1 Rings

Theorem 1.1 (Substitution Principle). Let \( \varphi : R \to R' \) be a ring homomorphism.

(a) Given an element \( \alpha \in R' \) there is a unique homomorphism \( \Phi : R[x] \to R' \) which agrees with the map \( \varphi \) on constant polynomials and sends \( x \to \alpha \).

(b) Given elements \( \alpha_1, \ldots, \alpha_n \in R' \) there is a unique ring homomorphism \( \Phi : R[x_1, \ldots, x_n] \) such that \( \Phi|_R = \varphi \) and \( \Phi[x_i] = \alpha_i \).

Lemma 1.2. For every ring \( R \) there is a unique ring homomorphism \( \mathbb{Z} \to R \).

Lemma 1.3. If \( R \) is a ring and \( a \in R \) then \( \{ ra : r \in R \} = (a) \) is an ideal.

Theorem 1.4. A ring \( R \) is a field if and only if it has exactly two ideals.

Corollary 1.5. Let \( F \) be a field and \( R \) a non-zero ring. Then every homomorphism \( \varphi : F \to R \) is injective.

Lemma 1.6. Every ideal in \( \mathbb{Z} \) is principle.

Theorem 1.7. Let \( g(x) \) be a monic polynomial in \( R[x] \) and let \( \alpha \) be an element of \( R \) such that \( g(\alpha) = 0 \). Then \( x - \alpha \) divides \( g(x) \).

Theorem 1.8. If \( F \) is a field then every ideal of \( F[x] \) is principle.

Corollary 1.9. Let \( F \) be a field and let \( f, g \in F[x] \) which are both non-zero. Then there is a unique monic \( d(x) \in F[x] \) called the greatest common divisor of \( f, g \) such that

(a) \( d \) generates the ideal \((f, g)\) of \( F[x] \) generated by \( f, g \).

(b) \( d \) divides \( f \) and \( g \)

(c) If \( h \) is any divisor of \( f \) and \( g \) then \( h \) divides \( d \).

(d) There are \( p, q \in F[x] \) such that \( d = pf + qg \)

Theorem 1.10. Let \( I \) be an ideal of a ring \( R \).

(a) There is a unique ring structure on the set \( R/I \) such that the canonical map \( \pi : R \to R/I \) sending \( a \to a + I \) is a homomorphism.
The kernel of \( \pi \) is \( I \).

**Theorem 1.11** (Mapping Property of Quotient Rings). Let \( f : R \rightarrow R' \) be a ring homomorphism with kernel \( I \) and let \( J \) be an ideal which is contained in \( I \). Denote \( R/J \) by \( \overline{R} \).

(a) There is a unique homomorphism \( f : \overline{R} \rightarrow R' \) such that \( f \pi = f \)

(b) First Isomorphism Theorem: If \( J = I \) then \( f \) maps \( \overline{R} \) isomorphically to the image of \( f \).

**Theorem 1.12** (Correspondence Theorem). Let \( \overline{R} = R/J \) and let \( \pi \) denote the canonical map \( R \rightarrow \overline{R} \)

(a) There is a bijective correspondence between the set of ideals of \( R \) which contain \( J \) and the set of all ideals of \( R \) given by \( I \rightarrow \pi(I) \) and \( \overline{I} \rightarrow \pi^{-1}(I) \)

(b) (Third Isomorphism Theorem) If \( I \subset R \) corresponds to \( \overline{I} \subset \overline{R} \) then \( R/I \) and \( \overline{R}/\overline{I} \) are isomorphic rings.

**Definition 1.13.** Let \( R' \) be a ring extension of \( R \) and let \( \alpha \in R' \). WE define \( R[\alpha] = \{ \Sigma r_i \alpha^i : r_i \in R \} \)

**Theorem 1.14.** Let \( R \subset R' \) and let \( \alpha \in R' \). Then there is a unique map \( \varphi : R[x] \rightarrow R' \) such that \( \varphi \) is the identity on \( R \) and takes \( x \rightarrow \alpha \). Further \( F[\alpha] = \text{im}[\alpha] \)

**Definition 1.15.** \( C = \mathbb{R}[i] \)

**Theorem 1.16.** Let \( R \) be a ring and let \( f(x) \) be a monic polynomial of positive degree with coefficients in \( R \). Let \( R[\alpha] \) be the ring obtained by adjoining an element satisfying \( f(\alpha) = 0 \). The elements of \( R[\alpha] \) are in bijective correspondence with vectors \( (r_0, \cdots, r_{n-1}) \in R^n \) via a map \( \mu \) where \( \mu(r_0, \cdots, r_{n-1}) = r_0 + r_1 \alpha + r_2 \alpha^2 + \cdots + r_{n-1} \alpha^{n-1} \)

**Theorem 1.17.** Let \( R \) be a ring and let \( a, b \in R \) such that \( ab = 0 \). Further let \( c \in R[\alpha] \) be such that \( \psi(a)c = 1 \) where \( \psi : R \rightarrow R[\alpha] \). Then if \( R[\alpha] \neq 0 \) we must have \( \psi(b) = 0 \).

