Galois Theory (2nd Ed.) - Ian Stewart

Eu-Jin Goh
eujin@cs.stanford.edu

January 12th, 2003

1 Background

1.1 General Properties of Rings

- A *ring* is a set R with binary operations $+$ and $\times$, such that R is an Abelian group under $+$, $\times$ is associative, and the distributive laws

$$(a+b)\times c = (a\times c)+(b\times c)$$
$$a\times(b+c) = (a\times b)+(a\times c)$$

  hold for all $a, b, c \in R$. Denote additive identity of R as 0.

- An *integral domain* is a ring D with three further properties:
  1. Multiplication in D is commutative;
  2. There exists an identity element $1 \in D$ such that $a1 = 1a = a$ for all $a \in D$;
  3. If $ab = 0$ for $a, b \in D$, then either $a = 0$ or $b = 0$.

- A *field* is a ring F such that $F\backslash\{0\}$ is an abelian group under the $\times$ operation. Thus, every non-zero element $a \in F$ has a multiplicative inverse a^{-1}. Every field is an integral domain, the element 1 being the identity of the multiplicative group.

- A *subring* of a ring R is a non-empty subset of R such that the subring is closed under +, - and $\times$ operations.

- A *subfield* of a field F is a non-empty subset S containing 0 and 1 such that if $a, b \in S$, then $a+b, a-b, ab \in S$, and further, if $a \neq 0$ then $a^{-1} \in S$.

- An *ideal* of a ring R is a subring I such that if $i \in I$ and $a \in R$, then $ia, ai \in I$. A field K has no ideals other than 0 or K.

  An example is the set of all integers divisible by a fixed integer n. Call this set $n\mathbb{Z}$. Then, $n\mathbb{Z}$ is an ideal of $\mathbb{Z}$, and the quotient ring $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ is the ring of integers mod n.

- If I is an ideal of the ring R, the *quotient ring* $R\backslash I$ which consists of the cosets of I in R (considered a group under addition with operations)

$$\begin{aligned}(I+r)+(I+s) &= I+(r+s)\\ (I+r)(I+s) &= I+rs\end{aligned}$$

  where $r, s \in R$ and $(I+r)$ is the coset $\{i+r | i \in I\}$.

Theorem 1.1. *The ring $\mathbb{Z}_n$ is a field if and only if n is prime.*

1.2 Characteristic of a Field

Definition. The prime subfield of a field K is the intersection of all subfields of K.

The fields $\mathbb{Q}$ and $\mathbb{Z}_p$ have no proper subfields, and so are equal to their prime subfields.

Theorem 1.2. *Every prime subfield is isomorphic to either the field $\mathbb{Q}$ of rationals or the field $\mathbb{Z}_p$ of integers modulo a prime p.*

Definition. If the prime subfield of K is isomorphic to $\mathbb{Q}$, we say K has *characteristic* 0. If the prime subfield of K is isomorphic to $\mathbb{Z}_p$, we say K has characteristic p.

An alternative definition of *characteristic* is the following.

Definition. A field $\mathbb{F}$ has *characteristic* $p \neq 0$ if for some positive integer p, $px = 0$ for all $x \in \mathbb{F}$, and no positive integer smaller than p has this property. If a field $\mathbb{F}$ is not of characteristic $p \neq 0$ for any positive integer p, then $\mathbb{F}$ has characteristic 0.

Lemma 1.3. *If K is a subfield of L, then K and L have the same characteristic.*

Lemma 1.4. *If k is a non-zero element of the field K, and if n is an integer such that $nk = 0$, then n is a multiple of the characteristic of K.*

1.3 Fields of Fractions

Definition. A field of fractions of the ring R is a field K containing a subring R' isomorphic to R, such that every element of K can be expressed in the form r/s where $r, s \in R'$ and $s \neq 0$.

Theorem 1.5. *Every integral domain possesses a field of fractions.*

1.4 Polynomials

Lemma 1.6. *If R is an integral domain and t is an indeterminate, then $R[t]$ is an integral domain.*

Theorem 1.5 implies that $R[t]$ has a field of fractions. This field of fractions is called the field of rational expressions in t over R and denoted by $R(t)$. Every element in $R(t)$ can be expressed in the form $f(t)/g(t)$ where $f, g \in R[t]$ and $g(t) \neq 0$.

1.5 Euclidean Algorithm

Definition. If f is a polynomial over a commutative ring R and $f \neq 0$, then the *degree* of f is the highest power of t occurring in f with non-zero coefficient.

Denote degree of f as $\partial(f)$.

Proposition 1.7. *If R is an integral domain and f, g are polynomials over R, then*

$$\begin{aligned} \partial(f+g) &\leq \max(\partial(f), \partial(g)) \\ \partial(fg) &= \partial(f) + \partial(g) \end{aligned}$$

Proposition 1.8. *Let f, g be polynomials over a field K, and suppose that f is non-zero. Then there exists unique polynomials k, r such that $g = kf + r$ where r has a smaller degree than f.*

Definition. Let f, g be polynomials over a field K. $f|g$ if there exists some polynomial h over K such that $g = fh$.

Definition (gcd). Let $f, g \in R[t]$. A polynomial $d \in R[t]$ is a *greatest common divisor (gcd)* of f and g if $d|f$ and $d|g$, and furthermore, if there is a polynomial $e \in R[t]$ such that $e|f$ and $e|g$, then $e|d$.

