_K(v)) \leq \delta$. In particular, there is some vertex w of L such that $\mathrm{st}'_K(v) \subseteq f^{-1}(\mathrm{st}_L(w))$. Hence $f(\mathrm{st}'_K(v)) \subseteq \mathrm{st}_L(w)$. Setting $g(v) = w$ and applying Proposition 25.2.3 gives the claim. □

Proposition 25.2.10. *Let* $A_1, \dots, A_n$ *be subcomplexes of* K *and let* $B_1, \dots, B_n$ *be subcomplexes of* L *such that* $f(A_i) \subseteq B_i$ *for each* i*. Then the simplicial map* $g : V(K') \to V(L)$ *by the above sends* A_i *to* B_i *and the homotopy between* f *and* $|g|$ *sends* A_i *to* B_i *throughout.*

Proof. A simple consequence from Proposition 25.2.4. □

Definition 25.2.11. *Let $K = (V, \Sigma)$ be an abstract simplicial complex. Then its* ***barycentric subdivision*** *$K^{(1)} = (V', \Sigma')$ defined by $V' = \Sigma$ and Σ' specified by the following rule : $(\sigma_0, \ldots, \sigma_n) \in \Sigma'$ if and only if (after possible reordering) $\sigma_0 \subsetneq \sigma_1 \subsetneq \cdots \subsetneq \sigma_n$.*

For each $r \geq 2$, the subdivision $K^{(r)}$ is given by setting $(K^{(r-1)})^{(1)}$.

Proposition 25.2.12. *A finite simplicial complex K has subdivisions $K^{(r)}$ such that the coarseness of $K^{(r)}$ tends to 0 as $r \to \infty$.*

Proof. (Sketch) Without loss of generality, we may consider the K to be the standard n-simplex, as we can perform the operation on this simplex on all the simplices of K simultaneously.

In the reduced case, for each face F of Δ^n with vertices $v_1, \ldots, v_r$, the barycenter of F is $(v_1 + \cdots + v_r)/r$. define a new simplicial complex K' with vertices precisely the barycenters of each of the faces. A set of vertices $w_1, \ldots, w_s$ of K' corresponding to faces $F_1, \ldots, F_s$ of Δ^n span a simplex of K' if and there are (up to re-ordering), there are inclusions $F_1 \subsetneq F_2 \subsetneq \cdots \subsetneq F_s$. This is a subdivision of Δ^n.

We finally note that the coarseness of this tends to 0 as r tends to infinity. □

Theorem 25.2.13 (Simplicial Approximation Theorem (Variant 2)). *Let K and L be simplicial complexes where K is finite, and let $f : |K| \to |L|$ be a continuous map. Then there is some subdivision K' of K and a simplicial map $g : K' \to L$ such that $|g|$ is homotopic to f.*

Proof. Follows from Theorem 25.2.9 and barycentric subdivision makes the coarseness of $K^{(r)}$ tend to 0 as $r \to \infty$. □

26 Groups

26.1 Free Group

Definition 26.1.1. *Given any set S, define S^{-1} to be a copy of S, where each element $x \in S$ is given a corresponding element of S^{-1} by x^{-1}. We note that $S \cap S^{-1} = \emptyset$, and that given $x^{-1} \in S^{-1}, (x^{-1})^{-1} = x$.*

Definition 26.1.2. *A* ***word*** *w is a finite sequence $x_1, \ldots, x_m$ where $m \in \mathbb{Z}_{\geq 0}$ and each $x_i \in S \cup S^{-1}$. We write w as $x_1 x_2 \ldots x_m$. The empty sequence given when $m = 0$ is denoted $\emptyset$.*

Definition 26.1.3. *The* ***concatenation*** *of two words $x_1 x_2 \ldots x_m$ and $y_1 y_2 \ldots y_n$ is the word $x_1 x_2 \ldots x_m y_1 y_2 \ldots y_n$.*

Definition 26.1.4. *A word w' is an* ***elementary contraction*** *of a word w, written $w \searrow w'$, if $w = y_1 x x^{-1} y_2$ and $w' = y_1 y_2$ for words y_1 and y_2, and $x \in S \cup S^{-1}$. We also write $w' \nearrow w$ and say that w is an* ***elementary expansion*** *of w'.*

Definition 26.1.5. *Two words w' and w are equivalent, written $w \sim w'$ if there are words $w_1, \ldots, w_n$ where $w = w_1$ and $w' = w_n$ such that for each i, $w_i \nearrow w_{i+1}$ or $w_i \searrow w_{i+1}$. The equivalence class of a word is denoted $[w]$.*

Definition 26.1.6. *The* ***free group*** *on the set S, denoted $F(S)$ consists of equivalence classes of words in the alphabet S. The composition of two elements $[w]$ and $[w']$ is the class $[ww']$. The identity element is $[\emptyset]$, denoted e. The inverse of an element $[x_1 x_2 \ldots x_n]$ is $[x_n^{-1} \ldots x_2^{-1} x_1^{-1}]$.*

Note that composition is well-defined, and is clear from definitions.

Definition 26.1.7. *A word is* ***reduced*** *if it does not admit an elementary contraction.*

Lemma 26.1.8. *Let w_1, w_2, w_3 be words such that $w_1 \nearrow w_2 \searrow w_3$. Then there is a word w_2' such that $w_1 \searrow w_2' \nearrow w_3$, or $w_1 = w_3$.*

Definition 26.1.9. *Since $w_1 \nearrow w_2$, we can write $w_1 = ab$ and $w_2 = axx^{-1}b$ for some $x \in S \cup S^{-1}$, and words a, b. As $w_2 \searrow w_3$, w_3 is obtained from w_2 by removing yy^{-1} for some $y \in S \cup S^{-1}$. The letters xx^{-1} and yy^{-1} intersect in either zero, one, or two letters. We do a case split.*

If they do not intersect, then we can remove yy^{-1} from w_1 Hence, denoting w_2' to be such a word, we have $w_1 \searrow w_2' \nearrow w_3$. If they intersect at a single letter, $x = y^{-1}$, so w_2 has a chain of letters $xx^{-1}x$ or $x^{-1}xx^{-1}$, and w_1, w_3 are obtained by performing an elementary contraction on these letters. Thus, $w_1 = w_3$. If they intersect in two letters, then we obviously have $w_1 = w_3$.

Proposition 26.1.10. *Any element of a free group $F(S)$ is represented by a unique reduced word.*

Proof. An elementary contraction to a word reduced the length by two. Thus, a shortest representative for an element of $F(S)$ must be reduced. We show that this representative is unique. Suppose there are two distinct words w and w' that are equivalent. Then by definition, we can find a sequence of words $w_1, \dots w_n$ such that $w = w_1$ and $w' = w_n$ and $w_i \nearrow w_{i+1}$ or $w_i \searrow w_{i+1}$ for all i. Consider a shortest such sequence. Then, we must have w_i distinct. Suppose that at some point we have $w_i \nearrow w_{i+1} \searrow w_{i+2}$. Then by Lemma 26.1.8, we can find a w_{i+1}' such that $w_i \searrow w_{i+1}' \nearrow w_{i+2}$. Repeating this, we can perform all $\searrow$ moves before $\nearrow$ ones. Thus, the sequence starts with $w_1 \searrow w_2$ or ends with $w_{n-1} \nearrow w_n$. This implies either w or w' was not reduced, a contradiction. □

Theorem 26.1.11 (Universal Property on Free Groups)**.** *Given any set S and group G and any function $f : S \to G$, there is a unique homomorphism $\phi : F(S) \to G$ such that the following diagram commutes:*

$$\begin{tikzcd}
S \arrow[r, "f"] \arrow[d, "\iota"'] & G \\
F(S) \arrow[ur, "\phi"'] &
\end{tikzcd}$$

where $\iota : S \to F(S)$ is the canonical inclusion.

Proof. We first show existence. Consider any word $w = x_1^{\epsilon_1} \dots x_n^{\epsilon_n}$, where $x_i \in S$ and $\epsilon_i \in \{-1, 1\}$. Define $\phi(w)$ to be $f(x_1)^{\epsilon_1} \dots f(x_n)^{\epsilon_n}$. To show that this is well-defined, given $w \sim w'$, they must have the same image under ϕ. It suffices to show that this is the case when w' is an elementary contraction of w, where $w = w_1xx^{-1}w_2$ or $w = w_1x^{-1}xw_2$ and $w' = w_1w_2$. In the case where $w = w_1xx^{-1}w_2$,

$$\phi(w) = \phi(w_1)f(x)f^{-1}(x)\phi(w_2) = \phi(w_1)\phi(w_2) = \phi(w')$$

The second case is similar. Thus ϕ is well-defined, and is clearly a homomorphism.

Note this map is unique, as if $x \in S$, $\phi(x) = f(x)$, and the fact ϕ is a homomorphism is determined by the map of the generators. □

26.2 Group Presentations

Definition 26.2.1. *Let B be a subset of a group G. The normal subgroup generated by B is the intersection of all normal subgroups of G that contain B. We write $\langle\langle B \rangle\rangle$ for this.*

Remark 26.2.2. The intersection of a collection of normal subgroups is a normal subgroup. Thus $\langle\langle B \rangle\rangle$ is normal in G. It is therefore also the smallest normal subgroup of G that contains B.

Proposition 26.2.3. *The subgroup $\langle\langle B\rangle\rangle$ consists of all expressions of the form*

$$\prod_{i=1}^{n} g_i b_i^{\epsilon_i} g_i^{-1}$$

where $n \in \mathbb{Z}_{\geq\nvdash}, g_i \in G, b_i \in B$ and $\epsilon_i = \pm 1$ for all i.

Proof. Any normal subgroup containing B must contain all the elements of the form gbg^{-1} and $gb^{-1}g^{-1}$. Thus it must also contain a finite product of them. Taking N to be the set of all these finite products, we certainly have $N \subseteq \langle\langle B\rangle\rangle$. It remains to show that N is a normal subgroup, as we have $B \subseteq N$, giving $\langle\langle B\rangle\rangle \subseteq N$.

Identity, inverse, and closure are straightforward. To show normality, note that

$$g\left(\prod_{i=1}^{n} g_i b_i^{\epsilon_i} g_i^{-1}\right) g^{-1} = \prod_{i=1}^{n} g g_i b_i^{\epsilon_i} g_i^{-1} g^{-1} = \prod_{i=1}^{n} (gg_i) b_i^{\epsilon_i} (gg_i)^{-1}$$

which lies in N. □

Definition 26.2.4. *Let X be a set, and let R be a collection of elements of $F(X)$. The group with presentation $\langle X|R\rangle$ is defined to be $F(X)/\langle\langle R\rangle\rangle$. We slightly abuse notation by allowing relations of the form $w_1 = w_2$, which is shorthand for $w_1 w_2^{-1}$.*

Therefore, two words in the alphabet represent the same element of G precisely when there is an element $y \in \langle\langle R\rangle\rangle$ such that $w' = wy$.

