Galois Theory Notes

Made by Leon :) *Note: Any reference numbers are to the lecture notes*

1 Galois Groups

Definition 1.1.1: Conjugate Numbers

Two complex numbers z and z' are **conjugate over** $\mathbb{Q}$ *(exact same def. for* $\mathbb{R}$ *but we usually use* $\mathbb{Q}$*)* iff either $z = z'$ or $\overline{z} = z'$. Alternatively, if for all polynomials p with coefficients in $\mathbb{Q}$,

$$p(z) = 0 \iff p(z') = 0$$

$(z_1, \dots, z_k)$, and $(z_1', \dots, z_k')$ k-tuples in $\mathbb{C}$ are **conjugate over** $\mathbb{Q}$ if for all polynomials $p(t_1, \dots, z_k)$ over $\mathbb{Q}$ in k variables,

$$p(z_1, \dots, z_k) = 0 \iff p(z_1', \dots, z_k') = 0$$

Additionally, if $(z_1, \dots, z_n)$ conjugate to $(z_1', \dots, z_n')$, then z_i is conjugate to z_i' for all i

2 Groups, Rings, and Fields

Definition 2.1.1: Group Action

Let G be a group and X a set. An **action** of G on X is a function $G \times X \to X$, written as $(g, x) \mapsto gx$ such that

$$(gh)x = g(hx) \text{ and } 1x = x$$

for all $g, h \in G$ and $x \in X$, where 1 is the identity of G

Definition 2.1.7: Faithful Actions

An action of a group G on a set X is **faithful** if for $g, h \in G$,

$$gx = hx \text{ for all } x \in X \implies g = h$$

"If two elements of the group do the same, they are the same."

Lemma 2.1.8: Properties of Faithful Actions

For an action of a group G on a set X, the following are equal:

1. The action is faithful
2. For $g \in G$, if $gx = x$ for all $x \in X$ then $g = 1$
3. The homomorphism $\Sigma : G \to \mathrm{Sym}(X)$ is injective
4. $\ker \Sigma$ is trivial.

Lemma 2.1.11: Isomorphisms of Faithful Groups

Let G be a group acting faithfully on a set X. then G is isomorphic to the subgroup of $\mathrm{Sym}(X)$, where $\Sigma : G \to \mathrm{Sym}(X)$

$$\operatorname{im} \Sigma = \{\overline{g} \mid g \in G\}, \text{ where } \overline{g} : X \to X \text{ and } \overline{g}(x) = gx$$

Definition 2.1.1: Fixed Set

For a group G acting on a set X, let $S \subseteq G$. The **fixed set** of S is

$$\mathrm{Fix}(S) = \{x \in X \mid sx = x \text{ for all } s \in S\}$$

Lemma 2.1.15: Normal Fixed Sets

Let G be a group acting on a set X, let $S \subseteq G$, and let $g \in G$. Then $\mathrm{Fix}(gSg^{-1}) = g\,\mathrm{Fix}(S)$.

Here, $gSg^{-1} = \{gsg^{-1} \mid s \in S\}$ and $g\,\mathrm{Fix}(S) = \{gx \mid x \in \mathrm{Fix}(S)\}$

Definition 2.2.1: Ring Homomorphism

Given rings R and S, a **homomorphism** from R to S is a function $\phi : R \to S$ satisfying the following equations for all $r, r' \in R$:

- $\phi(r + r') = \phi(r) + \phi(r')$
- $\phi(0) = 0$, $\phi(1) = 1$
- $\phi(rr') = \phi(r)\phi(r')$
- $\phi(-r) = -\phi(r)$

A **subring** of a ring R is a subset $S \subseteq R$ that contains 0 and 1 and is closed under addition, multiplication, and negatives. When S is a subring of R, the inclusion $\iota : S \to R$ is a homomorphism.

Lemma 2.2.3: Intersection of Subrings

Let R be a ring and let $\mathcal{S}$ be any set (perhaps infinite) of subrings of R. Then their intersection $\bigcap_{S \in \mathcal{S}} S$ is also a subring of R.

Recall 2.0.1: Ideals and Quotient Rings

Let R be a ring. $I \subseteq R$ is an **ideal**, $I \trianglelefteq R$, if the following hold:

1. $I \neq \emptyset$
2. I is closed under subtraction
3. for all $i \in I$ and $r \in R$ we have $ri, ir \in I$

Every ring homomorphism $\phi : R \to S$ has an image $\operatorname{im} \phi$, which is a subring of S, and a kernel $\ker \phi$, which is an ideal of R.

Given an ideal $I \trianglelefteq R$, define the quotient ring R/I and canonical homomorphism $\pi_I : R \to R/I$ which is surjective and has kernel I.

Universal Property of Factor Rings: Given a ring S and any homomorphism $\phi : R \to S$ satisfying $\ker \phi \supseteq I$, there is exactly one homomorphism $\overline{\phi} : R/I \to S$ s.t. this diagram commutes.

$$\begin{tikzcd} R \arrow[d, "\pi_I"'] \arrow[dr, "\phi"] & \\ R/I \arrow[r, "\overline{\phi}"'] & S \end{tikzcd}$$

Recall 2.0.2: Integral Domains and Generators

An **integral domain** is a ring R s.t. $0_R \neq 1_R$, and for $r, r' \in R$,

$$rr' = 0 \implies r = 0 \text{ or } r' = 0.$$

Generated Ideals

Let Y be a subset of a ring R. The **ideal** $\langle Y \rangle$ **generated by** Y is defined as the intersection of all the ideals of R containing Y.

- **Principal ideals** are ideals of the form $\langle r \rangle$. A **principle ideal domain** is an integral domain where every ideal is principal.
- Let r and s be elements of a ring R. r **divides** s, or $r \mid s$, if $\exists a \in R$ s.t. $s = ar$. This is equivalent to $s \in \langle r \rangle$, and $\langle s \rangle \supseteq \langle r \rangle$.
- An element $u \in R$ is a **unit** if it has a multiplicative inverse, i.e. if $\langle u \rangle = R$. The units form a group $R^\times$ under multiplication.
- Elements r and s of a ring are **coprime** if for $a \in R$,

$$a \mid r \text{ and } a \mid s \implies a \text{ is a unit}$$

2.2.11) For a ring R and a finite subset $Y = \{r_1, \dots, r_n\}$. Then

$$\langle Y \rangle = \{a_1 r_1 + \dots + a_n r_n : a_1, \dots, a_n \in R\}$$

2.2.16) Let R be a principal ideal domain and $r, s \in R$. Then

$$r \text{ and } s \text{ are coprime} \iff ar + bs = 1 \text{ for some } a, b \in R$$

Recall 2.3.A: Fields, Fieldeals, and Subfields

A **field** is a ring K in which $0 \neq 1$ and every nonzero element is a unit. Equivalently, it is a ring such that $K^\times = K \backslash \{0\}$. Every field is an integral domain. A field K has exactly two ideals: $\{0\}$ and K. A **subfield** of a field K is a subring that is a field

Example 2.3.2: Rational Expressions

Let K be a field. A **rational expression** over K is a ratio of two polynomials

$$f(t)/g(t)$$

where $f(t), g(t) \in K[t]$ with $g \neq 0$[a]. Two such expressions, f_1/g_1 and f_2/g_2 are regarded as equal if $f_1 g_2 = f_2 g_1$ in $K[t]$. i.e. equivalence class. The set of rational expressions over K is called $K(t)$

[a] Note that these are **not** functions, e.g. $1/(t-1)$ is a valid element of $K(t)$, and you don't need to worry about $t = 1$.

Definition 2.3.7: Equaliser

For sets X and Y, and $S \subseteq \{$ functions $X \to Y\}$, the **equalizer** of S is *"the part of X where all the functions in S are equal"*, i.e.

$$\mathrm{Eq}(S) = \{x \in X \mid f(x) = g(x) \text{ for all } f, g \in S\}$$

Lemma 2.3.B: Ring Homomorphism Properties

2.3.3) Every (ring) homomorphism between fields is injective.