Lemma 1.9. *If d is a* gcd *of polynomials f, g over a field K, and if $0 \neq k \in K$, then kd is also a* gcd *for f, g.*
If d, e are two gcd *for f, g, then there exists some non-zero element $k \in K$ such that $e = kd$.*

Algorithm 1.10. *Euclidean Algorithm.*

Theorem 1.11. *Let f, g be polynomials over a field K and let d be* $\gcd(f, g)$. *Then there exists polynomials a, b over K such that $d = af + bg$.*

2 Factorization of Polynomials

2.1 Irreducibility

Definition. A polynomial over a commutative ring is reducible if it is the product of two polynomials of smaller degree. Otherwise it is irreducible.

Polynomials of degree 0 or 1 are irreducible. The polynomial $t^2 - 2$ is irreducible in $\mathbb{Q}$ but not in $\mathbb{R}$.

Theorem 2.1. *Any non-zero polynomial over a field K is the product of irreducible polynomials over K.*

Definition. If f, g are polynomials over a field K with gcd 1, we say f, g are coprime (relatively prime).

Lemma 2.2. *If K is a field, f is an irreducible polynomial over K, and g, h are polynomials over K such that $f|gh$, then either $f|g$ or $f|h$.*

Theorem 2.3. *For any field K, factorization of polynomials over K into irreducible polynomials is unique up to constant factors and the order in which the factors are written.*

2.2 Tests for Irreducibility

Proposition 2.4. *Let f be an irreducible polynomial over $\mathbb{Z}$. Then f is also irreducible over $\mathbb{Q}$.*

Theorem 2.5 (Eisenstein Criterion). *Let $f(t) = a_0 + a_1 t + \ldots + a_n t^n$ be a polynomial over $\mathbb{Z}$. Suppose there is a prime q such that*

1. $q \nmid a_n$
2. $q | a_i$ *for* $i = 0, \ldots, n-1$
3. $q^2 \nmid a_0$

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

2.3 Zeroes of Polynomials

Definition. Let R be a commutative ring, and f a polynomial over R. Any element $\alpha \in R$ such that $f(\alpha) = 0$ is a *zero* of f in R.

Lemma 2.6. *Let f be a polynomial over the field K. An element $\alpha \in K$ is a zero of f if and only if $(t - \alpha)|f(t)$.*

Definition. Let f be a polynomial over the field K. An element $\alpha \in K$ is a *simple zero* if $(t-\alpha)|f(t)$ but $(t-\alpha)^2 \nmid f(t)$. The element α is a zero of *multiplicity* m if $(t-\alpha)^m | f(t)$ but $(t-\alpha)^{m+1} \nmid f(t)$. Zeroes of multiplicity greater than 1 are repeated or mutiple zeroes.

Lemma 2.7. *Let f be a non-zero polynomial over the field K, and let its distinct zeroes be $\alpha_1, \ldots, \alpha_r$ with multiplicities $m_1, \ldots, m_r$ respectively. Then*

$$f(t) = (t - \alpha_1)^{m_1} \ldots (t - \alpha_r)^{m_r} g(t) \qquad (1)$$

where $g(t)$ has no zeroes in K.

Conversely, if equation (1) holds and g has no zeroes in K, then the zeroes of f are $\alpha_1, \ldots, \alpha_r$ with multiplicities $m_1, \ldots, m_r$ respectively.

Theorem 2.8. *The number of zeroes of a polynomial over a field, counted according to multiplicity, is less than or equal to its degree.*

2.4 Symmetric Polynomials

Definition. The rth elementary symmetric polynomial $s_r(t_1, \ldots, t_n)$ in the indeterminates $t_1, \ldots, t_n$ is the sum of all possible distinct products, taken r at a time, of the elements $t_1, \ldots, t_n$.

Theorem 2.9. *Over a field K, any symmetric polynomial in $t_1, \ldots, t_n$ can be expressed as a polynomial of smaller or equal degree in the elementary symmetric polynomials $s_r(t_1, \ldots, t_n)(r = 0, \ldots, n)$.*

3 Field Extensions

Every polynomial f over a field K defines another field L containing K. This chapter defines field extensions and explains the link with polynomials.

3.1 Field Extensions

Definition. A *field extension* is a monomorphism $i : K \to L$ where K, L are fields; K is the small field, L the large field.

Examples.

1. The inclusion maps $i_1 : \mathbb{Q} \to \mathbb{R}$, $i_2 : \mathbb{R} \to \mathbb{C}$, and $i_3 : \mathbb{Q} \to \mathbb{C}$ are all field extensions.

2. If K is any field, and $K(t)$ is the field of rational expressions over K, then the natural monomorphism $i : K \to K(t)$ mapping each element of K to the corresponding constant polynomial is a field extension.

3. The natural monomorphism $i : K \to K[t]$ is also a field extension.

If $i : K \to L$ is a field extension, we can usually identify K with its image $i(K)$, so that i can be thought of as an inclusion map and K can be thought of as a subfield of L. Under these circumstances, we use the notation $L : K$ for the extension and say that L is an extension of K.

Definition. Let K be a field, X a non-empty subset of K. Then the subfield of K *generated* by X is the intersection of all subfields of K which contain X.

This definition is equivalent to

1. The smallest subfield of K which contains X.

2. The set of all elements of K which can be obtained from elements of X by a finite sequence of field operations, provided $X \neq \{0\}$.

Definition. If $L : K$ is an extension and Y is a subset of L, then the subfield of L generated by $K \cup Y$ is written $K(Y)$ and is said to be obtained from K by *adjoining* Y.

3.2 Simple Extensions

Definition. A *simple extension* is an extension $L : K$ having the property that $L = K(\alpha)$ for some $\alpha \in L$.

For example, $\mathbb{C} = \mathbb{R}(i)$ since $\mathbb{R}(i)$ contains all elements of the form $x + iy$ where $x, y \in \mathbb{R}$.