Example 26.2.5. The dihedral group D_{2n} can be written as

$$\langle \sigma, \tau \mid \sigma^n, \tau^2, \tau\sigma\tau\sigma\rangle$$

Proposition 26.2.6. *Let $G = \langle X|R\rangle$. Then two words w, w' in X represent the same element of G if and only if they differ by a finite sequence of the following moves*

1. *perform an elementary contraction or expansion*

2. *insert in the word one of the relations in R or its inverse*

Proof. Applying the moves does not change the element of G that it represents. To show that if w and w' represent the same elements of G, they differ by a finite sequence of moves. In particular, as elements of $F(X)$ have the equality $w' = wy$, we can write

$$w' = w\prod_{i=1}^{n} g_i r_i^{\epsilon_i} g_i^{-1}$$

We can obtain $wg_1g_1^{-1}$ by the first move, then obtain $wg_1r_1^{\epsilon_1}g_1^{-1}$ by the second move. Continuing, we can obtain w' from w. □

Example 26.2.7. We can turn $\tau\sigma^n\tau$ into e by the moves as follows :

$$\tau\sigma^n\tau \to \tau\sigma^n\sigma^{-n}\tau \to \tau\tau \to \tau^2\tau^{-2} \to e$$

Proposition 26.2.8. *Every group G has a presentation.*

Proof. Let $F(G)$ be the free group on the generating set G. Then $F(G)$ consists of all equivalence classes of words in G. Thus, if x_1 and x_2 are nontrivial elements of G and $x_3 = x_1x_2$ in G, $[x_3]$ and $[x_1][x_2]$ represent distinct elements of $F(G)$, as they are non-equivalent words in the alphabet G. We have a well-defined homomorphism from $F(G)$ to G, sending each generator of $F(G)$ to the corresponding element of G, which is clearly surjective. Let $R(G)$ be the kernel of this homomorphism. Then, by the first isomorphism theorem, we have $G \simeq F(G)/R(G)$. In particular G has presentation $\langle G|R(G)\rangle$. □

Definition 26.2.9. *The canonical presentation for* G *is* $\langle G|R(G)\rangle$.

Definition 26.2.10. *A presentation* $\langle X|R\rangle$ *is* ***finite*** *if* X *and* R *are both finite sets. A group is* ***finitely presented*** *if it has a finite presentation.*

Lemma 26.2.11. *Let* $\langle X|R\rangle$ *and* H *both be groups. Let* $f : X \to H$ *induce a homomorphism* $\phi : F(X) \to H$. *This descends to a homomorphism* $\langle X|R\rangle \to H$ *if and only if* $\phi(r) = e$ *for all* $r \in R$.

Proof. Note that $\phi(r) = e$ is a necessary condition for ϕ to be a homomorphism, as any $r \in R$ represents the identity element of $\langle X|R\rangle$.

Conversely, if $\phi(r) = e$ for all $r \in R$, we note that any element w of $\langle\langle R\rangle\rangle$ can be written as

$$\prod_{i=1}^{n} w_i r_i^{\epsilon_i} w_i^{-1}$$

for $w_i \in F(X), r_i \in R$. As $\phi(r) = e$, we have $\phi(w) = e$. In particular, ϕ descends to a homomorphism $F(X)/\langle\langle R\rangle\rangle$. □

Definition 26.2.12. *A* ***Tietze Transformation*** *is one of the following moves applied to a finite presentation* $\langle x_1, \ldots, x_m \mid r_1, \ldots, r_n\rangle$

1. *Re-order generators or relations*
2. *Add or remove the relation* e
3. *Perform an elementary contraction or expansion to a relation* r_i
4. *Insert a relation* r_i *or its inverse into one of the other* r_j *or remove it*
5. *Add a generator* x_{m+1} *together with a relation* $w(x_1, \ldots, x_m)x_{m+1}^{-1}$, *which defines it as a word in the old generators, or perform the reverse of this operation*

Note first that these transformations don't alter the group, and are also invertible.

Lemma 26.2.13. *Let* $\langle x_1, \ldots, x_m \mid r_1, \ldots, r_n\rangle$ *be a presentation for a group* G. *Suppose that a word* w *in the generators* $x_1, \ldots, x_m$ *is trivial in* G. *Then there is a sequence of* (ii), (iii), *and* (iv) *moves that transforms this presentation to* $\langle x_1, \ldots, x_m \mid r_1, \ldots, r_n, w\rangle$.

Proof. Start by adding the relation e. As w is trivial in G, we can write get to this element via moves (iii) and (iv). □

Theorem 26.2.14 (Tietze)**.** *Any two finite presentations of a group* G *are convertible into each other by a finite sequence of Tietze transformations.*

Proof. Let $\langle x_1, \dots, x_m \mid r_1, \dots, r_n\rangle$ and $\langle x'_1, \dots, x'_{m'} \mid r'_1, \dots, r'_{n'}\rangle$ be two presentations of G. Since each x'_i is an element of $\langle x_1, \dots, x_m \mid r_1, \dots, r_n\rangle$, it can be written as a word χ'_i in the generators $x_1, \dots, x_m$. Similarly each x_i can be written as a word χ_i in the generators $x'_1, \dots, x'_{m'}$.

We start by applying move (v) m' times to the first presentation to obtain

$$\langle x_1, \dots, x_m x'_1, \dots, x'_{m'} \mid r_1, \dots, r_n, \chi'_1(x'_1)^{-1}, \dots, \chi'_{m'}(x'_{m'})^{-1}\rangle$$

As the relation $x_i = \chi_i$ holds in the group, by Lemma 26.2.13, we can use moves $(ii) \sim (iv)$ to transform this into

$$\langle x_1, \dots, x_m x'_1, \dots, x'_{m'} \mid r_1, \dots, r_n, \chi'_1(x'_1)^{-1}, \dots, \chi'_{m'}(x'_{m'})^{-1}, \chi_1(x_1^{-1}), \dots, \chi_m(x_m^{-1})\rangle$$

Now, the relations $r'_1, \dots, r'_n$ also represent trivial words in the group. Thus by Lemma 26.2.13 again, we transform this into

$$\langle x_1, \dots, x_m x'_1, \dots, x'_{m'} \mid r_1, \dots, r_n, r'_1, \dots r'_{n'} \chi'_1(x'_1)^{-1}, \dots, \chi'_{m'}(x'_{m'})^{-1}, \chi_1(x_1^{-1}), \dots, \chi_m(x_m^{-1})\rangle$$

This presentation is symmetric with respect to primed and unprimed symbols up to reordering. Thus by applying (i) moves and then reversing the derivation, we can obtain the presentation

$$\langle x_1, \dots, x_m \mid r_1, \dots, r_n\rangle$$

□

Proposition 26.2.15. *Given $G_1 = \langle X_1 \mid R_1\rangle$ and $G_2 = \langle X_2 \mid R_2\rangle$, then we have*

$$G_1 \times G_2 \simeq \langle X_1 \sqcup X_2 \mid R_1 \cup R_2 \cup \{xyx^{-1}y^{-1} \mid x \in X_1, y \in X_2\}\rangle$$

Proof. Let $H := F(X_1 \sqcup X_2)/\langle\langle R_1, R_2, [x, y]\rangle\rangle$. Take

$$\tilde{\phi}(x) = \begin{cases} (x, 1) & x \in X_1 \\ (1, x) & x \in X_2 \end{cases}$$

each relator is mapped to the identity, so $\tilde{\phi}$ descends to a well-defined homomorphism ϕ. This is by construction surjective, and is injective as if we take any x in the kernel of ϕ, projecting onto G_1 and G_2 shows they are trivial in each side. Thus x is trivial as we can permute letters inside H. □

Example 26.2.16. D_{2n} has presentation $G := \langle a, b \mid a^n, b^2, abab\rangle$.

We give an explicit surjection from this group to D_{2n} and argue by size. specifically, note that sending $a \mapsto r$ and $b \mapsto s$, labelling rotation by r and reflection by s shows that each relator is sent to the identity by this map. In particular, we have a well-defined homomorphism to D_{2n}. We can reduce every symmetry of an n-gon to either r^k or sr^k, which is hit by words in G. By the same argument, this shows that $|G| \leq 2n$, thus the map is an isomorphism.

Proposition 26.2.17. *Every nontrivial word in the free group has infinite order.*

Proof. We first note that every nontrivial word is conjugate to a nontrivial reduced word such that the last letter is not the inverse of the first (by peeling off these elements, and this equals e if and only if the word itself is trivial). We call these words cyclically reduced for short. Now, conjugate words have the same order, and these words clearly have infinite order by a length argument. □

Proposition 26.2.18. *If S has multiple elements, the center of $F(S)$ is the identity element.*

Proof. Let $|S| \geq 2$ and $a, b \in S$ be generators. Suppose $z \in Z(F(S))$. Then we have $za = az$ and $zb = bz$, each of which forces the first character of z to be a or a^{-1} and b or b^{-1}, which is impossible. □

26.3 Push-out

Definition 26.3.1. *Let G_0, G_1, G_2 be groups and let $\phi_1 : G_0 \to G_1$ and $\phi_2 : G_0 \to G_2$ be homomorphisms. Let $\langle X_1 \mid R_1\rangle$ and $\langle X_2 \mid R_2\rangle$ be canonical presentations of G_1 and G_2, where $X_1 \cap X_2 = \emptyset$. We define the **push-out** $G_1 *_{G_0} G_2$ of*

$$G_1 \overset{\phi_1}{\leftarrow} G_0 \overset{\phi_2}{\rightarrow} G_2$$

to be the group

$$\langle X_1 \cup X_2 \mid R_1 \cup R_2 \cup \{\phi_1(g) = \phi_2(g) \mid g \in G_0\}\rangle$$

Note that the pushout depends on the homomorphism, but is not ambiguous up to isomorphism when ϕ_1 and ϕ_2 are injections (by viewing G_0 to be a subgroup of both G_1 and G_2).

Remark 26.3.2. The inclusions $X_1 \to X_1 \cup X_2$ and $X_2 \to X_1 \cup X_2$ induces canonical homomorphisms $\alpha_1 : G_1 \to G_1 *_{G_0} G_2$ and $\alpha_2 : G_2 \to G_1 *_{G_0} G_2$, such that the following diagrams commutes:

$$\begin{tikzcd}
 & G_0 \arrow[dl, "\phi_1"'] \arrow[dr, "\phi_2"] & \\
G_1 \arrow[dr, "\alpha_1"'] & & G_2 \arrow[dl, "\alpha_2"] \\
 & G_1 *_{G_0} G_2 &
\end{tikzcd}$$

This is because the relation $\phi_1(g) = \phi_2(g)$ holds for each $g \in G_0$ holds in $G_1 *_{G_0} G_2$.