2.3.6) Let $\phi : K \to L$ be a homomorphism between fields.
1. For a subfield K' of K, the image $\phi K'$ is a subfield of L
2. For a subfield L' of L, the preimage $\phi^{-1} L'$ is a subfield of K

2.3.8) Let K and L be fields, and let

$$S \subseteq \{\text{homomorphisms } K \to L\}$$

Then $\mathrm{Eq}(S)$ is a subfield of K.

Recall 2.3.9: Characteristic

For a ring R, there is a unique homomorphism $\chi : \mathbb{Z} \to R$ whose kernel is an ideal of the PID $\mathbb{Z}$. Hence $\ker \chi = \langle n \rangle$ for a unique integer $n \geq 0$. n is the **characteristic** of R (char R). So for $m \in \mathbb{Z}$, we have that $m \cdot 1_R = 0$ iff m is a multiple of char R. Or:

$$\operatorname{char} R = \begin{cases} \text{the least } n > 0 \text{ s.t. } n \cdot 1_R = 0_R, & \text{if such an } n \text{ exists} \\ 0 & \text{otherwise} \end{cases}$$

2.3.11) The characteristic of an integral domain is 0 or prime.

2.3.12) Let $\phi : K \to L$ be a homomorphism of fields. Then $\operatorname{char} K = \operatorname{char} L$.

Recall 2.3.C: Prime Subfield

The **prime subfield** of K is the intersection of all the subfields of K. Concretely, the prime subfield of K is

$$\left\{ \frac{m \cdot 1_K}{n \cdot 1_K} \mid m, n \in \mathbb{Z} \text{ with } n \cdot 1_K \neq 0 \right\}$$

Lemma 2.3.16

Let K be a field.

- If char $K = 0$ then the prime subfield of K is (iso to) $\mathbb{Q}$.
- If char $K = p > 0$ then the prime subfield of K is (iso to) $\mathbb{F}_p$

Lemma 2.3.17: Every finite field has positive characteristic.

Proposition 2.3.19: The Frobenius Map

Lemma 2.3.19: Let p be a prime and $0 < i < p$. Then $p \mid \binom{p}{i}$

Let p be a prime number and R a ring of characteristic p. Let the **Frobenius Map** be the homomorphism $\theta : R \to R \quad r \mapsto r^p$.

1. The Frobenius map is a homomorphism.
2. If R is a field then θ is injective.
3. If R is a finite field then θ is an automorphism of R. In this case we call θ the **Frobenius Automorphism**

Corollary 2.3.22: Roots by Characteristic

Let p be a prime number, and K be a field with characteristic p.

1. Every element in K has *at most* one pth root.
2. If K is a finite field, every element has *exactly* one pth root.

Recall 2.3.D: Reducible Elements

An element r of a ring R is **irreducible** if r is not 0 or a unit, and if for $a, b \in R$.

$$r = ab \implies a \text{ or } b \text{ is an unit}$$

For example, the irreducibles in $\mathbb{Z}$ are $\pm 2, \pm 3, \pm 5, \dots$. An element of a ring is **reducible** if it is not 0, a unit, or irreducible.

Warning: The 0 and units of a ring are neither reducible nor irreducible, in much the same way that the integers 0 and 1 are neither prime nor composite.

Proposition 2.3.26

Let R be a principal ideal domain and $0 \neq r \in R$. Then

$$r \text{ is irreducible} \iff R/\langle r \rangle \text{ is a field}$$

This lets us construct fields from irreducible elements of a PID.

3 Polynomials

Definition 3.1.1: Polynomial Ring

Let R be a ring. A **polynomial over** R is an infinite sequence $(a_0, a_1, a_2, \dots)$ of elements of R s.t. $\{i \mid a_i \neq 0\}$ is finite.

The set of polynomials over R, written $R[t]$, forms a ring:

$$(a_0, a_1, \dots) + (b_0, b_1, \dots) = (a_0 + b_0, a_1 + b_1, \dots),$$
$$(a_0, a_1, \dots) \cdot (b_0, b_1, \dots) = (c_0, c_1, \dots),$$
$$\text{where } c_k = \sum_{i,j : i+j=k} a_i b_j$$

Polynomials are typically written as f or $f(t)$ interchangeably. A polynomial $f = (a_0, a_1, \dots)$ over R gives rise to a function

$$R \to R, \quad r \mapsto a_0 + a_1 r + a_2 r^2 + \cdots.$$

Proposition 3.1.6: Universal Property of the Polyring

Let R, B be rings. For every homomorphism $\phi : R \to B$ and every $b \in B$, there is exactly one homomorphism $\theta : R[t] \to B$ such that

$$\theta(a) = \phi(a) \text{ for all } a \in R \tag{3.4}$$
$$\theta(t) = b \tag{3.5}$$

Definition 3.1.7: Induced Homomorphism

Let $\phi : R \to S$ be a ring homomorphism. We define

$$\phi_* : R[t] \to S[t]$$

as the **induced homomorphism**, which is the unique homomorphism $R[t] \to S[t]$ s.t. $\phi_* = \phi(a)$ for all $a \in R$ and $\phi_*(t) = t$.

Definition 3.1.9: Degree of a Polynomial

The **degree**, $\deg(f)$, of a nonzero polynomial $f(t) = \sum a_i t^i$ is the largest $n \geq 0$ s.t. $a_n \neq 0$. By convention, $\deg(0) = -\infty$, where $-\infty$ is a formal symbol which we give the properties for all $n \in \mathbb{Z}$:

$$-\infty < n, \quad (-\infty) + n = -\infty, \quad (-\infty) + (-\infty) = -\infty$$

Lemma 3.1.11

Let R be an integral domain. Then:

1. $\deg(fg) = \deg(f) + \deg(g)$ for all $f, g \in R[t]$
2. $R[t]$ is an integral domain.

$\deg(-\infty)$ implies the (unique) zero polynomial, $\deg(0)$ implies the nonzero constants, $\deg(> 0)$ implies the nonconstant polynomials.

Lemma 3.1.14

Let K be a field. Then

1. The units in $K[t]$ are the nonzero constants
2. $f \in K[t]$ is irreducible iff f is nonconstant and cannot be expressed as a product of two nonconstant polynomials.

Lemma 3.2.1 - Uniqueness of Poly Division

For a field K and $f, g \in K[t]$ with $g \neq 0$, there is exactly one pair of polynomials $q, r \in K[t]$ s.t. $f = qg + r$ and $\deg(r) < \deg(g)$

Lemma 3.2.A: Facts about Fields

3.2.2) Let K be a field. Then $K[t]$ is a principal ideal domain.

3.2.5) Let K be a field and let $0 \neq f \in K[t]$. Then

$$f \text{ is irreducible} \iff K[t]/\langle f \rangle \text{ is a field.}$$

3.2.6) Let K be a field and let $f(t) \in K[t]$ be a nonconstant polynomial. Then $f(t)$ is divisible by some irreducible in $K[t]$

3.2.7) Let K be a field and $f, g, h \in K[t]$. Suppose that f is irreducible and $f \mid gh$. Then $f \mid g$ or $f \mid h$.

Theorem 3.2.8: Unique Determination of Polys

Let K be a field and $0 \neq f \in K[t]$. Then

$$f = a f_1 f_2 \cdots f_n$$

for some $n \geq 0$, $a \in K$, and monic[a] irreducibles $f_1, \dots, f_n \in K[t]$. Moreover, n and a are uniquely determined by f, and $f_1, \dots, f_n$ are uniquely determind up to reordering.

[a] Monic means that the highest order element has coefficient 1.

Lemma 3.2.9: Root Finding

One way to find an irreducible factor of a polynomial $f(t) \in K[t]$ is to find a **root**. Let K be a field, $f(t) \in K[t]$, and $a \in K$. Then

$$f(a) = 0 \iff (t - a) \mid f(t).$$

Lemma 3.2.10: Algebraically Closed Field

A field is **algebraically closed** if every nonconstant polynomial has at least one root.