Definition. An *isomorphism between two field extensions* $i : K \to K^*, j : L \to L^*$ is a pair (λ, μ) of field isomorphisms $\lambda : K \to L, \mu : K^* \to L^*$, such that for all $k \in K$, $j(\lambda(k)) = \mu(i(k))$.

$$\begin{array}{ccc} K & \xrightarrow{i} & K^* \\ \lambda \downarrow & & \downarrow \mu \\ L & \xrightarrow{j} & L^* \end{array}$$

3.3 Constructing Simple Extensions

Definition. Let $K(\alpha) : K$ be a simple extension. If there exists a non-zero polynomial p over K such that $p(\alpha) = 0$, then α is an algebraic element over K and the extension is a *simple algebraic extension.* Otherwise, α is transcendental over K and $K(\alpha) : K$ is a *simple transcendental extension.*

Theorem 3.1. *The field of rational expressions $K(t)$ is a simple transcendental extension of the field K.*

Definition. A polynomial $f(t) = a_0 + a_1 t + \ldots + a_n t^n$ over a field K is *monic* if $a_n = 1$.

Definition. Let $L : K$ be a field extension and suppose that $\alpha \in L$ is algebraic over K. Then the *minimum polynomial* of α over K is the unique monic polynomial m over K of smallest degree such that $m(\alpha) = 0$.

Lemma 3.2. *If α is an algebraic element over the field K, then the minimum polynomial of α over K is irreducible over K. It divides every polynomial of which α is a zero.*

Let R and S be rings, and let $\phi : R \to S$ be a ring homomorphism. Recall that $ker(\phi) = \{r \in R : \phi(r) = 0\}$. The kernel is an ideal of R, and the quotient ring $R/ker(\phi)$ is isomorphic to the image of ϕ. A homomorphism is injective if and only if $ker(\phi) = 0$.

Lemma 3.3. *If ϕ is a ring homomorphism from a field K into a ring R and $\phi \neq 0$, then ϕ is a monomorphism.*

Lemma 3.4. *If m is a irreducible polynomial over the field K, if $\partial(m) > 0$, and I is the ideal of $K[t]$ consisting of all multiples of m, then the quotient ring $K[t]/I$ is a field.*

Theorem 3.5. *If K is any field and m is any irreducible monic polynomial over K, then there exists an extension $K(\alpha) : K$ such that α has minimum polynomial m over K.*

The simple algebraic extension in Theorem 3.5 is constructed using $\alpha = I + t \in K[t]/I$ where I is the ideal of $K[t]$ consisting of all the multiples of m.

3.4 Classifying Simple Extensions

Theorem 3.6. *Every simple transcendental extension $K(\alpha) : K$ is isomorphic to the extension $K(t) : K$ of rational expressions in an indeterminate t over K. The isomorphism can be chosen to carry t into α.*

The isomorphism in Theorem 3.6 is the map $\phi : K(t) \to K(\alpha)$ where $\phi(f(t)/g(t)) = f(\alpha)/g(\alpha)$.

Lemma 3.7. *Let $K(\alpha) : K$ be a simple algebraic extension, where α has minimum polymial m over K. Then, any element of $K(\alpha)$ has a unique expression in the form $p(\alpha)$ where p is a polynomial over K and $\partial(p) < \partial(m)$.*

In Theorem 3.7, $p(\alpha)$ of $f(\alpha)/g(\alpha) \in K(\alpha)$ is the remainder of $f(t)g(t)^{-1}$. To find the unique expression, first find suitable $a \in K(t)$ such that $a(t)g(t) + b(t)m(t) = 1$. When $t = \alpha$, the expression reduces to $a(\alpha)g(\alpha) = 1$, which gives the inverse of $g(\alpha)$. Then calculate $a(\alpha)f(\alpha)$ and reduce it mod m.

Theorem 3.8. *Suppose $K(\alpha) : K$ and $K(\beta) : K$ are simple algebraic extensions, such that α, β have the same minimum polymial m over K. Then the two extensions are isomorphic and the isomorphism of the large fields can be taken to map α to β.*

The isomorphism in Theorem 3.8 is $\tau(\alpha) = \beta$.

Definition. Let $i : K \to L$ be a field monomorphism. There is a monomorphism $\hat{i} : K[t] \to L[t]$ defined by

$$\hat{i}(k_0 + k_1 t + \ldots + k_n t^n) = i(k_0) + \ldots + i(k_n)t^n$$

where $(k_0 + k_1 + \ldots + k_n \in K)$. If i is an isomorphism, then so is $\hat{i}$.

Theorem 3.9. *Suppose K and L are fields and $i : K \to L$ is an isomorphism. Let $K(\alpha), L(\beta)$ be simple algebraic extensions of K and L respectively, such that α has minimum polynomial $m_\alpha(t)$ over K and β has minimum polynomial $m_\beta(t)$ over L. Suppose further that $m_\beta(t) = i(m_\alpha(t))$. Then there exists an isomorphism $j : K(\alpha) \to L(\beta)$ such that $j|_K = i$ and $j(\alpha) = \beta$.*

4 The Degree of an Extension

4.1 The Tower Law

Theorem 4.1. *If $L : K$ is a field extension, the operations*

$$\begin{array}{ll} (\lambda, u) \to \lambda u & \lambda \in K, u \in L \\ (u, v) \to u + v & (u, v \in L) \end{array}$$

define on L the structure of a vector space over K.

Definition. The *degree* $[L : K]$ of a field extension $L : K$ is the dimension of L considered as a vector space over K.