Proposition 26.3.3 (Universal Property of Pushouts)**.** *Let $G_1 *_{G_0} G_2$ be the pushout induced by $\phi_1 : G_0 \to G_1$ and $\phi_2 : G_0 \to G_2$. Let $\beta_1 : G_1 \to H$ and $\beta_2 : G_2 \to H$ be homomorphisms such that the following commutes:*

$$\begin{tikzcd}
 & G_0 \arrow[dl, "\phi_1"'] \arrow[dr, "\phi_2"] & \\
G_1 \arrow[dr, "\beta_1"'] & & G_2 \arrow[dl, "\beta_2"] \\
 & H &
\end{tikzcd}$$

Then there exists a unique homomorphism $\beta : G_1 *_{G_0} G_2 \to H$ such that the following commutes:

$$\begin{tikzcd}
G_1 \arrow[r, "\alpha_1"] \arrow[dr, "\beta_1"'] & G_1 *_{G_0} G_2 \arrow[d, dashed, "\beta"] & G_2 \arrow[l, "\alpha_2"'] \arrow[dl, "\beta_2"] \\
 & H &
\end{tikzcd}$$

Proof. The pushout $G_1 *_{G_0} G_2$ has generators $G_1 \cup G_2$. Define β on these generators by $\beta(g_i) = \beta_i(g_i)$ for all $g_i \in G_i$. Note that this is forced by the commutativity of the second diagram. Thus if the homomorphism exists, it is unique. To show this map is well-defined, it must send relations r in $G_1 *_{G_0} G_2$ with $\beta(r) = e$. This is true for relations in G_1 and G_2, as β_1 and β_2 are well-defined homomorphisms. The other type of relation is $\phi_1(g)(\phi_2(g))^{-1}$ for $g \in G_0$. But $(\beta(\phi_1(g)))(\beta(\phi_2(g)))^{-1} = e$ by the commutativity of the first diagram. □

Lemma 26.3.4. *Let $G_0, G_1, G_2, \phi_1, \phi_2$ be as in the definition for pushouts. Let $\langle X_1' \mid R_1' \rangle$ and $\langle X_2' \mid R_2' \rangle$ be any presentations for G_1 and G_2 where $X_1' \cap X_2' = \emptyset$. Then the pushout is isomorphic to*

$$H := \langle X_1' \cup X_2' \mid R_1' \cup R_2' \cup \{\phi_1(g) = \phi_2(g) \mid g \in G_0\}\rangle$$

Proof. Let $G := G_1 *_{G_0} G_2$ be the pushout. Define $G_1 \to \langle X_1' \mid R_1' \rangle$ and $G_2 \to \langle X_2' \mid R_2' \rangle$ be the 'identity' maps. The inclusions of X_1' and X_2' induce homomorphisms $\beta_1 : G_1 \to H$ and $\beta_2 : G_2 \to H$. This gives a commutative diagram as in Proposition 26.3.3, as the relation $\phi_1(g) = \phi_2(g)$ holds in H. Thus by the same proposition, we have a homomorphism $\beta : G \to H$ with commutative properties.

Now note that there is a function $X_i' \to G_i$ sending each generator to the corresponding element of G_i. Composing this map with α_i to give a function $f : X_1' \cup X_2' \to G$. This induces a homomorphism $\phi : F(X_1' \cup X_2') \to G$, why descends to a homomorphism $\phi : H \to G$ as $\phi(r) = e$ for each relation r in the presentation of H. By construction, this is an inverse for β, thus $G \cong H$. □

Definition 26.3.5. *When G_0 is the trivial group, the pushout $G_1 *_{G_0} G_2$ depends only on G_1 and G_2. This is known as the free product $G_1 * G_2$.*

Example 26.3.6. The free product $\mathbb{Z} * \mathbb{Z}$ is isomorphic to the free group on two generators, as we may take $\langle x \mid \rangle$ and $\langle y \mid \rangle$ for the two presentations, and we know by Lemma 26.3.4 that $\mathbb{Z} * \mathbb{Z}$ is isomorphic to $\langle x, y \mid \rangle$.

Definition 26.3.7. *When $\phi_1 : G_0 \hookrightarrow G_1$ and $\phi_2 : G_0 \hookrightarrow G_2$, the pushout $G_1 *_{G_0} G_2$ is known as the* ***amalgamated free product*** *of G_1 and G_2 along G_0.*

Example 26.3.8. Consider the pushout defined by

$$\mathbb{Z} \overset{\text{id}}{\leftarrow} \mathbb{Z} \overset{\times 2}{\to} \mathbb{Z}$$

Then taking the base set as $\langle t \mid \rangle$, the maps to $\langle x \mid \rangle$ and $\langle y \mid \rangle$ are given by $t \mapsto x$ and $t \mapsto y^2$. Then our imposed equality is $x^2 = y^{2n}$ for all $n \in \mathbb{Z}$. In particular $x = y^2$, so by eliminating the generator x, we are left with $\langle y \mid \rangle$ which is isomorphic to $\mathbb{Z}$

Example 26.3.9. Consider the pushout defined by

$$\mathbb{Z} \overset{\times 2}{\leftarrow} \mathbb{Z} \overset{\times 3}{\to} \mathbb{Z}$$

Then the push-out has presentation

$$\langle u, v \mid u^{2n} = v^{3n}, n \in \mathbb{Z} \rangle$$

which can be written simply as

$$\langle u, v \mid u^2 = v^3, n \in \mathbb{Z} \rangle$$

We then consider the map $u \mapsto yxy$ and $v \mapsto xy$. Then taking $xyx = yxy$, we have

$$\phi(v) = (xy)^3 = xyxyxy = yxyyxy = (yxy)^2 = \phi(u)^2$$

ϕ is surjective as $\phi(uv^{-1}) = y$ and $\phi(v^2u) = x$. This also gives a straightforward inverse, which satisfies the braiding relation, so in particular give isomorphisms.

Proposition 26.3.10. *Let $\alpha : G \to G * H$ be the (left) canonical homomorphism. Then α is injective.*

Proof. We give an explicit π such that $\pi \circ \alpha = \mathrm{id}_G$. Specifically, we take

$$\pi(x) = \begin{cases} x & \text{if } x \in G \\ 1 & \text{if } x \in H \end{cases}$$

This satisfies $\pi\alpha = \mathrm{id}_G$, thus α is injective. □

Remark 26.3.11. Given any $H := G_1 *_{G_0} G_2$, we can reduce any word $w \in H$ to a word of the form

$$w = g_1 h_1 \dots g_n h_n$$

where $g_i \in G_1$ and $h_i \in G_2$, by amalgamating successive letters in G_1 (resp. G_2) and removing identities. By repeating this reduction sequence, we reach a **reduced** word such that g_i, h_i are all nontrivial except possibly g_1 and or h_n.

In the case the product is free, the reduced word is unique (we note that the reduction satisfies the diamond property).

27 Fundamental Group

27.1 Definitions

Definition 27.1.1. *A **loop based at a point** $b \in X$ is a path $\ell : I \to X$ such that $\ell(0) = \ell(1) = b$. The point b is knows as its **basepoint**.*

Definition 27.1.2. *The homotopy classes relative to ∂I of loops based at b form a group, called the **fundamental group** of (X, b), denoted $\pi_1(X, b)$. If ℓ and ℓ' are loops based at b, then $[\ell]$ and $[\ell']$ are their homotopy classes relative to ∂I, with their composition defined as $[\ell].[\ell'] = [\ell.\ell']$.*

Note the base-point is required as a consequence of making sure that two loops can always be composed. If we don't have the requirement that homotopies are relative to ∂I, then any two paths in the same path-component of X are homotopic, as I is contractible (intuitively, collapse f to the path connected node, and move along it, and uncollapse at g). Finally, note that composition of paths itself is not necessarily associative, as the images are equal, but the path traverses through them at different speeds.

We show this is well-defined, is associative, has an identity, and also have inverses.

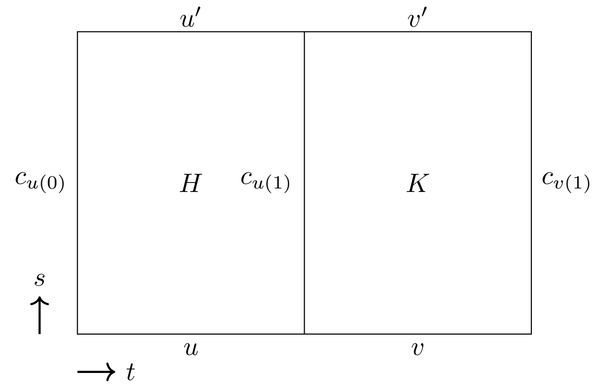
Lemma 27.1.3 (Well-definedness of Fundamental Groups)**.** *Suppose that u and v are paths in X such that $u(1) = v(0)$. Suppose also that u' (and respectively v') are paths with the same endpoints as u (respectively v). If $u \simeq u', v \simeq v'$ both relative to ∂I, then $u.v \simeq u'.v'$, relative to ∂I.*

Proof. Let $H : u \simeq u'$ and $K : v \simeq v'$ be the given homotopies. Then we can define $L : I \times I \to X$ by

$$L(t, s) = \begin{cases} H(2t, s) & \text{if } 0 \le t \le \frac{1}{2} \\ K(2t - 1, s) & \text{if } \frac{1}{2} \le t \le 1 \end{cases}$$

This is continuous by the Gluing Lemma, thus we have $L : u.v \simeq u'.v'$, relative to ∂I.

Alternatively, the following diagram represents L.



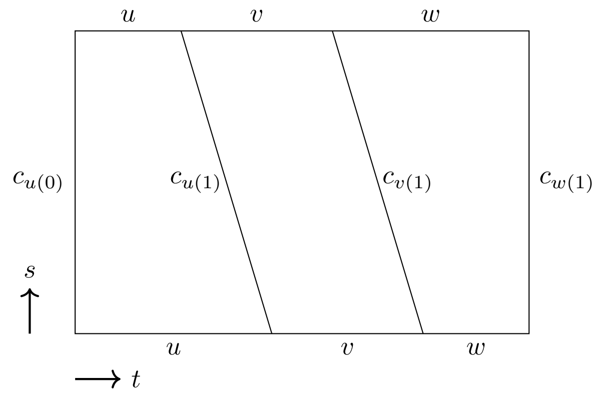
□

Lemma 27.1.4 (Associativity of Fundamental Groups)**.** *Let u, v, w be paths in X such that $u(1) = v(0)$ and $v(1) = w(0)$. Then $u.(v.w) \simeq (u.v).w$ relative to ∂I.*

Proof. We give an explicit homotopy $H : I \times I \to X$ by

$$H(t,s) = \begin{cases} u(\frac{4t}{2-s}) & \text{if } 0 \le t \le \frac{1}{2} - \frac{1}{4}s \\ v(4t-2+s) & \text{if } \frac{1}{2} - \frac{1}{4}s \le t \le \frac{3}{4} - \frac{1}{4}s \\ w(\frac{4t-3+s}{1+s}) & \text{if } \frac{3}{4} - \frac{1}{4}s \le t \le 1 \end{cases}$$

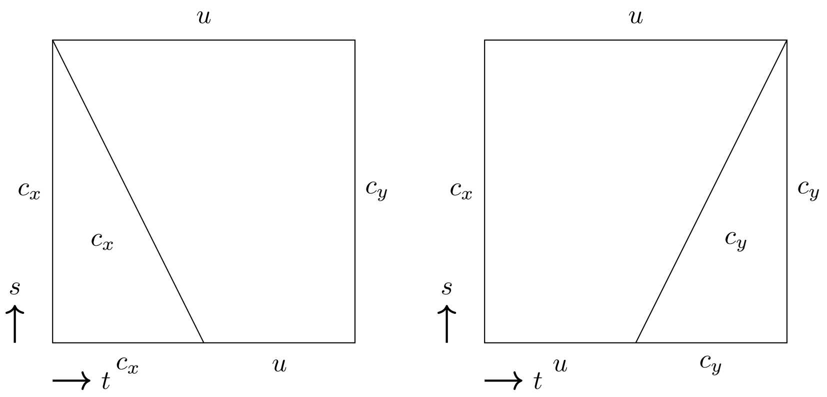
Again, continuity follows from the gluing lemma. Alternatively, we can use the following diagram:



□

Lemma 27.1.5 (Identity of Fundamental Groups)**.** *Let u be a path in X with $u(0) = x$ and $u(1) = y$. Then $c_x.u \simeq u$ relative to ∂I and $u.c_y \simeq u$ relative to ∂I. In particular, $[c_b]$ is the identity element in $\pi_1(X, b)$.*

Proof. We note the following diagrams:



□

Lemma 27.1.6 (Inverses in Fundamental Groups)**.** *Let u be a path in X with $u(0) = x$ and $u(1) = y$, and define u^{-1} as $u^{-1}(t) = u(1-t)$. Then $u.u^{-1} \simeq c_x$ relative to ∂I and $u^{-1}.u \simeq c_y$ relative to ∂I.*

Proof. We give an explicit homotopy between $u.u^{-1}$ and c_x:

$$H(t,s) = \begin{cases} u(2t(1-s)) & \text{if } 0 \leq t \leq \frac{1}{2} \\ u((2-2t)(1-s)) & \text{if } \frac{1}{2} \leq t \leq 1 \end{cases}$$

The idea is 'stopping' how far we go in u, and traversing back. A similar construction can be made for $u^{-1}.u$, by considering the inverse of their paths. □

Example 27.1.7. Let b be the origin in $\mathbb{R}^2$. Then $\pi_1(\mathbb{R}^2, b)$ is the trivial group. This is due to the fact every loop based at b is homotopic relative to ∂I to the constant loop c_b via straight-line homotopy.