Let K be an algebraically closed field and $0 \neq f \in K[t]$. then

$$f(t) = c(t - a_1)^{m_1} \cdots (t - a_k)^{m_k},$$

where c is the leading coefficient of f, and $a_1, \dots, a_k$ are the distinct roots of f in K, and $m_1, \dots, m_k \geq 1$

Lemma 3.3.1: Degrees and Irreducibility

Let K be a field and $f \in K[t]$.

1. If f is constant then f is not irreducible.
2. If $\deg(f) = 1$ then f is irreducible.
3. If $\deg(f) \geq 2$ and f has a root then f is reducible.
4. If $\deg(f) \in \{2, 3\}$ and f has no root then f is irreducible.

Warning: To show a polynomial is irreducible, it's generally *not* enough to show it has no root. The converse of 3 is false!

Definition 3.3.6: Primitive Polynomial

A polynomial over $\mathbb{Z}$ is **primitive** if its coefficients have no common divisor except for ± 1.

Lemma 3.3.7: Existence of Primitives

Let $f(t) \in \mathbb{Q}[t]$. Then there exists a primitive polynomial $F(t) \in \mathbb{Z}[t]$ and $\alpha \in \mathbb{Q}$ such that $f = \alpha F$.

Remark 3.3.A: Irreducibility over

If the coefficients of a polynomial $f(t) \in \mathbb{Q}[t]$ happen to all be integers, the word "irreducible" could mean two things: irreducibility in the ring $\mathbb{Q}[t]$ or in the ring $\mathbb{Z}[t]$. We say that f is irreducible **over** $\mathbb{Q}$ or $\mathbb{Z}$ to distinguish between the two.

Lemma 3.3.B: Irreducibility Tests

Lemma 3.3.8: Gauss' Lemma

1. The product of two primitive polynomials over $\mathbb{Z}$ is primitive.
2. If a nonconstant polynomial over $\mathbb{Z}$ is irreducible over $\mathbb{Z}$, it is irreducible over $\mathbb{Q}$

Lemma 3.3.9: Mod-p Method

Let $f(t) = a_0 + a_1 t + \cdots + a_n t^n \in \mathbb{Z}[t]$. If there is some prime p s.t. $p \nmid a_n$ and $\overline{f} \in \mathbb{F}_p[t]$ is irreducible, then f is irreducible over $\mathbb{Q}$.

Warning: This only tells you that a polynomial is *irreducible* over $\mathbb{Q}$ and says nothing about whether it is *reducible*.

Lemma 3.3.12: Eisenstein's Criterion

Let $f(t) = a_0 + \cdots + a_n t^n \in \mathbb{Z}[t]$, with $n \geq 1$. Suppose there exists a prime p such that

- $p \nmid a_n$
- $p \mid a_i, \forall i \in \{0, \dots, n-1\}$
- $p^2 \nmid a_0$

Then f is irreducible over $\mathbb{Q}$.

4 Field Extensions

Definition 4.1.1: Field Extension

It is sometimes easier to think of a subset as an injection. Given a set A and a subset $B \subseteq A$, define an **inclusion** function

$$\iota : B \to A \text{ defined by } \iota(b) = b \text{ for all } b \in B.$$

Let K be a field. An **extension** of K is a field M together with a homomorphism $\iota : K \to M$. We write $M : K$ to mean that M is an extension of K, not bothering to mention ι.

Example 4.1.2: Examples of Field Extensions

$$\iota_1 : \mathbb{Q} \to \mathbb{R}, \quad \iota_2 : \mathbb{R} \to \mathbb{C}, \quad \iota_3 : \mathbb{Q} \to \mathbb{C}$$

$\iota_4 : Q \to K$, where $K = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ (we call this $\mathbb{Q}(\sqrt{2})$)

Definition 4.1.4: Generated Subfields

For a field K, and X a subset of K, the subfield of K **generated by** X is the intersection of all subfields of K containing X. Let F be the subfield of K generated by X. F contains X, and F is also the *smallest* subfield of K containing X (i.e. any subfield of K containing X contains F)

Definition 4.1.8: Adjoined Subfields

For a field extension $M : K$, and $Y \subseteq M$, we write $K(Y)$ for the subfield of M generated by $K \cup Y$. We call it the subfield of M **generated by** Y **over** K, or K with Y **adjoined**.

$K(Y)$ is the smallest subfield of M containing both K, Y. If Y is a finite set $\{\alpha_1, \dots, \alpha_n\}$, write $K(\{\alpha_1, \dots, \alpha_n\})$ as $K(\alpha_1, \dots, \alpha_n)$

Definition 4.2.1: Algebraic Numbers

A complex number $\alpha \in \mathbb{C}$ is said to be "algebraic" if

$$a_0 + a_1\alpha + \cdots + a_n a^n = 0$$

for some rational numbers a_i, not all zero

Algebraic Numbers for Arbitrary Fields

For a field extension $M : K$, and $\alpha \in M$, α is **algebraic** over K if $\exists f \in K[t]$ s.t. $f(\alpha) = 0$ but $f \neq 0$, **transcendental** otherwise.

Lemma 4.2.6: Annihilators

Let $M : K$ be a field extension and $\alpha \in M$. An **annihilating polynomial** of α is a polynomial $f \in K[t]$ such that $f(\alpha) = 0$. So, α is algebraic iff it has some nonzero annihilating polynomial.

For a field extension $M : K$ and $\alpha \in M$, there is a polynomial $m(t) \in K[t]$ such that

$$\langle m \rangle = \{\text{annihilating polynomials of } \alpha \text{ over } K\}. \tag{4.2}$$

If α is transcendental over K then $m = 0$. If α is algebraic over K then there is a unique monic polynomial m satisfying (4.2).

Definition 4.2.7: Minimal Polynomial

Let $M : K$ be a field extension and let $\alpha \in M$ be *algebraic* over K. The **minimal polynomial** of α is the unique monic polynomial satisfying (4.2). **Warning**: This isn't defined over transcendentals, therefore some elements of M might not have a minimal polynomial.

Lemma 4.2.10: Minimal Polynomial Conditions

Let $M : K$ be a field extension, let $\alpha \in M$ be algebraic over K and let $m \in K[t]$ be a monic polynomial. The following are equivalent:

1. m is the minimal polynomial of α over K
2. $m(\alpha) = 0$, $m \mid f$ for all annihilating polynomials f of α over K
3. $m(\alpha) = 0$ and $\deg(m) \leq \deg(f)$ for all nonzero annihilating polynomials. *"monic annihilating polynomial of least degree."*
4. $m(\alpha) = 0$ and m is irreducible over K.

Definition 4.3.1

Let K be a field.

1. Let $m \in K[t]$ be monic and irreducible. Write $\alpha \in K[t]/\langle m \rangle$ for the image of t under the canonical homomorphism $K[t] \to K[t]/\langle m \rangle$. Then α has minimal polynomial m over K, and $K[t]/\langle m \rangle$ is generated by α over K.
2. The element t of the field $K(t)$ of rational expressions over K is transcendental over K, and $K(t)$ is generated by t over K

Definition 4.3.3: Homomorphism over Fields

For a field K, and let $\iota : K \to M$, $\iota' : K \to M'$ be extensions of K. A homomorphism $\phi : M \to M'$ is called a **homomorphism over** K if the following diagram commutes:

$$\begin{tikzcd} M \arrow[rr, "\phi"] & & M', \\ & K \arrow[ul, "\iota"] \arrow[ur, "\iota'"'] & \end{tikzcd}$$

Lemma 4.3.6: Uniqueness of Field Homomorphisms

Let M and M' be extensions of a field K, and let $\phi, \psi : M \to M'$ be homomorphisms over K. Let Y be a subset of M such that $M = K(Y)$. If $\phi(\alpha) = \psi(\alpha)$ for all $\alpha \in Y$ then $\phi = \psi$.