Theorem 4.2. *If K, L, M are fields and $K \subseteq L \subseteq M$, then $[M : K] = [M : L][L : K]$.*

Proposition 4.3. *Let $K(\alpha) : K$ be a simple extension. If it is transcendental, then $[K(\alpha) : K] = \infty$. If it is algebraic, then $[K(\alpha) : K] = \partial(m)$ where m is the minimum polynomial of α over K.*

Definition. A *finite extension* is one whose degree is finite.

Definition. An extension $L : K$ is *algebraic* if every element of L is algebraic over K.

The next lemma shows that every finite extension is algebraic.

Lemma 4.4. *$L : K$ is a finite extension if and only if L is algebraic over K and there exist finitely many elements $\alpha_1, \ldots, \alpha_s \in L$ such that $L = K(\alpha_1, \ldots, \alpha_s)$.*

4.2 Algebraic Numbers

However, every algebraic extension might not be finite.

Definition. Let $\mathbf{A}$ denote the set of all complex numbers which are algebraic over $\mathbb{Q}$. The elements of $\mathbf{A}$ are called *algebraic numbers.*

$\mathbf{A}$ is a field and is an algebraic extension of $\mathbb{Q}$ with infinite degree.

5 Constructibility

6 Transcendental Numbers

7 The Idea Behind Galois Theory

Definition. Let K be a subfield of the field L. An automorphism α of L is a *K-automorphism* of L if $\alpha(k) = k$ for all $k \in K$.

Theorem 7.1. *If $L : K$ is a field extension, then the set of all K-automorphisms of L forms a group under composition of maps.*

Definition. The *Galois group* $\Gamma(L : K)$ of the extension $L : K$ is the group of all K-automorphism of L under the composition of maps.

Definition. If $L : K$ is a field extension, a field M such that $K \subseteq M \subseteq L$ is called an *intermediate* field.

To each intermediate field M, we associate the group $M^* = \Gamma(L : M)$ of all M-automorphisms of L. K^* is the whole Galois group and $L^* = 1$ (identity map on L). Clearly, if $M \subseteq N$, then $M^* \supseteq N^*$, for any map fixing the elements of N certainly fixes the elements of M.

To each subgroup H of $\Gamma(L : K)$, we associate the set $H^\dagger$ of all elements $x \in L$ such that $\alpha(x) = x$ for all $\alpha \in H$. If $H \subseteq G \in \Gamma(L : K)$, then $H^\dagger \supseteq G^\dagger$.

Lemma 7.2. *If H is a subgroup of $\Gamma(L : K)$, then $H^\dagger$ is a subfield of L containing K.*

Definition. With the above notation, $H^\dagger$ is the *fixed field* of H.

If M is an intermediate field and H is a subgroup of the Galois group, then $M \subseteq M^{*\dagger}$ and $H \subseteq H^{\dagger *}$. These inclusions are not always equalities as shown by the extension $\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}$ which has a Galois group of order 1 and hence $\mathbb{Q}^{*\dagger} = \mathbb{Q}(\sqrt[3]{2})$ instead of $\mathbb{Q}$.

8 Normality and Separability

Often, a polynomial $p(t) \in K[t]$ has no zeroes in K. But it may have some zeroes in some extension field L of K. For example, $t^2 + 1 \in \mathbb{R}[t]$ has no zeroes in $\mathbb{R}$, but has zeroes $\pm i \in \mathbb{C}$.

This chapter shows that every polynomial can be resolved into a product of linear factors if the ground field is extended to a suitable splitting field. Splitting fields are shown to be closely related to the idea of normality.

8.1 Splitting Fields

Definition. If K is a field and f is a polynomial over K, then f *splits* over K if it can be expressed as a product of linear factors

$$f(t) = k(t - \alpha_1) \dots (t - \alpha_n)$$

where $k, \alpha_1, \dots, \alpha_n \in K$.

Definition. The field Σ is a *splitting field* for the polynomial f over the field K if $K \subseteq \Sigma$ and

1. f splits over Σ,
2. If $K \subseteq \Sigma' \subseteq \Sigma$ and f splits over Σ' then $\Sigma' = \Sigma$.

The second condition is clearly equivalent to

$\Sigma = K(\sigma_1, \dots, \sigma_n)$ where $\sigma_1, \dots, \sigma_n$ are the zeroes of f in Σ.

Theorem 8.1. *If K is any field and f is any polynomial over K, then there exists a splitting field for f over K.*

The splitting field in Theorem 8.1 is constructed by adjoining the zeroes of f that are not already in K to K.

Lemma 8.2. *Suppose that $i : K \to K'$ is an isomorphism of fields. Let f be a polynomial over K and let Σ be any splitting field for f over K. Let L be any extension field of K' such that $i(f)$ splits over L. Then there exists a monomorphism $j : \Sigma \to L$ such that $j|_K = i$.*

In the previous lemma, we use the isomorphism from Theorem 3.8 to map zeroes to zeroes.

Theorem 8.3. *Let $i : K \to K'$ be a field isomorphism. Let T be a splitting field for f over K, T' a splitting field for $i(f)$ over K'. Then there is an isomorphism $j : T \to T'$ such that $j|_K = i$. In other words, the extensions $T : K$ and $T' : K'$ are isomorphic.*

8.2 Normality

Definition. An extension $L : K$ is *normal* if every irreducible polynomial f over K which has at least one zero in L splits in L.

Theorem 8.4. *An extension $L : K$ is normal and finite if and only if L is a splitting field for some polynomial over K.*

8.3 Separability

Definition. An irreducible polynomial f over a field K is *separable* over K if it has no multiple zeroes in a splitting field.

Definition. An irreducible polynomial over a field K is *inseparable* over K if it is not separable over K.