Remark 27.1.8. We note that if X_0 is the path-component of X containing the basepoint b, then $\pi_1(X,b) = \pi_1(X_0, b)$. This is a simple consequence of the fact any loop in X based at b must lie entirely in X_0, and the homotopy between two such loops must also lie in X_0.

Proposition 27.1.9. *If b and b' lie in the same path-component of X, then $\pi_1(X,b) \simeq \pi_1(X,b')$.*

Proof. Let w be a path from b to b' in X. If ℓ is a loop based at b, then $w^{-1}.\ell.w$ is a loop based at b', and the function

$$\begin{aligned} w_\# : \pi_1(X,b) &\to \pi_(X,b') \\ [\ell] &\mapsto [w^{-1}.\ell.w] \end{aligned}$$

is well-defined. We also have

$$\begin{aligned} w_\#([\ell])w_\#([\ell']) &= [w^{-1}.\ell.w][w^{-1}.\ell'.w] \\ &= [w^{-1}.\ell.(w.w^{-1}).\ell'.w] \\ &= [w^{-1}.\ell.c_b.\ell'.w] \\ &= [w^{-1}.(\ell.\ell').w] \\ &= w_\#([\ell][\ell']) \end{aligned}$$

thus $w_\#$ is a homomorphism. Also, $w_\#$ has an inverse $(w^{-1})_\#$, since

$$(w^{-1})_\#(w_\#([\ell])) = (w^{-1})_\#([w^{-1}.\ell.w]) = [w.w^{-1}.\ell.w.w^{-1}] = [\ell]$$

□

Remark 27.1.10. The isomorphism $w_\#$ depends on the choice of w. If u is another path from b to b', $u_\#^{-1}w_\#$ is the map $[\ell] \mapsto [u.w^{-1}.\ell.w.u^{-1}]$, which is the operation of conjugation by the element $[w.u^{-1}]$ of $\pi_1(X, b)$. As the fundamental group need not be abelian, this map need not be the identity.

Remark 27.1.11. There is a bijection between unbased loops in X in the component of b to conjugacy classes in $\pi_1(X, b)$. Let $\ell : S^1 \to X$.

Pick an abitrary path from b to $\ell(1)$. Then the loop $w.\ell.w^{-1}$ is a loop in X based at b. Applying a homotopy to ℓ does not change the homotopy class relative to ∂I of this loop.

Changing the choice to path w would alter this element by a conjugacy. In particular, we obtain a well-defined conjugacy class in $\pi(X, b)$ from any homotopy class of loop in X.

TODO: Show correspondence, have only shown well-definedness

Proposition 27.1.12. *Let (X, x) and (Y, y) be spaces with basepoints. Then, any continuous map $f : (X, x) \to (Y, y)$ induces a homomorphism $f_* : \pi_1(X, x) \to \pi_1(Y, y)$. Further, we have*

1. $(\mathrm{id}_X)_* = \mathrm{id}_{\pi_1(X,x)}$
2. *if $g : (Y, y) \to (Z, z)$ is some map, $(gf)_* = g_*f_*$*
3. *if $f \simeq f'$ relative to $\{x\}$, then $f_* = f'_*$.*

Proof. Define $f_*([\ell]) = [f \circ \ell]$. Note this is well-defined by the version of Lemma 25.1.6 on homotopies relative to ∂I. Also, $f \circ (\ell.\ell') = (f \circ \ell).(f \circ \ell')$, thus f_* is a homomorphism.

The first two claims are straightforward, and the final one is a consequence of Lemma 25.1.6 for homotopies relative to a subspace (noting that $\ell(\partial I) \subseteq \{x\}$).

□

Proposition 27.1.13. *Let X and Y be path-connected spaces such that $X \simeq Y$. Then $\pi_1(X) \simeq \pi_1(Y)$.*

Proof. Let $f : X \to Y$ and $g : Y \to X$ be homotopy equivalences.

Choose $x_0 \in X$ and let $y_0 \in f(x_0)$ and $x_1 = g(y_0)$, such that we have induced homomorphisms

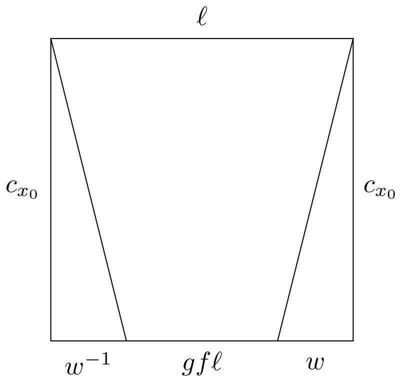
$$\pi_1(X, x_0) \xrightarrow{f_*} \pi_1(Y, y_0) \xrightarrow{g_*} \pi_1(X, x_1)$$

Let H be the homotopy between gf and id_X. Then $w(t) = H(x_0, t)$ is a path from x_1 to x_0. Let ℓ be a loop in X based at x_0 and consider $K = H \circ (\ell \times \mathrm{id}_I) : I \times I \to X$.

We then rescale K to the trapezoid with maps that are constant on the first variable. This gives a homotopy relative to ∂I between $w^{-1}.(g \circ f \circ \ell).w$ and ℓ.

Thus, we have $w_\# g_* f_*[\ell] = [\ell]$. In particular, $w_\# g_* f_* = \mathrm{id}_{\pi_1(X,x_0)}$. In particular, f_* is injective, and as $w_\#$ is an isomorphism, g_* is surjective. By composing the other way around, we see that g_* is injective, and in particular an isomorphism.

Consequently, if X is a contractible space, $\pi_1(X)$ is the trivial group.



□

Definition 27.1.14. *A space is **simply-connected** if it is path-connected and has trivial fundamental group.*

Note that it need not be the case that simply-connected spaces are contractible. A counterexample is the 2-sphere.

27.2 Seifert Van Kampen

Theorem 27.2.1 (Seifert Van Kampen)**.** *Let K be a space which is a union of two path-connected open sets K_1 and K_2, where $K_1 \cap K_2$ is also path-connected. Let b be a point in $K_1 \cap K_2$ and let $\iota_i : K_1 \cap K_2 \to K_1$ and $\iota_2 : K_1 \cap K_2 \to K_2$ be the inclusion maps. Then $\pi_1(K, b)$ is isomorphic to the push-out of*

$$\pi_1(K_1, b) \overset{\iota_{1*}}{\leftarrow} \pi_1(K_1 \cap K_2, b) \overset{\iota_{2*}}{\rightarrow} \pi_1(K_2, b)$$

Moreover, the homomorphisms $\pi_1(K_1, b) \to \pi_1(K, b)$ and $\pi_1(K_2, b) \to \pi_1(K, b)$ which are the composition of the canonical homomorphisms to the pushout and the isomorphism to $\pi_1(K, b)$, are the maps induced by inclusion.

Explicitly, if $\langle X_1 \mid R_1 \rangle$ and $\langle X_2 \mid R_2 \rangle$ are presentations for $\pi_1(K_1, b)$ and $\pi_1(K_2, b)$ with $X_1 \cap X_2 = \emptyset$, then a presentation of $\pi_1(K, b)$ is given by

$$\langle X_1 \cup X_2 \mid R_1 \cup R_2 \cup \{\iota_{1*}(g) = \iota_{2*}(g) \mid g \in \pi_1(X_1 \cap X_2, b)\}\rangle$$

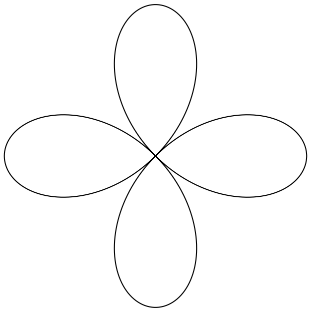
Moreover, the homomorphism $\langle X_i \mid R_i \rangle \to \pi_1(K, b)$ arising from the inclusion of generators $X_i \to X_1 \cup X_2$ is the map induced by the inclusion $K_i \to K$.

Proof. □

Definition 27.2.2. *The **wedge** $(X, x) \vee (Y, y)$ of two spaces with basepoints is the quotient of the disjoint union $X \sqcup Y$ with the identification $x \sim y$. It's basepoint is the image of x and y in the quotient.*

Example 27.2.3. By picking an arbitrary basepoint b in S^1 and wedging n copies of S^1, b together, we obtain the space $\bigvee^n S^1$ which is known as the **bouquet of circles**. For instance, the case with

$n = 4$ is the following:



Corollary 27.2.4. *the fundamental group of $\bigvee^n S^1$ is isomorphic to the free group on n generators.*

Proof. We apply induction on n. For the case $n = 1$, we have $\pi_1(S^1) \cong \mathbb{Z}$. For the inductive case, suppose that $\pi_1(\bigvee^{n-1} S^1)$ is the free group on $n-1$ generators. Let b be the vertex of this wedge, which we take to be the basepoint. Let N be a small open neighborhood of b. Decompose $\bigvee^n S^1$ as $K_1 = N \cup \bigvee^{n-1} S^1$ and $K_2 = N \cup S^1$. Then $\bigvee^{n-1} S^1$ is a homotopy retract of K_1 and S^1 is a homotopy retract of K_2. The intersection $K_1 \cap K_2$ is N, which is clearly contractible. So by Seifert Van Kampen, $\pi_1(\bigvee^n S^1)$ has a presentation with n generators and no relations. □

Theorem 27.2.5. *Let K be a connected cell complex, and let $\ell_i : S^1 \to K^1$ be the attaching maps of its 2-cells, where $1 \leq i \leq n$. Let b be a basepoint in K^0. Let $[\ell_i]$ be the conjugacy class of the loop ℓ_i in $\pi_1(K^1, b)$. Then $\pi_1(K, b)$ is isomorphic to $\pi_1(K^1, b)/\langle\langle[\ell_1], \ldots, [\ell_n]\rangle\rangle$.*

Theorem 27.2.6. *Let K be a connected cell complex, and let $\ell_i : S^1 \to K^1$ be the attaching maps of its 2-cells, where $1 \leq i \leq n$. Let b be a basepoint in K^0. Let $[\ell_i]$ be the conjugacy class of the loop ℓ_i in $\pi_1(K^1, b)$. Then*

$$\pi_1(K^1, b)/\langle\langle[\ell_1], \ldots, [\ell_n]\rangle\rangle \simeq \pi_1(K, b)$$

As $\pi_1(K^1, b)$ is free, then this also gives a presentation for $\pi_1(K, b)$.