Proposition 4.3.7: Universal Props of $K[t]/\langle m \rangle$, $K(t)$

Universal Property of $K[t]/\langle m \rangle$

Let K be a field, and:

- $m \in K[t]$ monic and irreducible
- $L : K$ an extension of K
- $\beta \in L$ with minimal polynomial m
- Write α for the image of t under the canonical homomorphism $K[t] \to K[t]/\langle m \rangle$.
- Then there is exactly one homomorphism $\phi : K[t]/\langle m \rangle \to L$ over K such that $\phi(a) = \beta$.

$$\begin{tikzcd} \alpha \arrow[rr, dotted, mapsto] & & \beta \\ K[t]/\langle m \rangle \arrow[rr, dotted, "\phi"] & & L \\ & K \arrow[ul] \arrow[ur] & \end{tikzcd}$$

Universal Property of $K(t)$

For $L : K$ an extension of K, and transcendental $\beta \in L$, there is exactly one homomorphism $\phi : K(t) \to L$ over K s.t. $\phi(t) = \beta$.

Corollary 4.3.11: Isomorphisms and Uniqueness

Let M and M' be extensions of a field K. A homomorphism $\phi : M \to M'$ is an **isomorphism over** K if it is a homomorphism over K and an isomorphism of fields. If such a ϕ exists, we say that M and M' are **isomorphic over** K.

Let K be a field.

1. Let the conditions from 4.3.7 apply, alongside the condition that $L = K(\beta)$. Then there is exactly one isomorphism $\phi : K[t]/\langle m \rangle \to L$ over K such that $\phi(\alpha) = \beta$.
2. Let $L : K$ be an extension of K, and let $\beta \in L$ be transcendental with $L = K(\beta)$. Then there is exactly one isomorphism $\phi : K(t) \to L$ over K such that $\phi(t) = \beta$.

Definition 4.3.13: Simple Extension

A field extension $M : K$ is **simple** if $\exists \alpha \in M$ s.t. $M = K(\alpha)$.

Theorem 4.3.16: Classification of Simple Extensions

Let K be a field.

1. Let $m \in K[t]$ be a monic irreducible polynomial. Then there exists an extension $M : K$ and an algebraic element $\alpha \in M$ such that $M = K(\alpha)$ and α has minimal polynomial m over K. Moreover, if (M, α) and (M', α') are two such pairs, there is exactly one isomorphism $\phi : M \to M'$ over K s.t. $\phi(\alpha) = \alpha'$
2. There exists an extension $M : K$ and a transcendental element $\alpha \in M$ such that $M = K(\alpha)$. Moreover, if (M, α) and (M', α') are two such pairs, there is exactly one isomorphism $\phi : M \to M'$ over K such that $\phi(\alpha) = \alpha'$.

5 Degree

Definition 5.1.1: Degree of a Field Extension

Let $M : K$ be a field extension. Then M can be seen as a vector space over K. When we view M as a vector space over K rather than an extension, we forget how to multiply together elements of M that aren't in K.

The **degree** $[M : K]$ of a field extension $M : K$ is the dimension of M as a vector space over K. If M is an *infinite-dimensional* vector space over K, we write $[M : K] = \infty$, where ∞ is a formal symbol with the properties

$$n < \infty, \quad n \cdot \infty = \infty \; (n \geq 1), \quad \infty \cdot \infty = \infty$$

for integers n. An extension $M : K$ is **finite** if $[M : K] < \infty$.

Warning 5.1.4

The degree $[K : K]$ of K over itself is 1, not 0. Degrees of extensions are never 0.

Theorem 5.1.5: Basis of Field Extensions

Let $K(\alpha) : K$ be a simple extension.

1. Suppose that α is algebraic over K. Write $m \in K[t]$ for the minimal polynomial of α and $n = \deg(m)$. Then
$$1, \alpha, \ldots, \alpha^{n-1}$$
is a basis of $K(\alpha)$ over K. In particular, $[K(\alpha) : K] = \deg(m)$
2. Suppose that α is transcendental over K. Then $1, \alpha, \alpha^2, \ldots$ are linearly independent over K. In particular, $[K(\alpha) : K] = \infty$

Theorem 5.1.17: Tower Law

For field extensions $M : L : K$ and (potentially infinite) sets I, J,

1. If $(\alpha_i)_{i \in I}$ is a basis of L over K and $(\beta_j)_{j \in J}$ is a basis of M over L, then $(\alpha_i \beta_j)_{(i,j) \in I \times J}$ is a basis of M over K.
2. $M : K$ is finite $\iff$ $M : L$ and $L : K$ are finite.
3. $[M : K] = [M : L][L : K]$

A family $(\alpha_i)_{i \in I}$ of elements of a field is **finitely supported** if the set $\{i \in I \mid \alpha_i \neq 0\}$ is finite.

Corollary 5.1.A: Degree Results

Corollary 5.1.10: Degree means Algebraic

Let $M : K$ be a field extension and $\alpha \in M$, the **degree** of α over K is $[K(\alpha) : K]$. We write it as $\deg_K(\alpha)$. Then

$$\deg_K(\alpha) < \infty \iff \alpha \text{ is algebraic over } K.$$

If α is algebraic over K then the degree of α over K is the degree of the minimal polynomial of α over K.

Corollary 5.1.12: Size of Nested Extension

Let $M : L : K$ be a field extension and $\beta \in M$. Then

$$[L(\beta) : L] \leq [K(\beta) : K]$$

Corollary 5.1.14: Polynomial Form of Extensions

Let $M : K$ be an extension and $\alpha_1, \ldots, \alpha_n \in M$, with α_i algebraic over K of degree d_i. Then every element $\alpha \in K(\alpha_1, \ldots, \alpha_n)$ can be expressed as a polynomial in $\alpha_1, \ldots, \alpha_n$ over K. More exactly,

$$\alpha = \sum_{r_1, \ldots, r_n} c_{r_1, \ldots, r_n} a_1^{r_1} \cdots a_n^{r_n}$$

for some $c_{r_1, \ldots, r_n} \in K$, where r_i ranges over $0, \ldots, d_i - 1$.

Corollary 5.1.19: Dividing Extensions

Let $M : L' : L : K$ be field extensions. If $M : K$ is finite, then $[L' : L]$ divides $[M : K]$

Corollary 5.1.21: Triangle Tower Inequality

Let $M : K$ be a field extension and $\alpha_1, \ldots, \alpha_n \in M$. Then

$$[K(\alpha_1, \ldots, \alpha_n) : K] \leq [K(\alpha_1) : K] \cdots [K(\alpha_n) : K].$$

Definition 5.2.1: Finitely Generated Extensions

A field extension $M : K$ is **finitely generated** if $M = K(Y)$ for some finite subset $Y \subseteq M$.

Definition 5.2.2: Algebraic Extension

A field ext. M:K is **algebraic** if all elements of M are algebraic over K

Proposition 5.2.4: Algebraic and Finiteness

The following conditions on a field extension $M : K$ are equivalent:

1. $M : K$ is finite
2. $M : K$ is finitely generated and algebraic
3. $M = K(\alpha_1, \ldots, \alpha_n)$ for some finite set $\{\alpha_1, \ldots, \alpha_n\}$ of elements of M algebraic over K.

Corollary 5.2.6: Variation for Simple Extensions

Let $K(\alpha) : K$ be a simple extension. The following are equivalent:

1. $K(\alpha) : K$ is finite
2. $K(\alpha) : K$ is algebraic
3. α is algebraic over K.

Corollary 5.2.7: $\overline{\mathbb{Q}}$ is a subfield of $\mathbb{C}$.

Def 5.3.3: Ruler and Compass Constructions

A point C in the plane is **immediately constructible** from Σ if it is a point of intersection between lines or circles. C is **constructible** from Σ if there is a finite sequence $C_1, \ldots, C_n = C$ of points such that C_i is immediately constructible from $\Sigma \cup \{C_1, \ldots, C_{i-1}\}$ for each i.