8.4 Formal Differentiation

Formal differentiation provides a method for determining if a polynomial over an arbitrary field has multiple zeroes.

Definition. Suppose that $f(t) = a_0 + a_1 t + \ldots + a_n t^n \in K[t]$ for a field K. Then the *formal derivative* of f is the polynomial $Df = a_1 + 2a_2 t + \ldots + n a_n t^{n-1}$.

D has the standard properties

$$\begin{aligned} D(f+g) &= Df + Dg \\ D(fg) &= Df \cdot g + f \cdot Dg \\ D(\lambda) &= 0 \\ D(\lambda f) &= \lambda \cdot Df \end{aligned}$$

where $f, g \in K[t]$ and $\lambda \in K$.

Lemma 8.5. *A polynomial $f \neq 0$ over a field K has a multiple zero in a splitting field (is inseparable) if and only if f and Df have a common factor of degree ≥ 1.*

Suppose f is an irreducible polynomial. If f and Df have a common factor g, then f is not irreducible. Therefore, for all f, f and Df do not have a common factor. This statement holds for all f, and therefore $Df = 0$.

Proposition 8.6. *If K is a field of characteristic 0, then every irreducible polynomial over K is separable over K. If K has characteristic $p > 0$, then an irreducible polynomial f over K is inseparable if and only if $f(t) = k_0 + k_1 t^p + \ldots + k_r t^{rp}$ where $k_0, \ldots, k_r \in K$.*

Definition. An arbitrary polynomial over a field K is *separable* over K if all its irreducible factors are separable over K.

Definition. If $L : K$ is an extension, then an algebraic element $\alpha \in L$ is *separable* over K if its minimum polynomial over K is separable over K.

Definition. An algebraic extension $L : K$ is a *separable extension* if every $\alpha \in L$ is separable over K.

Lemma 8.7. *Let $L : K$ be a separable algebraic extension and let M be an intermediate field. Then $M : K$ and $L : M$ are separable.*

9 Field Degrees and Group Orders

To prove the fundamental theorem of Galois theory, we need to show that if H is a subgroup of the Galois group of a finite separable normal extension $L : K$, then $H^{\dagger *} = H$. The method is to show that H and $H^{\dagger *}$ are finite groups with the same order. Since we know that $H \subseteq H^{\dagger *}$, the two groups must be equal.

This chapter develops the techniques needed to partially calculate the order of $H^{\dagger *}$. i.e. we find the degree of $[H^{\dagger} : K]$ in terms of the order of H.

9.1 Linear Independence of Monomorphisms

Suppose K, L are fields, and λ, μ are monomorphisms $K \to L$. Then, λ cannot be a constant (constant here means an element of L) multiple of μ unless $\lambda = \mu$.

Definition (Linearly Independent Monomorphisms). Suppose K, L are fields. Let $\lambda_1, \ldots, \lambda_n$ be monomorphisms $K \to L$. Then, $\lambda_1, \ldots, \lambda_n$ are linearly independent over L if there do not exist elements $a_1, \ldots, a_n \in L$ such that

$$a_1 \lambda_1(x) + \ldots + a_n \lambda_n(x) = 0$$

for all $x \in K$, unless all the a_i are 0.

Lemma 9.1 (Dedekind). *If K, L are fields, then every set of distinct monomorphisms $K \to L$ is linearly independent over L.*

Lemma 9.2. *If $n > m$, then a system of m homogeneous equations $a_{m1} x_1 + \ldots + a_{mn} x_n = 0$ in n unknowns $x_1, \ldots, x_n$ with coefficients a_{ij} taken from a field has a solution in which the x_i are not all zero.*

Lemma 9.3. *If G is a group whose distinct elements are $g_1, \ldots, g_n$, and if $g \in G$, then as j varies from 1 to n, the elements $g g_j$ run through the whole of G, each element of G occuring precisely once.*

Theorem 9.4. *Let G be a finite subgroup of the group of automorphisms of a field K, and let $G^\dagger$ be the fixed field of G. Then $[K : G^\dagger] = |G|$.*

Corollary 9.5. *If G is the Galois group of the finite extension $L : K$ and H is a finite subgroup of G, then $[H^\dagger : K] = [L : K]/|H|$.*

10 Monomorphisms, Automorphisms, and Normal Closures

For normal extensions, we can use K- monomorphisms to build up K-automorphisms. With a K-automorphism, we can calculate the order of the Galois group of any finite separable normal extension. This technique allows us to fully utilize the result in the previous chapter.

This chapter also introduces the concept of a normal closure of a finite extension. This concept allows us to steer around complications caused by non-normal extensions.

10.1 K-Monomorphisms

Definition. Suppose that K is a subfield of each of the fields M and L. Then a *K-monomorphism* of M into L is a map $\phi : M \to L$ which is a field monomorphism such that $\phi(k) = k$ for every $k \in K$.

Theorem 10.1. *Suppose that $L : K$ is a finite normal extension and $K \subseteq M \subseteq L$. Let τ be any K-monomorphism $M \to L$. Then there exists a K-automorphism σ of L such that $\sigma|_M = \tau$.*

Proposition 10.2. *Suppose $L : K$ is a finite normal extension and α, β are zeroes in L of the irreducible polynomial p over K. Then there exists a K-automorphism σ of L such that $\sigma(\alpha) = \beta$.*

10.2 Normal Closures

When extensions are not normal, we can try to recover normality by making the extensions bigger.

Definition. Let L be an algebraic extension of K. A *normal closure* of $L : K$ is an extension N of L such that

1. $N : K$ is normal
2. If $L \subseteq M \subseteq N$ and $M : K$ is normal, then $M = N$.

N is the smallest extension of L which is normal over K.