Proof. Note first that ℓ_i need not be based at b, but give well-defined conjugacy classes. Picking out representatives ℓ_i' for $[\ell_i]$, we can write

$$\pi_1(K^1, b)/\langle\langle \ell_1', \ldots, \ell_n'\rangle\rangle \simeq \pi_1(K, b)$$

We split the space into open sets $K_1 = \{z \in D^n \mid |z| < \frac{2}{3}\}$ and $K_2 = \{z \in D^n \mid |z| > \frac{1}{3}\} \sqcup X/\sim$. Then, K_1 is homeomorphic to an open n-ball, and $K_1 \cap K_2$ is homeomorphic to $S^{n-1} \times (\frac{1}{3}, \frac{2}{3})$, which is homotopy equivalent to S^{n-1}. K_2 is homotopy eqiuvalent to X by homotopy retraction. We apply Seifert Van Kampen. When $n > 2$, $\pi_1(K_1 \cap K_2)$ and $\pi_1(K_1)$ are both trivial, so the attaching map has no effect on the fundamental group. When $n = 2$, $\pi_1(K_1 \cap K_2) \simeq \mathbb{Z}$ and $\pi_1(K_1)$ is trivial, so this has an effect of adding a relation to $\pi_1(X)$ that represents the loop $[f]$ (by construction). □

Corollary 27.2.7. *Any finitely presented group can be realised as the fundamental group of a finite connected cell-complex. Moreover, this may be given a triangulation.*

Proof. Given $\langle x_1, \ldots, x_m \mid r_1, \ldots, r_n\rangle$, take $K^0 = *$, $K^1 = \bigvee_m S^1$. Give a triangulation on this by splitting the circle into three 1-simplices. Then $\pi_1(K^1)$ is afree group on m generators. Attach 2-cells along the words r_i, then by the previous theorem, this gives the required fundamental group. We note that 2-cells have a canonical simplicial structure, which gives the whole space a triangulation. □

Corollary 27.2.8. *The following are equivalent for a group G*

- *G is finitely presented*
- *G is isomorphic to the fundamental group of a finite simplicial complex*
- *G is isomorphic to the fundamental group of a finite cell complex*

Proof. $(i) \Rightarrow (ii)$ is from above. Note that any finite simplicial complex is a finite cell complex, so $(ii) \Rightarrow (iii)$. Finally, we note that attaching maps of $n > 2$ have no effect on the fundamental group, so in particular from Theorem 27.2.6 is finitely presented. □

27.3 Classification of Fundamental Groups

27.3.1 Fundamental Group of Simplicial Complexes

Definition 27.3.1. *Let α be an edge path. An* ***elementary contraction*** *of α is an edge path obtained from α by performing one of the following :*

1. *removing a_i given $a_{i-1} = a_i$*
2. *replacing a_{i-1}, a_i, a_{i+1} with a_{i-1} given $a_{i-1} = a_{i+1}$*
3. *replacing a_{i-1}, a_i, a_{i+1} with a_{i-1}, a_{i+1} provided $\{a_{i-1}, a_i, a_{i+1}\}$ span a 2-simplex of K.*

α is an elementary expansion of β if β is an elementary expansion of α. We write $\alpha \sim \beta$ if we can pass from α to β. This gives an equivalence relation on edge paths.

Theorem 27.3.2. *Let K be a simplicial complex, and let b be a vertex of K. The equivalence classes of edge loops in K based at b form a group denoted $E(K, b)$, called the edge-loop group.*

Proof. The product is induced by the product of edge loops. This respects the equivalence relation. It is associative because the product of edge loops is associative. The identity is the equivalence class of (b). The inverse of $(b, b_1, \ldots, b_{n-1}, b)$ is $(b, b_{n-1}, \ldots, b_1, b)$. □

Theorem 27.3.3. *For a simplicial complex K and vertex b, $E(K, b)$ is isomorphic to $\pi_1(|K|, b)$.*

Proof. Let $I_{(n)}$ be the triangulation of I with n 1-simplices each of length $\frac{1}{n}$. We can regard an edge path of length n as a simplicial map $I_{(n)} \to K$. This gives a mapping

$$\{\text{edge loops in } K \text{ based at } b\} \xrightarrow{\theta} \{\text{loops in } |K| \text{ based at } b\}$$

If α is obtained from β by an elementary contraction, $\theta(\alpha)$ and $\theta(\beta)$ are homotopic relative to ∂I. Thus, θ gives a well-defined mapping from $E(K, b) \to \pi_1(|K|, b)$. It remains to show that is is an isomorphism.

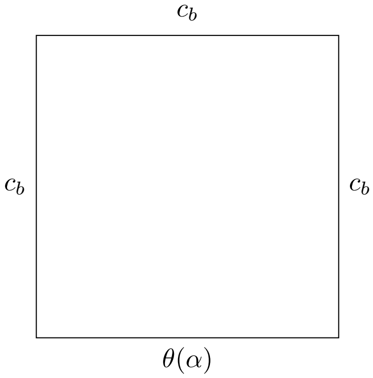
For edge loops α and β, we have $\theta(\alpha.\beta) \simeq \theta(\alpha).\theta(\beta)$, this is a homomorphism.

Surjectivity: Let $\ell : I \to |K|$ be any loop in $|K|$ based at b. Give I the triangulation $I_{(1)}$ and view $I_{(n)}$ as the subdivision. The coarseness of $I_{(n)}$ is $4/r$, which tends to 0 as $n \to \infty$, so by the Simplicial Approximation Theorem (Variant 1), there is a simplicial map $\alpha : I_{(n)} \to K$ for some n such that $\ell \simeq \theta(\alpha) = |\alpha|$ relative to ∂I. In particular, $\theta([\alpha]) = [\ell]$.

Injectivity: Let $\alpha = (b_0, \ldots, b_n)$ be an edge loop based at b. Suppose that $\theta([\alpha])$ is the identity in $\pi_1(|K|, b)$. Then $\theta(\alpha) \simeq c_b$ relative to ∂I via some homotopy $H : I \times I \to |K|$. Triangulate $I \times I$

using the triangulation $(I \times I)_{(r)}$. By The Simplicial Approximation Theorem, for a sufficiently large r, we have a simplicial map $G : (I \times I)_{(r)} \to K$ with $G \simeq H$.

By Proposition 25.2.10, we can ensure that G sends $\partial I \times I$ and $I \times \{1\}$ to b.



Using the same Proposition, when r is a multiple of n, we can ensure that $G(i/n, 0) = b_i$, sending the 1-simplices between $(i/n, 0)$ and $((i+1)/2, 0)$ to (b_i, b_{i+1}). Thus, the restriction of G to $I \times \{0\}$ is an edge path which contracts to α.

We can apply a sequence of elementary contractions and expansion that take this edge path to the edge path where every vertex is b. This is equivalent to (b). In particular, $[\alpha]$ is the identity element of $E(K, b)$ (as the map preserves fundamental groups).

□

Definition 27.3.4. *For any simplicial complex and non-negative integer n, define the **n-skeleton** of K, denoted* $\text{skel}^n(K)$ *is the subcomplex of K consisting of simplices with dimension at most n.*

Corollary 27.3.5. *For any simplicial complex K and vertex b, $\pi_1(|K|, b)$ is isomorphic to $\pi_1(|\text{skel}^2(K)|, b)$.*

Proof. $E(K, b)$ involves only simplices of dimension at most 2, and $E(K, b) \simeq \pi_1(|K|, b)$, □

Corollary 27.3.6. *For $n \geq 2$, $\pi_1(S^n)$ is trivial.*

Proof. Impose a triangulation on S^n, coming from the n-skeleton of Δ^{n+1}. Then S^n and Δ^{n+1} have the same 2-skeleton. But Δ^{n+1} is contractible, so has trivial fundamental group, so does S^n. □

27.3.2 Fundamental Group of the Circle

We view S^1 here as a circle in $\mathbb{C}$, taking $1 \in S^1$ to be the basepoint.

Theorem 27.3.7. *$\pi_1(S^1) \simeq \mathbb{Z}$.*

Proof. Impose a triangulation K on S^1 using three vertices and three 1-simplices. We aim to show that $E(K, 1)$ is isomorphic to $\mathbb{Z}$.

Consider a simplicial loop $\alpha = (b_0, \ldots, b_n)$ based at 1. If $b_i = b_{i+1}$ for some i, then we may preform some elementary contraction. If the loop traverses a 1-simplex and then in reverse, we may also perform an elementary contraction. Thus, a shortest loop equivalent to α traverses all the simplices with the same orientation. It is therefore equivalence to ℓ^n for some $n \in \mathbb{Z}$.

Define the winding number to be the time a simplicial path traverses the (1,2) simplex minus the times it traverses it in the backwards direction. Then, the winding number of ℓ^n is n, and any elementary contraction or expansion leaves the winding number unchanged.

Thus, we can set up a bijection $E(K, 1) \to \mathbb{Z}$ based on its winding number. This is an isomorphism, since $\ell^n.\ell^m = \ell^{n+m}$. □

Theorem 27.3.8 (Fundamental Theorem of Algebra)**.** *Any non-constant polynomial with complex coefficients has at least one root in $\mathbb{C}$.*

Proof. let $p(x) = a_n x^n + \cdots + a_0$ be a polynomial where $a_n \neq 0$ and $n > 0$. Let $C_r = \{x \in \mathbb{C} \mid |x| < r\}$. Let $k = p(r)/r^n$ and $q(x) = kx^n$. Then $p(r) = q(r)$.

We claim that if r is sufficiently large, then $p|_{C_r}$ and $q|_{C_r}$ and the straight-line homotopy all miss 0. If not, then for some $x \in C_r$ and some $t \in [0,1]$,

$$(1-t)p(x) + tq(x) = 0$$

Equivalently,

$$(1-t)(a_n x^n + \cdots + a_0) + t(\frac{a_n|x|^n + \cdots + a_0}{|x|^n})x^n = 0$$

rearranging,

$$a_n x^n + \cdots + a_0 = t(a_{n-1}x^{n-1} + \cdots + a_0 - a_{n-1}\frac{x^n}{|x|} - \cdots - a_0\frac{x^n}{|x|^n})$$

The left side has order x^n, whereas the right is at most x^{n-1}. Hence as $|x| \to \infty$, $|t| \to \infty$. In particular, given r sufficiently large, there is no solution in the range $t \in [0,1]$.