For a subfield $K \subseteq \mathbb{R}$, an extension $K : \mathbb{Q}$ is **iterated quadratic** if there is some finite sequence of subfields

$$\mathbb{Q} = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_n = K$$

such that $[K_i : K_{i-1}] = 2$ for all $i \in \{1, \ldots, n\}$

Let L and L' be subfields of a field M. The **compositum** LL' of L and L' is the subfield of M generated by $L \cup L'$. That is, LL' is the smallest subfield of M containing both L and L'.

Lemma 5.3.B: Ruler and Compass Results

Lemma 5.3.6: For a field extension $M : K$ and L, L' subfields of M containing K, if $[L : K] = 2$ then $[LL' : L'] \in \{1, 2\}$.

Lemma 5.3.8: Let K and L be subfields of $\mathbb{R}$ s.t. the extensions $K : \mathbb{Q}$ and $L : \mathbb{Q}$ are iterated quadratic. Then there is some subfield M of $\mathbb{R}$ s.t. the $M : \mathbb{Q}$ is iterated quadratic and $K, L \subseteq M$.

Proposition 5.3.9: Iterated Quadratics from Points

Let $(x, y) \in \mathbb{R}^2$. If (x, y) is constructable from $\{(0, 0), (1, 0)\}$ then there is an iterated quadratic extension of $\mathbb{Q}$ containing x and y.

Theorem 5.3.10: Quadratics and Constructability

Let $(x, y) \in \mathbb{R}^2$. If (x, y) is constructible from $\{(0, 0), (1, 0)\}$ then x, y are algebraic over $\mathbb{Q}$, and their degrees over $\mathbb{Q}$ are powers of 2.

6 Splitting Fields

Definition 6.1.1: Extending Homomorphism

Let $\iota : K \to M$ and $\iota : K' \to M'$ be field extensions. Let $\psi : K \to K'$ be a homomorphism of fields. A homomorphism $\phi : M \to M'$ **extends** ψ if the square commutes ($\phi \circ \iota = \iota' \circ \psi$).

$$\begin{tikzcd} M \arrow[r, "\phi"] & M' \\ K' \arrow[u, "\iota"] \arrow[r, "\psi"] & K \arrow[u, "\iota'"'] \end{tikzcd}$$

Usually we view K as a subset of M, and K' as a subset of M', with inclusions ι and ι'. In this case, for ϕ to extend ψ means that

$$\pi(a) = \psi(a) \text{ for all } a \in K$$

Lemma 6.1.3: Extending Isomorphisms

Induced Homomorphism 2: Let $M : K$ and $M' : K'$ be field extensions, let $\phi : K \to K'$ be a homomorphism, and let $\phi : M \to M'$ be a homomorphism extending ψ. Let $\alpha \in M$ and $f(t) \in K[t]$. Then

$$f(\alpha) = 0 \iff (\psi_* f)(\phi(\alpha)) = 0.$$

Prop 6.1.6: Extending Isomorphisms

Let $\psi : K \to K'$ be an isomorphism of fields, $K(\alpha) : K$ a simple extension where α has minimal polynomial m over K, and $K'(\alpha') : K'$ a simple extension where α' has minimal polynomial $\psi_* m$ over K'.

Then there is exactly one isomorphism $\phi : K(\alpha) \to K'(\alpha')$ that extends ψ and satisfies $\phi(\alpha) = \alpha'$. *(Dotted arrow: a map whose existence is part of the conclusion.)*

$$\begin{tikzcd} K(\alpha) \arrow[r, dotted, "\phi", "\cong"'] & K'(\alpha') \\ K' \arrow[u] \arrow[r, "\cong", "\psi"'] & K' \arrow[u] \end{tikzcd}$$

Definition 6.2.2: Splitting Polynomial

Let f be a polynomial over a field M. Then f **splits** in M if

$$f(t) = \beta(t - \alpha_1)\cdots(t - a_n)$$

for some $n \neq 0$ and $\beta, \alpha_1, \dots, \alpha_n \in M$. Equivalently, f splits in M if all its irreducible factors in $M[t]$ are linear.

Definition 6.2.6: Splitting Field

Let f be a nonzero polynomial over a field K. A **splitting field** of f over K is an extension M of K such that:

1. f splits in M
2. $M = K(\alpha_1, \dots, \alpha_n)$, where $\alpha_1, \dots, \alpha_n$ are the roots of f in M. *"If L is a subfield of M containing K, and f splits in L, then $L = M$"*

Lemma 6.2.A: Splitting Field Results

Lemma 6.2.10: Let $f \neq 0$ be a polynomial over a field K. Then there exists a splitting field M of f over K s.t. $[M : K] \leq \deg(f)!$.

Prop 6.2.11: Splitting Fields and Isomorphisms

Let $\psi : K \to K'$ be an isomorphism of fields, $0 \neq f \in K[t]$, M be a splitting field of f over K, and M' be a splitting field of $\psi_* f$ over K'. Then

1. There exists an isomorphism $\phi : M \to M'$ extending ψ.
2. There are at most $[M : K]$ such extensions ϕ.

We often use this result when $K' = K$ and $\psi = \mathrm{id}_K$.

Theorem 6.2.13: Isos and Autos of a Splitting Field

Let f be a nonzero polynomial over a field K. Then

1. There exists a splitting field of f over K
2. Any two splitting fields of f are isomorphic over K
3. When M is a splitting field of f over K,

$$\text{num. of automorphisms of } M \text{ over } K \leq [M : K] \leq \deg(f)$$

Lemma 6.2.14: Splitting Fields and Extensions

1. Let $M : S : K$ be field extensions, $0 \neq f \in K[t]$, and $Y \subseteq M$. Suppose that S is the splitting field of f over K. Then $S(Y)$ is the splitting field of f over $K(Y)$
2. Let $f \neq 0$ be a polynomial over a field K, and let L be a subfield of $\mathrm{SF}_K(f)$ containing K (so that $\mathrm{SF}_K(f) : L : K$). Then $\mathrm{SF}_K(f)$ is the splitting field of f over L.

Definition 6.3.1: Galois Group of an Extension

The **Galois Group** $\mathrm{Gal}(M : K)$ of a field extension $M : K$ is the group of automorphisms of M over K, with composition as the group operation. In other words, an element of $\mathrm{Gal}(M : K)$ is an isomorphism $\theta : M \to M$ such that $\theta(a) = a$ for all $a \in K$.

Definition 6.3.5: Galois Group of a Polynomial

Let f be a nonzero polynomial over a field K. The **Galois Group** $\mathrm{Gal}_K(f)$ of f over K is $\mathrm{Gal}(\mathrm{SF}_K(f) : K)$.

$$\text{polynomial} \quad \longmapsto \quad \text{field extension} \quad \longmapsto \quad \text{group}$$

Via Theoreem 6.2.13,

$$|\mathrm{Gal}_K(f)| \leq [\mathrm{SF}_K(f) : 0K] \leq \deg(f)!$$

In particular, $\mathrm{Gal}_K(f)$ is always a finite group.

Lemma 6.3.7: Restriction of Actions on GGs

For a nonzero polynom F over a field K, the action of $\mathrm{Gal}_K(f)$ on $\mathrm{SF}_K(f)$ **restricts** to an action on the set of roots of f in $\mathrm{SF}_K(f)$.

Terminology: Given a group G acting on a set X and a subset $A \subseteq X$, the action **restricts** to A if $ga \in A$, $\forall g \in G$ and $a \in A$.

Lemma 6.3.8: Galois Actions are Faithful

Let f be a nonzero polynomial over a field K. Then the action of $\mathrm{Gal}_K(f)$ on the roots of f is **faithful**.