Theorem 10.3. *If $L : K$ is a finite extension, then there exists a normal closure N of $L : K$ which is a finite extension of K. If M is another normal closure, then the extensions $M : K$ and $N : K$ are isomorphic.*

In the previous Theorem, we construct the normal closure N by setting N as the splitting field for the product of the minimum polynomials of all the elements in the basis of $L : K$.

We construct normal closure from a finite extension by appending to the extension all missing zeroes of the minimal polynomials of (adjoined) elements in the extension.

The next lemma shows how normal closures enable us to place restrictions on the image of a monomorphism.

Lemma 10.4. *Suppose that $K \subseteq L \subseteq N \subseteq M$ where $L : K$ is finite and N is a normal closure of $L : K$. Let τ be any K-monomorphism $L \to M$. Then $\tau(L) \subseteq N$.*

Theorem 10.5. *For a finite extension $L : K$, the following are equivalent*

1. *$L : K$ is normal*
2. *For every extension M of K containing L, every K-monomorphism $\tau : L \to M$ is a K-automorphism of L.*
3. *There exists a normal extension N of K containing L such that every K-monomorphism $\tau : L \to N$ is a K-automorphism of L*

Theorem 10.6. *Suppose $L : K$ is a finite separable extension of degree n. Then there are precisely n distinct K-monomorphisms of L into a normal closure N (and hence into any given normal extension M of K containing L).*

The next Corollary allows us to calculate the order of the Galois group of a finite, separable, and normal extension.

Corollary 10.7. *If $L : K$ is a finite separable normal extension of degree n, then there are precisely n distinct K-automorphisms of L, so that $|\Gamma(L : K)| = n$.*

Theorem 10.8. *Let $L : K$ be a finite extension with Galois group G. If $L : K$ is normal and separable, then K is the fixed field of G.*

There is a converse to Theorem 10.8 which shows why we must consider separable normal extensions to make the Galois correspondence a bijection. The following theorem is needed to prove the converse.

Theorem 10.9. *Suppose that $K \subseteq L \subseteq M$, and that $M : K$ is finite, and that $[L : K] = n$. Then there are at most n K-monomorphisms $L \to M$.*

From the proof of Theorem 10.9, if $L : K$ is not separable, then there are fewer than n K-monomorphisms $L \to M$.

Theorem 10.10. *If $L : K$ is a finite extension with Galois group G such that K is the fixed field of G, then $L : K$ is normal and separable.*

Theorem 10.10 is the converse of Theorem 10.8. Let $L : K$ be a finite extension with Galois group G. Then, $L : K$ is normal and separable if and only if K is the fixed field of G.

11 The Galois Correspondence

This chapter provides the fundamental properties of the Galois correspondence between a field extension and its Galois group.

11.1 Fundamental Theorem

Let $L : K$ be a field extension with Galois group G, which consists of all K-automorphisms of L. Let $\mathcal{F}$ be the set of intermediate fields M, and $\mathcal{G}$ the set of all subgroups H of G.

The maps $^* : \mathcal{F} \to \mathcal{G}$ and $^\dagger : \mathcal{G} \to \mathcal{F}$ are defined as follows: if $M \in \mathcal{F}$, then M^* is the group of all M-automorphisms of L. If $H \in \mathcal{G}$, then $H^\dagger$ is the fixed field of H.

Theorem 11.1. *(Fundamental Theorem of Galois Theory) If $L : K$ is a finite separable normal field extension of degree n, with Galois group G, and if $\mathcal{F}, \mathcal{G}, ^*, ^\dagger$ are defined as above, then*

1. *The Galois group G has order n*
2. *The maps * and † are mutual inverses and set up an order-reversing 1-1 correspondence between $\mathcal{F}$ and $\mathcal{G}$*
3. *If M is an intermediate field then $[L : M] = |M^*|$ and $[M : K] = |G|/|M^*|$*
4. *An intermediate field M is a normal extension of K if and only if M^* is a normal subgroup of G*
5. *If an intermediate field M is a normal extension of K, then the Galois group of $M : K$ is isomorphic to the quotient group G/M^*.*

The following lemma is used to prove parts 4 and 5 of the fundamental theorem.

Lemma 11.2. *Suppose that $L : K$ is a field extension, M is an intermediate field, and τ is a K-automorphism of L. Then, $(\tau(M))^* = \tau M^* \tau^{-1}$.*

12 Example

The Galois group of the splitting field of $t^4 - 2$ over $\mathbb{Q}$.

13 Soluble and Simple Groups

13.1 Soluble Groups

Definition (Soluble Groups). A group G is *soluble* if it has a finite series of subgroups

$$1 = G_0 \subseteq G_1 \subseteq \ldots \subseteq G_n = G$$

such that

1. $G_i \lhd G_{i+1}$ for $i = 0, \ldots, n-1$
2. G_{i+1}/G_i is abelian for $i = 0, \ldots, n-1$.

Example. Every abelian group is soluble.

Suppose we say that a group G is an extension of a group A by a group B if G has a normal subgroup N isomorphic to A such that G/N is isomorphic to B. Then we can show that the class of soluble groups is closed under taking subgroups, quotients, and extensions. To prove this, we require the second and third isomorphism theorems stated below.

Lemma 13.1. *Let G, H, and A be groups.*

1. *Second Isomorphism Theorem*
   If $H \lhd G$, and $A \subseteq G$, then $H \cap A \lhd A$ and $A/(H \cap A) \cong HA/H$.
2. *Third Isomorphism Theorem*
   If $H \lhd G$, and $H \subseteq A \lhd G$, then $H \lhd A$, $A/H \lhd G/H$ and $(G/H)/(A/H) \cong G/A$.