So $p|_{C_r}$ and $q|_{C_r}$ are homotopic relative to $\{r\}$. Suppose that p has no root in $\mathbb{C}$. Then we have a commutative diagram

$$\begin{tikzcd}
\mathbb{C} \arrow[r, "p"] & \mathbb{C} - \{0\} \\
C_r \arrow[u, "\iota"] \arrow[ur, swap, "p|_{C_r}"] &
\end{tikzcd}$$

This induces a function between fundamental groups

$$\begin{tikzcd}
0 = \pi_1(\mathbb{C}, r) \arrow[r, "p_*"] & \mathbb{Z} \simeq \pi_1(\mathbb{C} - \{0\}, r) \\
\mathbb{Z} \simeq \pi_1(C_r, r) \arrow[u, "\iota_*"] \arrow[ur, swap, "(p|_{C_r})_*"] &
\end{tikzcd}$$

In particular, $(p|_{C_r})_*$ is the 0-homomorphism. But $(p|_{C_r})_* = (q|_{C_r})_*$, which sends a generator of $\pi_1(C_r)$ to n times the generator of $\pi_1(\mathbb{C} \setminus \{0\})$, which is a contradiction. □

27.3.3 Fundamental Group of a Graph

Theorem 27.3.9. *The fundamental group of a connected graph is a free group.*

Proof. Let T be a maximal tree in Γ, which exists by Lemma 23.2.5. Let b be a vertex of Γ, which we take as the baespoint. For any vertex $v \in \Gamma$, let $\theta(v)$ be the unique embedded edge path from b to v in T. This exists as $V(T) = V(\Gamma)$ by Lemma 23.2.4. Set $E(\Gamma)$ and $E(T)$ to be the edges of Γ and T respectively. Assign an orientation to each edge $e \in E(\Gamma) \setminus E(T)$, taking $\iota(e), \pi(e)$ to be its initial and terminal vertices. We claim that the elements $\{\theta(\iota(e)).e.\theta(\pi(e))^{-1} \mid e \in E(\Gamma) \setminus E(T)\}$ form a free generating set for $\pi_1(\Gamma, b)$. □

28 Covering Spaces

28.1 Basic Definitions

Definition 28.1.1. *A continuous map $p : \tilde{X} \to X$ is a **covering map** if X and $\tilde{X}$ are non-empty path connected spaces, and given any $x \in X$, there exists some open set U_x containing x such that $p^{-1}(U_x)$ is a disjoint union of open sets V_j such that $p|_{V_j} : V_j \to U_x$ is a homeomorphism for some indexing set J. The open sets U_x are are called **elementary open sets**. $\tilde{X}$ is a **covering space** of X.*

*If we give basepoints $\tilde{b}$ and b such that $p(\tilde{b}) = b$, then $p : (\tilde{X}, \tilde{b}) \to (X, b)$ is a **based covering map**.*

Example 28.1.2. There is a covering map $p : \mathbb{R} \to S^1$ with $t \mapsto \exp(2\pi i t)$.

Given $x \in S^1$, take U_x to be the open semi-circle with x as its midpoint. For instance, $p^{-1}(U_1) = \bigcup_{n\in\mathbb{Z}}(n - \frac{1}{4}, n + \frac{1}{4})$.

Example 28.1.3. For any nonzero integer n, the map $S^1 \to S^1$ by $z \mapsto z^n$ is also covering.

Example 28.1.4. Let $\mathbb{R}P^n$ be the set of 1-dimensional subspaces of $\mathbb{R}^{n+1}$. Define $p : S^n \to \mathbb{R}P^n$ to be the map that sends a point $y \in S^n$ to the 1-dimensional subspace through y.

For each point $x \in \mathbb{R}P^n$, $p^{-1}(x)$ is two points. Take the quotient topology induced by p. Then, taking U_x sufficiently small, $p^{-1}(U_x)$ is two copies of U_x, and the restriction gives a homeomorphism onto U_x. Thus, p is a covering map.

Proposition 28.1.5. *Let $p : \tilde{X} \to X$ be a covering map. Then,*

1. *p is an open mapping*
2. *for $x_1, x_2 \in X$, $p^{-1}(x_1), p^{-1}(x_2)$ have the same cardinality on J*
3. *p is surjective*
4. *p is a quotient map*

Proof. (i) Let U be an open set in $\tilde{X}$. For any $y \in U$, we wish to find an open set $p(y)$ contained in $p(U)$. Let V_j be the copy of $U_{p(y)}$ in $p^{-1}(U_{p(y)})$ that contains y. As the restriction of p to V_j is a homeomorphism, $p(V_j \cap U)$ is open in X. This is an open set containing $p(y)$ in $p(U)$.

(ii) The cardinality of $p^{-1}(x)$ is locally constant on $\tilde{X}$. As $\tilde{X}$ is connected, it must be globally constant

(iii) As $\tilde{X}$ is nonempty, $p^{-1}(x)$ is nonempty for some $x \in X$. As the cardinality is constant, $p^{-1}(x)$ is nonempty for any $x \in X$, thus p is surjective.

(iv) A surjective open mapping is a quotient map. □

Definition 28.1.6. *The **degree** of a covering map $p : \tilde{X} \to X$ is the cardinality of $p^{-1}(x)$ for any $x \in X$.*

Definition 28.1.7. *If $p : \tilde{X} \to X$ is a covering map and $f : Y \to X$ is a map, then a **lift** of f is a map $\tilde{f} : Y \to \tilde{X}$ such that $p\tilde{f} = f$. Equivalently, the following diagram commutes:*

$$\begin{tikzcd}
 & \tilde{X} \arrow[d, "p"] \\
Y \arrow[ur, "\tilde{f}"] \arrow[r, "f"'] & X
\end{tikzcd}$$

Example 28.1.8. Given a covering map $p : \mathbb{R} \to S^1$ from before, the map $f : I \to S^1$ sending $t \mapsto \exp(2\pi i t)$ lifts to $\tilde{f} : I \to \mathbb{R}$, where $\tilde{f}(t) = t$.

Conversely, the identity map from $S^1 \to S^1$ does not lift, as if a lift $\tilde{f} : S^1 \to \mathbb{R}$ existed, then by commutativity, $\tilde{f}(1) = n$ for some $n \in \mathbb{Z}$. This induces a commutative diagram,

$$\begin{tikzcd}
& \pi_1(\mathbb{R}, n) \arrow[d, "p_*"] \\
\pi_1(S^1, 1) \arrow[ur, "\tilde{f}_*"] \arrow[r, "\mathrm{id}"'] & \pi_1(S^1, 1)
\end{tikzcd}$$

which is impossible, as $\pi_1(\mathbb{R})$ is trivial, whereas $\pi_1(S^1)$ is nontrivial.

Theorem 28.1.9 (Uniqueness of lifts)**.** *Let $p : \tilde{X} \to X$ be a covering map, and let $f : Y \to X$ be a map, where Y is connected. Suppose that g and h are lifts of f and that $g(y_0) = h(y_0)$ for some $y_0 \in Y$. Then $g = h$.*

Proof. Let $C = \{y \in Y \mid g(y) = h(y)\}$. By $y_0 \in C$, C is nonempty. We show that C is closed and open, and as Y is connected, it is the entirety of Y.

As p is a covering map, there is an elementary open set $U_{f(y)}$ containing $f(y)$ for any $y \in Y$, and open sets V_1, V_2 in $\tilde{X}$ such that $p|_{V_1}$ and $p|_{V_2}$ are homeomorphisms from V_1 and V_2 to $U_{f(y)}$ and $g(y) \in V_1$, $h(y) \in V_2$.

Now let $y \in Y - C$. Then $V_1 \cap V_2 = \emptyset$. Thus, $g^{-1}(V_1) \cap h^{-1}(V_2)$ is contained in $Y - C$. This is an open set containing y, so $Y - C$ is open.

Suppose that $y \in C$. Then $V_1 = V_2$. Taking $g^{-1}(V_1) \cap h^{-1}(V_2)$, we have $p \circ g = p \circ h$. As $p|_{V_1}$ is an injection, $g = h$ on this set. Thus it is in C. This is an open set containing y, so C is open. □

Theorem 28.1.10 (Path Lifting)**.** *Let $p : \tilde{X} \to X$ be a covering map. Let $\alpha : I \to X$ be a path with $\alpha(0) = x$. Given $\tilde{x} \in p^{-1}(x)$, α has a lift $\tilde{\alpha} : I \to \tilde{X}$ such that $\tilde{\alpha}(0) = \tilde{x}$.*

Proof. Let $A = \{t \in I \mid$ there exists a lift of $\alpha|_{[0,t]}$ starting at $\tilde{x}\}$. A is nonempty, as it contains 0. Take T to be the supremum of A. Pick an elementary open set $U_{\alpha(T)}$ around $\alpha(T)$.

Pick an $\epsilon > 0$ such that $(T - \epsilon, T + \epsilon) \cap [0, 1]$ is mapping into $U_{\alpha(T)}$ by α. Let $t = \max\{0, T - \frac{\epsilon}{2}\}$. Let $\tilde{\alpha} : [0, t] \to \tilde{X}$ be a lift of $\alpha|_{[0,t]}$ starting at $\tilde{x}$.

Let V_j be the copy of $U_{\alpha(T)}$ in $p^{-1}(U_{\alpha(T)})$ that contains $\tilde{\alpha}(t)$. The homeomorphism $U_{\alpha(T)} \cong V_j$ specifies a way of extending $\tilde{\alpha}$ to a lift of $\alpha|_{[0,T+\epsilon]\cap[0,1]}$. This implies $T = 1$. Hence A is all of I, and thus $\tilde{\alpha}$ has been defined on all $[0, 1]$. □

Theorem 28.1.11 (Homotopy Lifting)**.** *Let $p : \tilde{X} \to X$ be a covering map. Let Y be a space, and let $H : Y \times I \to X$ be a map. If h is a lift of $H_{Y\times\{0\}}$, then H has a unique lift $\tilde{H} : Y \times I \to \tilde{X}$ such that $\tilde{H}|_{Y\times\{0\}} = h$.*

Proof. TODO!! Omitted for revision sake □

Remark 28.1.12. When $Y = \{*\}$, then it always exists by Path lifting.

Corollary 28.1.13. *If $p : (\tilde{X}, \tilde{b}) \to (X, b)$ is a based covering map, then $p_* : \pi_1(\tilde{X}, \tilde{b}) \to \pi_1(X, b)$ is an injection.*

Proof. Let ℓ be a loop in $\tilde{X}$ based at $\tilde{b}$. Then $p \circ \ell$ is a loop in X based at b. Suppose that $p_*[\ell] = [p \circ \ell]$ is trivial in $\pi_1(X, b)$, and let $H : I \times I \to X$ be the homotopy relative to ∂I between

$p \circ \ell$ and c_b. Now ℓ is a lift of $H|_{I\times\{0\}}$. Thus by Homotopy Lifting, there is a lift $\tilde{H} : I \times I \to \tilde{X}$ of H such that $\tilde{H}|_{I\times\{0\}} = \ell$.

Now, $\tilde{H}_{\{0\}\times I}, \tilde{H}_{\{1\}\times I}, \tilde{H}_{I\times\{1\}}$ are all constant maps, as the lift of a constant map is constant, as $p^{-1}(b)$ is discrete, and continuous functions map path-connected sets to path-connected sets. Thus, they must all be $\tilde{b}$, as this is where ℓ sends ∂I. In particular, $\tilde{H}$ is a homotopy relative to ∂I between ℓ and $c_{\tilde{b}}$. Thus $[\ell]$ is trivial in $\pi_1(X, b)$, giving p_* to be an injection. □

Remark 28.1.14. Fix a based covering map $p : (\tilde{X}, \tilde{b}) \to (X, b)$. If two loops ℓ and ℓ' based at b are homotopic relative to ∂I, they can be lifted to paths $\tilde{\ell}$ and $\tilde{\ell}'$ starting at $\tilde{b}$. By the previous corollary, they are homotopic relative to ∂I.

Thus, $\tilde{\ell}(1) = \tilde{\ell}'(1)$

Definition 28.1.15. *Noting the above remark, define a function*

$$\pi_1(X, b) \overset{\lambda}{\to} p^{-1}(b)$$

by $[\ell] \mapsto \tilde{\ell}(1)$.