Definition 6.3.9: Conjugacy for real this time

Let $M : K$ be a field extension, let $k \geq 0$, and let $(\alpha_1, \dots, \alpha_k)$ and $(\alpha_1', \dots, \alpha_k')$ be k-tuples of elements of M. Then $(\alpha_1, \dots, \alpha_k)$ and $(\alpha_1', \dots, \alpha_k')$ are **conjugate** over K if for all $p \in K[t_1, \dots, t_k]$,

$$p(\alpha_1, \dots, \alpha_k) = 0 \iff p(\alpha_1', \dots, \alpha_k') = 0$$

If $k = 1$ we omit the brackets and say α and α' are conjugate.

Remark 6.3.B: What The Galois Group Actually Means

An element of $\mathrm{Gal}_K(f)$ is completely determined by how it permutes the roots of f. So you can view elements of $\mathrm{Gal}_K(f)$ as *being* permutations of the roots. However, not every permutation of the roots belongs to the Galois group. Suppose $f \in K[t]$ has distinct roots $\alpha_1, \dots, \alpha_k$ in its splitting field. For each $\theta \in \mathrm{Gal}_K(f)$ there is a permutation $\sigma_\theta \in S_k$ defined by

$$\theta(\alpha_i) = \alpha_{\sigma_\theta(i)} \qquad \text{for } i \in \{1, \dots, k\}$$

Then $\mathrm{Gal}_K(f)$ is isomorphic to the subgroup $\{\sigma_\theta \mid \theta \in \mathrm{Gal}_K(f)\}$ of S_K. The isomorphism is given by $\theta \mapsto \sigma_\theta$.

Proposition 6.3.10: Permutation Definition of Galois

Let f be a nonzero polynomial over a field K with distinct roots $\alpha_1, \dots, \alpha_k$ in $\mathrm{SF}_k(f)$. Then

$$\{\sigma \in S_k \mid (\alpha_1, \dots, \alpha_k) \text{ and } (\alpha_{\sigma(1)}, \dots, \alpha_{\sigma(k)}) \text{ are conj. over } K\}$$

is a subgroup of S_k isomorphic to $\mathrm{Gal}_K(f)$

Corollary 6.3.12: Galois Groups and Extensions

Let $L : K$ be a field extension and $0 \neq f \in K[t]$. Then $\mathrm{Gal}_L(f)$ is isomorphic to a subgroup of $\mathrm{Gal}_K(f)$.

Corollary 6.3.14: Division of Roots in Galois

Let f be a nonzero polynomial over a field K, with k distinct roots in $\mathrm{SF}_K(f)$. Then $|\mathrm{Gal}_K(f)|$ divides $k!$.

7 Preparation for the Fundamental Theorem

Definition 7.1.1: Normal Extensions

An algebraic field extension $M : K$ is **normal** if for all $\alpha \in M$, the minimal polynomial of α splits in M. We also say M **is normal over** K to mean that $M : K$ is normal.

Lemma 7.1.2

Let $M : K$ be an algebraic extension. Then $M : K$ is normal iff every irreducible polynomial over K either has no roots in M or splits in M. Put another way, normality means that any irreducible polynomial over K with *at least one* root in M has *all* its roots in M.

Thm 7.1.5: Maps

$$\begin{tikzcd}
 & \mathrm{SF}_M(m) \\
M = K(\alpha_1, \dots, \alpha_n) \arrow[r, dotted, "\phi"] & M = K(\alpha_1, \dots, \alpha_n, \epsilon) \arrow[u] \\
K(\delta) \arrow[u] \arrow[r, dotted, "\theta"] & K(\epsilon) \arrow[u] \\
K \arrow[u] \arrow[ur] &
\end{tikzcd}$$

Thm 7.1.5: Splitting and Normality

Let $M : K$ be a field extension. Then

$$M = \mathrm{SF}_K(f) \text{ for some nonzero } f \in K[t]$$
$$\iff M : K \text{ is finite and normal}$$

Corollary 7.1.6

Let $M : L : K$ be field extensions. If $M : K$ is finite and normal then so is $M : L$.

Warning: This does *not* follow that $L : K$ is normal.

Proposition 7.1.9: Conjugacy and Orbits

Let $M : K$ be a finite normal extension and α, $\alpha' \in M$. Then

$$\alpha \text{ and } \alpha' \text{ conjugate over } K \iff \alpha' = \phi(\alpha) \text{ for some } \phi \in \mathrm{Gal}(M : K)$$

Corollary 7.1.11: Transitivity of Actions

Let f be an irreducible polynomial over a field K. Then the action of $\mathrm{Gal}_K(f)$ on the roots of f in $\mathrm{SF}_K(f)$ is transitive, i.e. for all $x, x' \in X$ there exists $g \in G$ such that $gx = x'$

Theorem 7.1.15: Quotients of Normal Extensions

Let $M : L : K$ be field extensions with $M : K$ finite and normal.

1. $L : K$ is a normal extension $\iff \phi L = L$ for all $\phi \in \mathrm{Gal}(M : K)$
2. If $L : K$ is a normal extension then $\mathrm{Gal}(M : L)$ is a normal subgroup of $\mathrm{Gal}(M : K)$ and

$$\frac{\mathrm{Gal}(M : K)}{\mathrm{Gal}(M : L)} \cong \mathrm{Gal}(L : K)$$

Definition 7.2.2: Separable Polynomial

For a polynomial $f(t) \in K[t]$ and a root α of f in some extension M of K, we say that α is a **repeated** root if $(t - a)^2 \mid f(t)$ in $M[t]$.

An irreducible polynomial over a field is **separable** if it has no repeated roots in its splitting field. Equivalently, an irreducible polynomial $f \in K[t]$ is separable if it splits into *distinct* linear factors in $\mathrm{SF}_K(f)$:

$$f(t) = a(t - \alpha_1)\cdots(t - a_n)$$

for some $a \in K$ and *distinct* $\alpha_1, \dots, \alpha_n \in \mathrm{SF}_K(f)$. Put another way, an irreducible f is separable iff it has $\deg(f)$ distinct roots in its splitting field. **Warning**: this only works for *irreducible polynomials*.

Definition 7.2.6: Formal Derivative

For a field K and $f(t) = \sum_{i=0}^{n} i_i t_n^i \in K[t]$, the **formal derivative** of f is

$$(Df)(t) = \sum_{i=1}^{n} i a_i t^{i-1} \in K[t]$$

Lemma 7.2.7: Basic Derivative Rules

Let K be a field. Then

$$D(f + g) = Df + Dg, \quad D(fg) = f \cdot Dg + Df \cdot g, \quad Da = 0$$

for all f, $g \in K[t]$ and $\alpha \in K$.

Lemma 7.2.9: Separability Results

Lemma 7.2.9: Repeated Roots

Let f be a nonzero polynomial over a field K. The following are equivalent:

1. f has a repeated root in $\mathrm{SF}_K(f)$
2. f and Df have a common root in $\mathrm{SF}_K(f)$
3. f and Df have a nonconstant common factor in $K[t]$

Lemma 7.2.10: Inseparability of Zero

Let f be an irreducible polynomial over a field. f is inseparable iff $Df = 0$

Corollary 7.2.11: Separability of Irreducibles

Let K be a field.

1. If $\mathrm{char}\, K = 0$, every irreducible polynomial over K is separable.
2. If $\mathrm{char}\, K = p > 0$, an irreducible polynomial $f \in K[t]$ is inseparable iff

$$f(t) = b_0 + b_1 t^p + \cdots + b_r t^{rp}$$

for some $b_0, \dots, b_r \in K$

i.e. the only irreducible inseparable polynomials are ones in t^p in $\mathrm{char}\, p$.

Definition 7.2.13: Separable Elements

Let $M : K$ be an algebraic extension. An element of M is **separable** over K if its miminal polynomial over K is separable. The extension $M : K$ is **separable** if every element of M is separable over K.

Lemma 7.2.16: Let $M : L : K$ be field extensions, with $M : K$ algebraic. If $M : K$ is separable then so are $M : L$ and $L : K$.