Theorem 13.2. *Let G be a group. Also let H be a subgroup of H and N be a normal subgroup of G.*

1. *If G is soluble, then H is soluble.*
2. *If G is soluble, then G/N is soluble.*
3. *If N and G/N are soluble, then G is soluble.*

The previous theorem tells us that subgroups and quotients of soluble groups are also soluble. Furthermore, if a normal subgroup and the quotient derived from that normal subgroup are both soluble, then the entire group must be soluble.

13.2 Simple Groups

Simple groups are in a sense the opposite of soluble groups.

Definition (Simple Group). A group G is simple if its only normal subgroups are 1 and G.

Theorem 13.3. *A soluble group is simple if and only if it is cyclic of prime order.*

Theorem 13.4. *If $n \geq 5$, then the alternating group A_n of degree n is simple.*

A_5 is the smallest simple non-abelian group.

Corollary 13.5. *The symmetric group S_n of degree n is not soluble if $n \geq 5$.*

Lemma 13.6. *For any n, the symmetric group S_n is generated by the cycles $(12\ldots n)$ and (12).*

13.3 p-Groups

Definition (Conjugate). Elements a and b of a group G are *conjugate* in G if there exists $g \in G$ such that $a = g^{-1}bg$.

Conjugacy is an equivalence relation; the equivalence classes are the conjugacy classes of G.

Definition (Class Equation). Let the conjugacy classes of a group G be $C_1, \ldots, C_r$. Suppose C_1 contains the identity element of G which implies that $|C_1| = 1$. Since the conjugacy classes form a partition of G, we derive the equation $|G| = 1 + |C_2| + \ldots + |C_r|$ which is the *class equation*.

Definition (Centralizer). If G is a group and $x \in G$, then the *centralizer* $C_G(x)$ of x in G is the set of all $g \in G$ such that $xg = gx$.

The centralizer is always a subgroup of G. The following lemma provides a connection between centralizers and conjugacy classes.

Definition (Index). If G is a group and H is a subgroup of G, the number of left cosets of H in G is called the *index* of H in G.

Lemma 13.7. *If G is a group and $x \in G$, then the number of elements in the conjugacy class of x is the index of $C_G(x)$ in G.*

Corollary 13.8. *The number of elements in any conjugacy class of a finite group G divides the order of G.*

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

Definition (Center). The *center* $Z(G)$ of a group G is the set of elements $x \in G$ such that $xg = gx$ for all $g \in G$.

The center of G is a normal subgroup of G. Many groups have trivial centers. For example, $Z(S_3) = 1$ and $Z(G) = G$ where G is abelian.

Theorem 13.9. *If $G \neq 1$ is a finite p-group, then G has non-trivial center.*

Lemma 13.10. *If G is a finite p-group of order p^n, then G has a series of normal subgroups $1 = G_0 \subseteq G_1 \subseteq \ldots \subseteq G_n = G$ such that $|G_i| = p^i$ for all $i = 0, \ldots, n$.*

Corollary 13.11. *Every finite p-group is soluble.*

Theorem 13.12 (Sylow). *Let G be a finite group of order $p^\alpha r$ where p is a prime and does not divide r. Then*

1. *G possesses at least one subgroup of order p^α*
2. *All such subgroups are conjugate in G*
3. *Any p-subgroup of G is contained in one of order p^α*
4. *The number of subgroups of G of order p^α leaves remainder 1 on division by p.*

The previous theorem motivates the following definition.

Definition (Sylow p-subgroup). If G is a finite group of order $p^\alpha r$ where p is a prime and does not divide r, then a *Sylow p-subgroup* of G is a subgroup of G of order p^α.

The following lemma and theorem are used to prove the first part of Sylow's theorem.

Lemma 13.13. *If A is a finite abelian group whose order if divisible by a prime p, then A has an element of order p.*

Theorem 13.14 (Cauchy). *If a prime p divides the order of a finite group G, then G has an element of order p.*

14 Solutions of Equations by Radicals

We use the Galois correspondence to show that for a equation to be soluble by radicals, the associated Galois group must be soluble. We then construct a quintic polynomial whose Galois group is not soluble, which shows that the quintic equation cannot be solved by radicals.

14.1 Radical Extensions

Definition (Radical Extensions). An extension $L : K$ is *radical* if $L = K(\alpha_1, \dots, \alpha_m)$ where for each $i = 1, \dots, m$, there exists an integer $n(i)$ such that $\alpha_i^{n(i)} \in K(\alpha_1, \dots, \alpha_{i-1})$ where $i \geq 2$. The elements α_i are said to form a *radical sequence* for $L : K$.

The following definition states that a polynomial should be soluble by radicals provided all of its zeroes are radical expressions over the ground field.

Definition (Soluble by Radicals). Let f be a polynomial over a field K of characteristic 0, and let Σ be a splitting field for f over K. We say that f is *soluble by radicals* if there exists a field M containing Σ such that $M : K$ is a radical extension.

Remarks.

1. Definition 14.1 is restricted to fields of characteristic 0. Fields of characteristic $p > 0$ have a wider definition of solubility.
2. $\Sigma : K$ need not be radical. Everything in the splitting field should be expressible by radicals but requiring that everything expressible by the same radicals to be in the splitting field adds no value. Furthermore, if $M : K$ is radical and L is an intermediate field, then $L : K$ need not be radical.
3. The definition also requires that all zeroes are f are expressible by radicals. Furthermore, if an irreducible polynomial f has one zero expressible by radicals, then all the zeroes are also expressible by radicals (by Theorem 3.8 simple extensions with the same minimum polynomial are isomorphic).