Proposition 28.1.16. *Fix a based covering map* $p : (\tilde{X}, \tilde{b}) \to (X, b)$. *Given elements* g_1, g_2 *of* $\pi_1(X, b)$, $\lambda(g_1) = \lambda(g_2)$ *if and only if* g_1 *and* g_2 *belong to the same right coset of* $p_*\pi_1(\tilde{X}, \tilde{b})$. *This induces a bijection between right cosets of* $p_*\pi_1(\tilde{X}, \tilde{b})$ *and points of* $p^{-1}(b)$.

$$\begin{tikzcd}
\tilde{X} \arrow[d, "p"] & p^{-1}(b) \arrow[l, hook', "\supseteq"'] \arrow[d, Leftrightarrow] & \pi_1(\tilde{X}, \tilde{b}) \arrow[d, "p_*"] \\
X & \textit{right cosets of } p_*(\pi_1(\tilde{X}, \tilde{b})) & \pi_1(X, b) \arrow[ul, dashed, "\lambda"]
\end{tikzcd}$$

Proof. Let ℓ_1 and ℓ_2 be loops based at b such that $[\ell_i] = g_i$. Suppose that $\tilde{\ell}_1(1) = \tilde{\ell}_2(1)$. Then $\tilde{\ell}_1 \cdot \tilde{\ell}_2^{-1}$ is a loop based at $\tilde{b}$. The map p sends this to $\ell_1\dot{\ell}_2^{-1}$, so

$$[\ell_1][\ell_2]^{-1} = p_*[\tilde{\ell}_1\tilde{\dot{\ell}}_2^{-1}] \in p_*\pi_1(\tilde{X}, \tilde{b})$$

Thus g_1 and g_2 belong to the same right coset of $p_*\pi_1(\tilde{X}, \tilde{(b)})$.

Conversely, suppose that $[\ell_1]$ and $[\ell_2]$ belong to the same right coset of $p_*\pi_1(\tilde{X}, \tilde{b})$ such that $[\ell_1][\ell_2]^{-1} \in p_*\pi_1(\tilde{X}, \tilde{b})$. Then $\ell_1\dot{\ell}_2^{-1}$ is homotopic relative to ∂I to $p \circ \ell$ for some loop ℓ in $\tilde{X}$ based at $\tilde{b}$. This homotopy lifts to a homotopy relative to ∂I between ℓ and a lift of $\ell_1\dot{\ell}_2^{-1}$. Thus, $\ell_1\dot{\ell}_2^{-1}$ lifts to a loop based at $\tilde{b}$. The lift is $\tilde{e}ll_1.\tilde{\ell}_2^{-1}$. Thus $\tilde{\ell}_1(1) = \tilde{\ell}_2(1)$. □

Corollary 28.1.17. *A loop* ℓ *in* X *based at* b *lifts to a loop based at* $\tilde{b}$ *if and only if* $[\ell] \in p_*\pi_1(\tilde{X}, \tilde{b})$.

Proof. ℓ lifts to a loop based at $\tilde{b}$ if and only if $\lambda[\ell] = \tilde{b}$, but *tildeb* corresponds to the identity coset of $p_*\pi_1(\tilde{X}, \tilde{b})$, in particular $[\ell] \in p_*\pi_1(\tilde{X}, \tilde{b})$. □

Remark 28.1.18. When $p_*\pi_1(\tilde{X}, \tilde{b})$ is a normal subgroup of $\pi_1(X, b)$, the right cosets form a group in which we can quotient by, and is bijective with $p^{-1}(b)$. To see the group structure from the quotient, consider the following. Let $\tilde{\ell}_1$ and $\tilde{\ell}_2$ be paths from $\tilde{b}$ to b_1 and b_2 respectively. Then $\ell_1 = p \circ \tilde{\ell}_1$ and $\ell_2 = p \circ \tilde{\ell}_2$ are loops in X based at b such that $\lambda([\ell_i]) = b_i$. To compute $\lambda([\ell_1].[\ell_2])$, lift $\ell_1.\ell_2$ to a path based at b, and then $b_1.b_2$ is the endpoint. Alternatively, take the lift of ℓ_2 that starts at b_1.

Definition 28.1.19. *When $\tilde{X}$ is simply connected, a based covering map $p : (\tilde{X}, \tilde{b}) \to (X, b)$ is known as the* ***universal cover*** *of X.*

Remark 28.1.20. In this case, $p^{-1}(b)$ is bijective with $\pi_1(X, b)$, as $\pi_1(\tilde{X}, \tilde{b}) = \{1\}$.

Corollary 28.1.21. *The fundamental group of a circle is isomorphic to $\mathbb{Z}$.*

Proof. We give a uniersal cover $\mathbb{R} \to S^1$ in the usual sense, and then this bijectively corresponds to $p^{-1}(1) = \mathbb{Z}$. Using the procedure above, this gives an isomorphism $\pi_1(S^1, 1) = \mathbb{Z}$. □

Remark 28.1.22. The above proof works for any $\prod S^1$ by taking the universal cover $\mathbb{R}^n$.

28.2 Uniqueness of Coverings

Definition 28.2.1. *A space Y is* ***locally path-connected*** *if for each point y of Y and each neighborhood V of y, there is an open neighborhood of y contained in V that is path-connected.*

Example 28.2.2. Any 2-manifold is locally path-connected. In particular, simplicial complex is locally path-connected.

Theorem 28.2.3 (Existence of Lifts). *Let $p : (\tilde{X}, \tilde{b}) \to (X, b)$ be a based covering map. Let Y be a path-connected, locally path-connected space and let $f : (Y, y_0) \to (X, b)$ be some map. Then f has a lift $\tilde{f} : (Y, y_0) \to (\tilde{X}, \tilde{b})$ if and only if $f_* \pi_1(Y, y_0) \subseteq p_* \pi_1(\tilde{X}, \tilde{b})$.*

Definition 28.2.4. *Two based covering spaces $p : (\tilde{X}, \tilde{b}) \to (X, b)$ and $p' : (\tilde{X}', \tilde{b}') \to (X, b)$ are* ***equivalent*** *if there is a homeomorphism f such that the following commutes:*

$$\begin{tikzcd}
(\tilde{X}, \tilde{b}) \arrow[rr, "f"] \arrow[dr, "p"'] & & (\tilde{X}', \tilde{b}') \arrow[dl, "p'"] \\
& (X, b) &
\end{tikzcd}$$

Theorem 28.2.5 (Uniqueness of Covering Spaces). *Let X be a path-connected, locally path-connected space, and let b be a basepoint in X. Then for any subgroup H of $\pi_1(X, b)$, there is at most one based covering space $p : (\tilde{X}, \tilde{b}) \to (X, b)$ up to equivalence such that $p_* \pi_1(\tilde{X}, \tilde{b}) = H$.*

Proof. Let $p' : (\tilde{X}', \tilde{b}') \to (X, b)$ be another another covering such that $p'_* \pi_1(\tilde{X}', \tilde{b}') = H$. Then by Theorem 28.2.3, p' admits a lift $\tilde{p}' : (\tilde{X}', \tilde{b}') \to (\tilde{X}, \tilde{b})$, and similarly for p, such that the following commutes:

$$\begin{tikzcd}
(\tilde{X}', \tilde{b}') \arrow[r, "\tilde{p}'"] \arrow[dr, "p'"'] & (\tilde{X}, \tilde{b}) \arrow[r, "\tilde{p}"] \arrow[d, "p"'] & (\tilde{X}', \tilde{b}') \arrow[dl, "p'"] \\
& (X, b) &
\end{tikzcd}$$

By uniqueness of lifts (as the basepoints agree), $\tilde{p}' \tilde{p} = \mathrm{id}_{\tilde{X}}$, thus $\tilde{p}'$ is a homeomorphism, and so the coverings are equivalent. □

Theorem 28.2.6. *Let K be a path-connected simplicial complex, and let b be a vertex of K. Then for any subgroup H of $\pi_1(K, b)$ there is a based covering $p : (\tilde{K}, \tilde{b}) \to (K, b)$ such that $p_* \pi_1(\tilde{K}, \tilde{b}) = H$. Moreover, $\tilde{K}$ is a simplicial complex and p is a simplicial map.*

Corollary 28.2.7. *Let K be a path-connected simplicial complex, and let b be a vertex of K. Then there is precisely one based covering space up to equivalence for each subgroup of $\pi_1(K, b)$.*

Theorem 28.2.8 (Nielsen-Schreier)**.** *Any subgroup of a finitely generated free group is free.*

Proof. Let F be the free group on n generators. Let X be the wedge of n circles, and let b be the central vertex. Then $\pi_1(X, b) \simeq F$. Taking any subgroup H of F, there is a based covering map $p : (\tilde{X}, \tilde{b}) \to (X, b)$ such that $p_*\pi_1(\tilde{X}, \tilde{b}) = H$. As p_* is injective, so $\pi_1(\tilde{X}, \tilde{b}) \simeq H$. By Theorem 28.2.6, $\tilde{X}$ is a simplicial complex and p is a simplcial map. As p is a local homeomorphism, $\tilde{X}$ can contain only zero and one dimensional simplices. Hence $\tilde{X}$ is a graph, thus has free fundamental group. □

Remark 28.2.9. To construct the free generating set given a graph, take a maximal tree and use those.

Remark 28.2.10. Lift exists iff image of lift is in image of covering map (as a fundamental group) (so if there is a lift, it is a subgroup)

Theorem 28.2.11. *Let G be a finitely generated group and let H be a finite index subgroup. Then H is finitely presented.*

Definition 28.2.12. *Let $p : \tilde{X} \to X$ be a covering map. Then a* ***covering transformation*** *is a homeomorphism $t : \tilde{X} \to \tilde{X}$ such that the following commutes:*

$$\begin{tikzcd}
\tilde{X} \arrow[rr, "t"] \arrow[dr, "p"'] & & \tilde{X} \arrow[dl, "p"] \\
& X &
\end{tikzcd}$$

Definition 28.2.13. *A covering map $p : (\tilde{X}, \tilde{b})$ is* ***regular*** *if any two points of $p^{-1}b$ differ by a covering transformation.*

Theorem 28.2.14. *Let $p : (\tilde{X}, \tilde{b}) \to (X, b)$ be a regular covering map. Then $p_*\pi_1(\tilde{X}, \tilde{b})$ is a normal subgroup of $\pi_1(X, b)$.*

Proof. Sketch, lifting $\alpha \in \pi_1(X, b)$ takes you to a point $\tilde{\alpha}(1)$. Use regularity to transform ℓ to $t\ell$, moving from a loop based at $\tilde{b}$ to $\tilde{\alpha}(1)$. □

Theorem 28.2.15. *Let $p : (\tilde{X}, \tilde{b}) \to (X, b)$ be a covering map, where X is locally path-connected. Suppose that $p_*\pi_1(\tilde{X}, \tilde{b})$ is a normal subgroup of $\pi_1(X, b)$. Then p is regular.*

Proof. Sketch, use normality, transform path based at $\tilde{b}'$ to $\tilde{b}$, use subset argument to generate lift, uniqueness of lifts to argue $tt' = \text{id}$. □

29 Notes

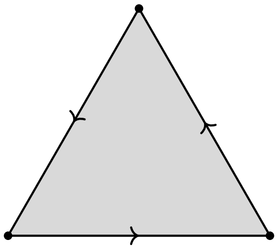
29.0.1 Cell attaching

We can view the attaching map as a pushout square:

$$\begin{tikzcd}
S^{n-1} \arrow[r, "f"] \arrow[d] & X \arrow[d] \\
D^n \arrow[r] & X \cup_f D^n
\end{tikzcd}$$

When the attaching maps are homotopic, we can 'slide' along the attaching map on $\Phi : X \cup_f D^n \to X \cup_g D^n$ which is constant on X and the interior of the disk, and on the boundary, uses the homotopy H to carry the gluing f continuously over to the gluing g.