Proposition 7.2.17: Splitting Field Isomorphisms

Let $\phi : K \to K'$ be an isomorphism of fields, let $0 \neq f \in K[t]$, let M be a splitting field of f over K, and let M' be a splitting field of $\phi_* f$ over K'. Suppose that the extension $M' : K'$ is separable. Then there are exactly $[M : K]$ isomorphisms $\phi : M \to M'$ extending ψ.

Theorem 7.2.18: Size of Galois Extensions

$|\mathrm{Gal}(M : K)| = [M : K]$ for every finite normal separable extension $M : K$

Lemma 7.3.1: Fixed Fields

$\mathrm{Aut}(M)$ is the group of automorphisms of a field M, which acts naturally on M. Given $S \subseteq \mathrm{Aut}(M)$, $\mathrm{Fix}(S)$ is the set of elements of M fixed by S.

$\mathrm{Fix}(S)$ is a subfield of M, for any $S \subseteq \mathrm{Aut}(M)$.

Thm 7.3.3: Size of Fixed Field

Let M be a field and H a finite subgroup of $\mathrm{Aut}(M)$. Then $[M : \mathrm{Fix}(H)] \leq |H|$. This is actually an equality.

Fixed Field Normal Extensions

Let $M : K$ be a finite normal extension and H a normal subgroup of $\mathrm{Gal}(M : K)$. Then $\mathrm{Fix}(H)$ is a normal extension of K.

8 The Fundamental Theorem of Galois Theory!

Remark 8.1.A: Intermediate Field

Let $M : K$ be a field extension, with K viewed as a subfield of M. An **intermediate field** of $M : K$ is a subfield of M containing K.

Write

$$\mathscr{F} = \{\text{intermediate fields of } M : K\}$$

For $L \in \mathscr{F}$, we draw diagrams like this:

$$\begin{array}{c} M \\ | \\ L \\ | \\ K \end{array}$$

with the bigger fields *higher up*.

We also write

$$\mathscr{G} = \{\text{subgroups of } \mathrm{Gal}(M : K)\}$$

For $H \in \mathscr{G}$, we draw diagrams like this:

$$\begin{array}{c} I \\ | \\ H \\ | \\ \mathrm{Gal}(M : K) \end{array}$$

with the bigger groups *lower down*.

For $L \in \mathscr{F}$, the group $\mathrm{Gal}(M : K)$ consists of all automorphisms ϕ of M that fix each element of L. Since $K \subseteq L$, any such ϕ certainly fixes each element of K. Hence $\mathrm{Gal}(M : L)$ is a subgroup of $\mathrm{Gal}(M : K)$. this process defines a function

$$\begin{aligned} \mathrm{Gal}(M : -) : \mathscr{F} &\mapsto \mathscr{G} \\ L &\mapsto \mathrm{Gal}(M : L) \end{aligned}$$

In the expression $\mathrm{Gal}(M : -)$, the symbol $-$ should be seen as a blank space into which arguments can be inserted.

In the other direction, for $H \in \mathscr{G}$, the subfield $\mathrm{Fix}(H)$ of M contains K. Indeed $H \subseteq \mathrm{Gal}(M : K)$, and by definition, every element of $\mathrm{Gal}(M : K)$ fixes every element of K, so $\mathrm{Fix}(H) \supseteq K$. Hence $\mathrm{Fix}(H)$ is an intermediate field of $M : K$. This process defines a function

$$\begin{aligned} \mathrm{Fix} : \mathscr{G} &\mapsto \mathscr{F} \\ H &\mapsto \mathrm{Fix}(H) \end{aligned}$$

We have now defined functions

$$\mathscr{F} \underset{\mathrm{Fix}}{\overset{\mathrm{Gal}(M:-)}{\rightleftarrows}} \mathscr{G}$$

Lemma 8.1.2: Ordering of Intermediates

Let $M : K$ be a field extension, and define $\mathscr{F}$ and $\mathscr{G}$ as above.

1. For $L_1, L_2 \in \mathscr{F}$,
$$L_1 \subseteq L_2 \implies \mathrm{Gal}(M : L_1) \supseteq \mathrm{Gal}(M : L_2)$$
For $H_1, H_2 \in \mathscr{G}$,
$$H_1 \subseteq H_2 \implies \mathrm{Fix}(H_1) \supseteq \mathrm{Fix}(H_2)$$
2. For $L \in \mathscr{F}$ and $H \in \mathscr{G}$,
$$L \subseteq \mathrm{Fix}(H) \iff H \supseteq \mathrm{Gal}(M : L)$$
3. For all $L \in \mathscr{F}$, $L \subseteq \mathrm{Fix}(\mathrm{Gal}(M : L))$
For all $H \in \mathscr{G}$, $H \subseteq \mathrm{Gal}(M : \mathrm{Fix}(H))$

$$\begin{array}{ccc} M & & 1 \\ | & & | \\ L_2 & & \mathrm{Gal}(M : L_2) \\ | & & | \\ L_1 & & \mathrm{Gal}(M : L_1) \\ | & & | \\ K & & \mathrm{Gal}(M : K) \end{array}$$

Remark 8.1.B: Galois Correspondence

The functions

$$\mathscr{F} \underset{\mathrm{Fix}}{\overset{\mathrm{Gal}(M:-)}{\rightleftarrows}} \mathscr{G}$$

are called the **Galois correspondence** for $M : K$. This terminology is mostly used in the case where the functions are **mutually inverse**, i.e.

$$L = \mathrm{Fix}(\mathrm{Gal}(M : L)), \quad H = \mathrm{Gal}(M : \mathrm{Fix}(H))$$

for all $L \in \mathscr{F}$ and $H \in \mathscr{G}$. In both cases, the LHS is a subset of the RHS. (But they are not always equal.) If $\mathrm{Gal}(M : -)$ and Fix *are* mutually inverse then they set up a one-to-one correspondence between $\mathscr{F}$ and $\mathscr{G}$.

Thm 8.2.1: The Fundamental Theorem of Galois Theory

Let $M : K$ be a finite normal separable extension. Write

$$\begin{aligned} \mathscr{F} &= \{\text{intermediate fields of } M : K\} \\ \mathscr{G} &= \{\text{subgroups of } \mathrm{Gal}(M : K)\} \end{aligned}$$

1. The functions $\mathscr{F} \underset{\mathrm{Fix}}{\overset{\mathrm{Gal}(M:-)}{\rightleftarrows}} \mathscr{G}$ are mutually inverse.
2. $|\mathrm{Gal}(M : L)| = [M : L]$ for all $L \in \mathscr{F}$ and $[M : \mathrm{Fix}(H)] = |H|$ for all $H \in \mathscr{G}$
3. Let $L \in \mathscr{F}$. Then
L is a normal extension of $K \iff$
$\mathrm{Gal}(M : L)$ is a normal subgroup of $\mathrm{Gal}(M : K)$.
and in that case,
$$\frac{\mathrm{Gal}(M : K)}{\mathrm{Gal}(M : L)} \cong \mathrm{Gal}(L : K)$$

Remark 8.2.3: Useful Results

1. Lemmas 6.3.7 and 6.3.8 say that $\mathrm{Gal}_K(f)$ acts faithfully on the set of roots of f in $\mathrm{SF}_K(f)$. i.e. an element of the Galois group can be understood as a permutation of the roots
2. Corollary 6.3.14 states that $|\mathrm{Gal}_K(f)|$ divides $k!$, where k is the number of distinct foots of f in its splitting field.
3. Let α and β be roots of f in $\mathrm{SF}_K(f)$. Then there is an element of the Galois group mapping α to β iff α and β are conjugate over K (have the same minimal polynomial). This follows from Prop 7.1.9.
4. In particular, when f is irreducible, the action of the Galois group on the roots is transitive (Corollary 7.1.11).