The theorem we want to prove is the following.

Theorem 14.1. *If K is a field of characteristic 0 and $K \subseteq L \subseteq M$ where $M : K$ is a radical extension, then the Galois group of $L : K$ is a soluble group.*

Intuitively, a radical extension is a series of extension by nth roots. Such extensions have abelian Galois groups so the Galois group of a radical extension is made by fitting together a sequence of abelian groups. The following lemmas are required.

Lemma 14.2. *If $L : K$ is a radical extension and M is a normal closure of $L : K$, then $M : K$ is radical.*

Lemma 14.3. *Let K be a field of characteristic 0, and let L be a splitting field for $t^p - 1$ over K, where p is prime. Then the Galois group of $L : K$ is abelian.*

Lemma 14.4. *Let K be a field of characteristic 0 in which $t^n - 1$ splits. Let $a \in K$ and let L be a splitting field for $t^n - a$ over K. Then the Galois group of $L : K$ is abelian.*

Lemma 14.5. *If K has characteristic 0 and $L : K$ is normal and radical, then $\Gamma(L : K)$ is soluble.*

Definition (Galois Group of a Polynomial). Let f be a polynomial over a field K with a splitting field Σ over K. The *Galois group of f over K* is the Galois group $\Gamma(\Sigma : K)$.

Since Σ is generated by the zeroes of f, G can be thought of as a group of permutations on the zeroes of f. We can restate Theorem 14.1 using this definition.

Theorem 14.6. *Let f be a polynomial over a field K of characteristic 0. If f is soluble by radicals, then the Galois group of f over K is a soluble group.*

The converse of the theorem also holds.

14.2 An Insoluble Quintic

We will exhibit a specfic polynomial with rational coefficients whose Galois group is not soluble. Hence, this polynomial is not soluble by radicals, and so the quintic equation cannot be solved by radicals.

Lemma 14.7. *Let f be an irreducible polynomial with prime degree p over $\mathbb{Q}$. If f has exactly 2 non-real roots in $\mathbb{C}$, then the Galois group of f over $\mathbb{Q}$ is the symmetric group S_p.*

Theorem 14.8. *The polynomial $t^5 - 6t + 3$ over $\mathbb{Q}$ is not soluble by radicals.*

The Galois group of an irreducible polynomial has a useful special property.

Definition (Transitive Permutation Group). Let G be a permutation group on $\{1, \dots, n\}$. We say that G is *transitive* if for all $i, j \leq n$, there exists $\gamma \in G$ such that $\gamma(i) = j$.

Equivalently, it is enough to show that for all $i \leq n$, there exists $\gamma \in G$ such that $\gamma(1) = i$ because there exists $\delta \in G$ such that $\delta(1) = j$ and $(\delta\gamma^{-1})(i) = j$.

Proposition 14.9. *The Galois group of an irreducible polynomial f is transitive on the zeroes of f.*

15 The General Polynomial Equation

Another method of showing the insolubility of the quintic.

16 Finite Fields

In this chapter, we give a complete classification of all finite fields. It turns out that a finite field is uniquely determined up to isomorphism by the number of elements it contains; that this number must be a power of a prime; and that for every prime p and integer $n > 0$, there exists a field with p^n elements.

16.1 Structure of Finite Fields

The next theorem proves that the number of elements in a finite field must be a power of a prime.

Theorem 16.1. *If $\mathbb{F}$ is a finite field, then $\mathbb{F}$ has characteristic $p > 0$, and the number of elements in $\mathbb{F}$ is p^n where n is the degree of $\mathbb{F}$ over its prime subfield.*

The following theorems show that finite fields of the same order must be isomorphic.

Lemma 16.2. *Let K be a field of characteristic $p > 0$. Then the map $\phi : K \to K$ defined by $\phi(k) = k^p$ where $k \in K$ is a field monomorphism. If K is finite, then ϕ is an automorphism.*

Definition (Frobenius Monomorphism). If K is a field of characteristic $p > 0$, then the map $\phi : K \to K$ defined by $\phi(k) = k^p$ where $k \in K$ is the *Frobenius monomorphism* of K. If K is finite, ϕ is called the *Frobenius automorphism.*

Theorem 16.3. *Let p be any prime number and let $q = p^n$ where n is any integer greater than 0. A field $\mathbb{F}$ has q elements if and only if $\mathbb{F}$ is a splitting field for $f(t) = t^q - t$ over the prime subfield $P \cong \mathbb{Z}_p$ of $\mathbb{F}$.*

Since splitting fields exist and are unique up to isomorphism, we have the following theorem.

Theorem 16.4. *A finite field must have $q = p^n$ elements where p is a prime number and n is a positive integer. For each such q, there exists up to isomorphism precisely one field with q elements, which can be constructed as a splitting field for $t^q - t$ over $\mathbb{Z}_p$.*

The field with q elements is denoted $GF(q)$ where GF stands for Galois Field.

16.2 The Multiplicative Group

We explore the structure of the multiplicative group $\mathbb{F}\backslash\{0\}$ of any finite field $\mathbb{F}$.

Definition. The *exponent* $e(G)$ of a finite group G is the least common multiple of the orders of the elements of G.

It is clear that $e(G)$ divides the order of G but in general G need not possess an element of order $e(G)$.

Lemma 16.5. *Any finite abelian group G contains an element of order $e(G)$.*

Corollary 16.6. *If G is a finite abelian group such that $e(G) = |G|$, then G is cyclic.*

Theorem 16.7. *If G is a finite subgroup of the multiplicative group $K\backslash\{0\}$ of a field K, then G is cyclic.*

Corollary 16.8. *The multiplicative group of a finite field is cyclic.*