Example 29.0.1. The dunce-hat is contractible.



The attaching map onto the single loop 1-skeleton is homotopic to the identity on S^1, so the resulting space is homotopic to D^2, which is contractible.

29.0.2 Aside on Contractible Spaces

Proposition 29.0.2. *Let X be contractible and Y be any space. Then,*

- *X is path-connected*
- *$X \times Y \simeq Y$*
- *Any $f, g : Y \to X$ are homotopic*
- *If Y is path connected, any two maps $X \to Y$ are homotopic*

Proof. By contractibility, picking any basepoint $x_0 \in X$, we have a homotopy $H : X \times I \to X$ with $H(x, 0) = x$ and $H(x, 1) = x_0$. Then for any x, the path $\gamma(t) = H(x, t)$ runs from x to x_0. This proves (i).

The projector $p_Y : X \times Y \to Y$ is a deformation with homotopy

$$(x, y) \mapsto (H(x, t), y)$$

which in $t = 1$ collapses X to a single x_0. This shows (ii)

Consider the function $K_f : Y \times I \to X$ with $K_f(y, t) = H(f(y), t)$. This gives a homotopy $f \simeq c_{x_0}$. By considering K_g and with transitivity of homotopy, we have $f \simeq g$.

The important part about mapso from contractible domains is that it essentially only depends on a point it contracts to. That is, given $f, g : Y \to X$, build homotopies

$$f_t(x) = f(H(x, t))$$

such that at $t = 0$, we have $f_0(x) = f(x)$ and at $t = 1$, we have $f_1(0) = f(x_0)$. In particular, $f \simeq c_{f(x_0)}$, and similarly for g. Finally, we connect the two constant paths via the homotopy that path connects $f(x_0)$ and $g(x_0)$, as Y is path connected. □

29.0.3 Aside on higher-dimensional balls

We specifically consider functions about S^n and their behavior with antipodal points.

Proposition 29.0.3. *The antimpodal map $\alpha : S^n \to S^n$ where $\alpha(x) = -x$ is homotopic to id_{S^n} when n is odd.*

Proof. When $n = 2k+1$ for some integer k, we note that

$$S^{2k+1} \subseteq \mathbb{R}^{2k+2} = \underbrace{\mathbb{R}^2 \otimes \cdots \otimes \mathbb{R}^2}_{k+1 \text{ copies}}$$

Now we can view a point on $x \in S^{2k+1}$ as $(x_1, \ldots, x_{k+1})$ where $x_i \in \mathbb{R}^2$. Then we give explicit homotopy

$$\begin{aligned} &H(x,0) = (x_1, \ldots, x_{k+1}) = x \\ &H(x,1) = (R_\pi(x_1), \ldots, R_\pi(x_{k+1})) = (-x_1, \ldots, -x_{k+1}) = -x \end{aligned}$$

where R_θ is the rotation in the plane by angle θ. Thus H is a homotopy id $\simeq \alpha$ □

Proposition 29.0.4. *If $f, g : X \to S^n$ never hit antipodes, they are homotopic. That is,*

$$f(x) \neq -g(x)$$

for all $x \in X$.

Proof. We consider the straightline homotopy in $\mathbb{R}^{n+1}$, and then normalize it back to the sphere, as they never pass through the origin. Thus, we take

$$H(x,t) = \frac{(1-t)f(x) + tg(x)}{||(1-t)f(x) + tg(x)||}$$

□

29.0.4 Homotopic Equivalent Spaces

Proposition 29.0.5. *The following are homotopy equivalent :*

1. $S^1 \vee S^1$
2. $S^1 \times S^1$ *with one point removed*
3. $\mathbb{R}^2$ *minus two distinct points*

Proof. $(i) \simeq (ii)$ is straightforward, by considering the cell complex of the torus, and noting that removing a point acts as removing the 2-cell.

$(i) \simeq (iii)$ by noting that removing two distinct points on $\mathbb{R}^2$ gives exactly the structure we expect from $S^1 \vee S^1$ up to retraction.

□

29.1 Additonal Properties about Spaces

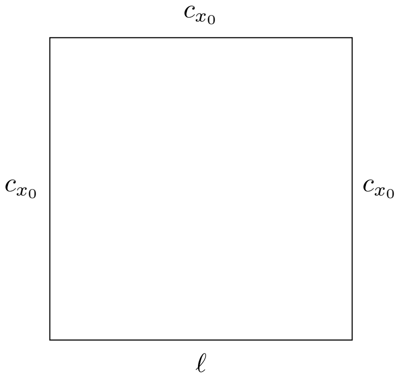
Proposition 29.1.1. *For any space X, the following conditions are equivalent:*

- *Every map $S^1 \to X$ is homotopic to a constant map*
- *Every map $S^1 \to X$ extends to a map $D^2 \to X$*
- $\pi_1(X, x_0) = 0$ *for all $x_0 \in X$.*

Proof. $(i) \Rightarrow (ii)$ Let $f : S^1 \to X$ be null-homotopic, such that $H : S^1 \times I \to X$ is the homotopy that takes f to c_x for some $x \in X$. Now note that $S^1 \times I$ is homeomorphic to the Annulus $\{w \in \mathbb{C} \mid 1 \leq |w| \leq 2\}$. The boundary components come from $S^1 \times \{0\}$ and $S^1 \times \{1\}$, which under H is sent to f and c_x respectively. Noting that $D^2 = (S^1 \times [0,1])/(S^1 \times \{1\})$, we see the natural extension that sends elements on the outside boundary to x.

$(ii) \Rightarrow (i)$ If $f : S^1 \to X$ extends to a $\tilde{f} : D^2 \to X$, then precomposing with the deformation $\rho : D^2 \to \{0\} \subseteq D^2$, gives a homotopy from f to the constant map at $\tilde{f}(0)$. Explicitly, we take the retraction $R : D^2 \times [0,1] \to D^2$ with $R(x,0) = x$ and $R(x,1) = 0$. Then, we construct a homotopy $H : S^1 \times [0,1] \to X$ with $H(z,t) = \tilde{f}(R(z,t))$.

$(ii) \Leftrightarrow (iii)$ If a loop $S^1 \to X$ extends to a map $D^2 \to X$, then this is null homotopic. This follows from the fact we have the square



which is homotopic to the disk. Thus extendable implies every loop is trivial in $\pi_1(X)$. In the other direction, we use the exact same argument in reverse to go from the square to the disk for an extension. □

Proposition 29.1.2. *The fundamental group of a product splits. That is, given (X, x_0) and (Y, y_0) be based spaces,*

$$\pi_1(X \times Y, (x_0, y_0)) = \pi_1(X, x_0) \times \pi_1(Y, y_0)$$

Proof. We give an explicit group isomorphism $\phi : \pi_1(X, x_0) \times \pi_1(Y, y_0)$ by

$$\phi([\ell_1], [\ell_2]) = [t \mapsto (\ell_1(t), \ell_2(t))]$$

This is well-defined (concatenation of loops in factors goes to concatenation in the product). It is injective by considering projections to X and Y, and is surjective as homotopies in the product are exactly the pairs of homotopies in each factor. □

Corollary 29.1.3. *The torus has fundamental group $\mathbb{Z}^2$.*

Proof. Immediate, noting that $\pi_1(S^1 \times S^1) = \pi_1(S^1) \times \pi_1(S^1) = \mathbb{Z} \times \mathbb{Z}$. □

Definition 29.1.4. *A **retraction** of a space X onto a subspace A is a map $r : X \to A$ such that $ri = \mathrm{id}_A$ where $i : A \to X$ is the inclusion map.*

Example 29.1.5. There is no retraction map $r : D^2 \to S^1$.

We note the induced map from S^1 to D^2 then S^1 looks on the fundamental group looks like

$$\mathbb{Z} \xrightarrow{i_*} 0 \xrightarrow{r_*} \mathbb{Z}$$

But the composition is clearly not the identity.

Thus, every $f : D^2 \to D^2$ has a fixed point. If for every $x \in D^2$ we have $f(x) \neq x$, then we can draw a ray from $f(x)$ to x and define the map r to be the assignment of x to the point the ray hits on S^1. This is a continuous retraction, but no such retraction exists.

Proposition 29.1.6. *Given $n > 2$, none of* $\mathbb{R}$*,* $\mathbb{R}^2$*,* $\mathbb{R}^n$ *are homeomorphic.*

Proof. $\mathbb{R}$ is not homeomorphic to neither of these, as removing a point makes $\mathbb{R}$ disconnected but not the others. For the case $\mathbb{R}^2$ and $\mathbb{R}^n$, we note that removing a point from both gives S^1 and S^{n-1}, which have different fundamental groups, so are not homeomorphic. □

Proposition 29.1.7. *S^2 is not homeomorphic to S^n for any $n \neq 2$.*

Proof. Use the fact S^n minus two points is homotopic to S^{n-1}. □

Proposition 29.1.8. *There is no retraction of the Möbius band onto its boundary.*

Proof. Sketch: take the induced maps on fundamental groups, and note that the inclusion sends to $2\mathbb{Z}$. □

Remark 29.1.9. Considering the Torus obtained by side identifications of a square, we can consider the cell decomposition, such that removing a single disk about the center of the square is homotopic to $S^1 \vee S^1$. Reading back, the generators spell $xyx^{-1}y^{-1}$ on the generating set of $\pi_1(X, b)$.

Example 29.1.10. Let S be the two-holed torus. We obtain this via X, who is $S^1 \times S^1$ minus a disc D. Then we have

$$S = X_1 \cup_{\partial D} X_2$$

where $X_1 \cap X_2 \simeq S^1$.

obtained by taking two copies of the torus, cutting them out about a disc and identifying them. We will show that $\pi_1(S)$ is an amalgamated free product.

Then by Seifert Van Kampen, the fundamental group is simply

$$\langle x_1, y_1, x_2, y_2 \mid x_1 y_1 x_1^{-1} y_1^{-1} = x_2 y_2 x_2^{-1} y_2^{-1} \rangle$$

And is an amalgamated free product induced by $X_1 \cup N *_N X_2 \cup N$, where N is a slight-extension of X_1 and X_2 who is homeomorphic to $S^1 \times (0, 1)$.

Example 29.1.11. Some examples of simply connected covering spaces:

- If we consider the square with side identifications which is homeomorphic to the Möbius band, the universal cover is the bundle of these over the real line in an infinite strip, with $\tilde{M} \simeq \mathbb{R} \times I$
- The wedge $S^2 \vee S^1$ has fundamental group $\mathbb{Z}$, its universal cover is an infinite string along $\mathbb{R}$ where we have a copy of S^2 along each integer $n \in \mathbb{Z}$
- The punctured plane $\mathbb{R}^2\{\text{pt}\}$ has universal cover $\tilde{U} = \mathbb{R}^2$ with covering map $p(u, v) = (e^u \cos v, e^u \sin v)$ (which comes from the mapping $z \mapsto e^z$).