Corollary 8.2.7: Automorphisms with FTGT

Let $M : K$ be a finite normal separable extension. Then for every $\alpha \in M \backslash K$, there is some automorphism ϕ of M over K such that $\phi(\alpha) \neq \alpha$

9 Solvability by Radicals

Definition 9.1.2: Radical Number

Let $\mathbb{Q}^{\mathrm{rad}}$ be the smallest subfield of $\mathbb{C}$ such that for $\alpha \in \mathbb{C}$,

$$\alpha^n \in \mathbb{Q}^{\mathrm{rad}} \text{ for some } n \geq 1 \implies \alpha \in \mathbb{Q}^{\mathrm{rad}}.$$

A complex number is **radical** if it belongs to $\mathbb{Q}^{\mathrm{rad}}$

Definition 9.1.5: Solvability by Radicals

A nonzero polynomial over $\mathbb{Q}$ is **solvable by radicals** if all of its complex roots are radical.

Lemma 9.1.6: Abelian Groups

Lemma 9.1.6: For all $n \geq 1$, the group $\mathrm{Gal}_{\mathbb{Q}}(t^n - 1)$ is abelian.

Lemma 9.1.8: Let K be a field and $n \geq 1$. Suppose that $t^n - 1$ splits in K. Then $\mathrm{Gal}_K(t^n - a)$ is abelian for all $a \in K$.

Definition 9.2.1: Solvable Extension

Roughly, the diagram of solvable polynomials is

$$\text{solvable polynomial} \longmapsto \text{solvable extension} \longmapsto \text{solvable group}$$

In other words, we define "solvable extension" in such a way that

1. If $f \in \mathbb{Q}[t]$ is a polynomial solvable by radicals then $\mathrm{SF}_{\mathbb{Q}}(f) : \mathbb{Q}$ is a solvable extension.
2. If $M : K$ is a solvable extension then $\mathrm{Gal}(M : K)$ is a solvable group. Hence if f is solvable by radicals then $\mathrm{Gal}_{\mathbb{Q}}(f)$ is solvable.

Let $M : K$ be a finite normal separable extension. Then $M : K$ is **solvable** (or M is **solvable over** K) if there exist $r \geq 0$ and intermediate fields

$$K = L_0 \subseteq L_1 \subseteq \cdots \subseteq L_r = M$$

s.t. $L_i : L_{i-1}$ is normal and $\mathrm{Gal}(L_i : L_{i-1})$ is abelian for each $i \in \{1, .., r\}$.

Lemma 9.2.A: Solvable Results

Lemma 9.2.4: Solvable Galois and Extensions

Let $M : K$ be a finite normal separable extension. Then

$$M : K \text{ is solvable} \iff \mathrm{Gal}(M : K) \text{ is solvable}$$

Lemma 9.2.6: Finite Normal Results

Let $M : K$ be a field extension and let L and L' be intermediate fields.

1. If $L : K$ and $L' : K$ are finite and normal, then so is $LL' : K$.
2. If $L : K$ is finite and normal, then so is $LL' : L'$.
3. If $K : K$ is finite, normal with abelian Galois group, then so is $LL' : L'$

Lemma 9.2.7: Iterated Subfields

Let L and M be subfields of $\mathbb{C}$ such that the extensions $L : \mathbb{Q}$ and $M : \mathbb{Q}$ are finite, normal, and solvable. Then there is some subfield M of $\mathbb{C}$ such that $N : \mathbb{Q}$ is finite, normal, and solvable and $L, M \subseteq N$.

Working with the Rationals

Lemma 9.2.8: Let $\mathbb{Q}^{\mathrm{sol}}$ be defined as

$$\mathbb{Q}^{\mathrm{sol}} = \{\alpha \in \mathbb{C} \mid \alpha \in L \text{ for some subfield } L \subseteq \mathbb{C} \text{ that is finite, normal, and solvable over } \mathbb{Q}\}.$$

Then $\mathbb{Q}^{\mathrm{sol}}$ is a subfield of $\mathbb{C}$.

Lemma 9.2.9: Let $\alpha \in \mathbb{C}$ and $n \geq 1$. If $\alpha^n \in \mathbb{Q}^{\mathrm{sol}}$ then $\alpha \in \mathbb{Q}^{\mathrm{sol}}$.

Proposition 9.2.12: $\mathbb{Q}^{\mathrm{rad}} \subseteq \mathbb{Q}^{\mathrm{sol}}$. That is, every radical number is contained in some subfield of $\mathbb{C}$ that is a finite, normal, solvable extension of $\mathbb{Q}$.

Theorem 9.2.13: Solvability of Galois Group

Let $0 \neq f \in \mathbb{Q}[t]$. If the polynomial f is solvable by radicals then the group $\mathrm{Gal}_{\mathbb{Q}}(f)$ is solvable.

Lemma 9.3: Unsolvable Polynomials

Lemma 9.3.1: Let f be an irreducible polynomial over a field K, with $\mathrm{SF}_K(f) : K$ separable. Then $\deg(f)$ divides $|\mathrm{Gal}_K(f)|$.

Lemma 9.3.2: For $n \geq 2$, the symmetric group S_n is generated by (12) and $(12 \ldots n)$.

Lemma 9.3.3: Let p be a prime number, and let $f \in \mathbb{Q}[t]$ be an irreducible polynomial of degree p with exactly $p - 2$ real roots. Then $\mathrm{Gal}_{\mathbb{Q}}(f) \cong S_p$.

Theorem 9.3.5: Unsolvability of the Quintics

Not every polynomial over $\mathbb{Q}$ of degree 5 is solvable by radicals.

10 Finite Fields

Lemma 10.1: Classification of the Finite Fields

Lemma 10.1.1: Let M be a finite field. Then char M is a prime number p, and $|M| = p^n$ where $n = [M : \mathbb{F}_p] \geq 1$. In particular, the order of a finite field is a prime power.

Lemma 10.1.5: Let p be a prime number and $n \geq 1$. Then the splitting field of $t^{p^n} - t$ over $\mathbb{F}_p$ has order p^n.

Lemma 10.1.6 Let M be a finite field of order q. Then $\alpha^q = \alpha$ for all $\alpha \in M$.

Lemma 10.1.8: Every finite field of order q is a splitting field of $t^q - t$ over $\mathbb{F}_p$

Theorem 10.1.9: Classification of Finite Fields

1. Every finite field has order p^n for some prime p and integer $n \geq 1$.
2. For each prime p and integer $n \geq 1$, there is exactly one field of order p^n, up to isomorphism. It has characterstic p and is a splitting field for $t^{p^n} - t$ over $\mathbb{F}_p$.

Lemma 10.2: Multiplicative Structure

Proposition 10.2.1: For an arbitrary field K, every finite subgroup of $K^\times$ is cyclic. In particular, if K is finite, then $K^\times$ is cyclic.

Corollary 10.2.5: Every extension of one finite field over another is simple.

Corollary 10.2.8: For every prime number p and integer $n \geq 1$, there exists an irreducible polynomial over $\mathbb{F}_p$ of degree n.

Lemma 10.3: Galois Groups for Finite Fields

Lemma 10.3.2: Let $M : K$ be a field extension.

1. If K is finite then $M : K$ is separable.
2. If M is also finite then $M : K$ is finite and normal.

Proposition 10.3.3: Let p be a prime and $n \geq 1$. Then $\mathrm{Gal}(\mathbb{F}_{p^n} : \mathbb{F}_p)$ is cyclic of order n, generated by the Frobenius Automorphism of $\mathbb{F}_{p^n}$

Proposition 10.3.6: Let p be a prime and $n \geq 1$. Then $\mathbb{F}_{p^n}$ has exactly one subfield of order p^m for each divisor m of n, and no others. It is

$$\{\alpha \in \mathbb{F}_{p^n} : \alpha^{p^m} = \alpha\}$$

Proposition 10.3.8: Let $M : K$ be a field extension with M finite. Then $\mathrm{Gal}(M : K)$ is cyclic of order $[M : K]$.