**Definition 1.18.** We say \( b \in R \) is a Zero Divisor if there is a non-zero \( a \in R \) such that \( ab = 0 \).
1.1 Integral Domains

Definition 1.19. A ring \( R \) is an Integral Domain if it has no zero divisors. I.e. \( 0 \neq 1 \) and if \( ab = 0 \) then \( a = 0 \) or \( b = 0 \).

Theorem 1.20. If \( R \) is an integral domain then it satisfies the cancelation law

\[(\forall a, b, c)(a \neq 0) \land (ab = ac) \rightarrow (b = c)\]

Theorem 1.21. If \( R \) is an integral domain then so is \( R[x] \).

Theorem 1.22. Let \( R \) be an integral domain with finitely many elements is a field.

Theorem 1.23. Let \( R \) be an integral domain. Then there exists an embedding \( \phi : R \rightarrow F \) into a field \( F \).

Definition 1.24. Let \( R \) be an integral domain. A fraction in \( R \) will be a pair \( a/b \) where \( a, b \in R \) and \( b \neq 0 \). Two fractions \( a_1/b_1, a_2/b_2 \) are called equivalent \( a_1/b_1 \sim a_2/b_2 \) if \( a_1b_2 = a_2b_1 \).

There is a ring structure on \( F = \{[a/b] \text{ equivalence classes of fractions}\} \) such that \( F \) is a field. It is called the Field of Fractions of \( R \).

Theorem 1.25. Let \( R \) be an integral domain with field of fractions \( F \) and let \( \varphi : R \rightarrow K \) be an injective homomorphism from \( R \) into a field \( K \). Then

\[\Phi(a/b) = \varphi(a)\varphi(b)^{-1}\]

Definition 1.26. An ideal \( M \) is Maximal if \( M \neq R \) but \( M \) is not contained in any other ideals other than \( M, R \).

Theorem 1.27. If \( R \) is an integral domain then \( M \) is a maximal ideal if and only if \( R/M \) is a field.

Theorem 1.28. The maximal ideals of the ring \( \mathbb{Z} \) of integers are the principle ideals generated by the prime integers.

Theorem 1.29. The maximal ideals of the polynomial ring \( \mathbb{C}[x] \) are the principle ideals generated by the linear polynomials \( x - a \).
Theorem 1.30 (Hilbert’s Nullstellensatz). The maximal ideals of the polynomial ring $C[x_1, \ldots, x_n]$ are in a bijective correspondence with points of complex $n$-dimensional space. $a = \langle a_1, \cdots, a_n \rangle \rightarrow M_a = (x_1-a_1, x_2-a_2, \ldots, x_n-a_n)$.

Theorem 1.31. If $a, b \in \mathbb{Z}$ have no factor in common other than $\pm 1$ then there are $c, d$ such that $ac + bd = 1$.

Theorem 1.32. Let $p$ be a prime integer and let $a, b$ be integers. Then if $p$ divides $ab$ $p$ divides $a$ or $p$ divides $b$.

Theorem 1.33 (Fundamental Theorem of Arithmetic). Every integer $a \neq 0$ can be written as a product

$$a = cp_1 \cdots p_k$$

where $c$ is $\pm 1$ and each $p_i$ is prime. And further, up to the ordering this product is unique.

Theorem 1.34. Let $F$ be a field

(a) If two polynomials $f, g \in F[x]$ have no common non-constant factors then there are polynomials $r, s \in F[x]$ such that $rf + sg = 1$

(b) If an irreducible polynomial $p \in F[x]$ divides a product $fg$ then $p$ divides one of the factors.

(c) Every nonzero polynomial $f \in F[x]$ can be written as a product

$$cp_1 \cdots p_n$$

where $c \in F[x]$ and the $p_i$ are monic irreducible polynomials and $n \geq 0$. This factorization is unique except for the ordering of terms.

Theorem 1.35. Let $F$ be a field and let $f(x)$ be a polynomial of degree $n$ with coefficients in $F$. Then $f$ has at most $n$ roots in $F$.

Definition 1.36. Let $R$ be an integral domain. If $a, b \in R$ we say $a$ divides $b$ if $(\exists r \in R)ar = b$

We say that $a$ is a proper divisor of $b$ if $b = qa$ for some $q \in R$ and neither $q \in R$ and neither $q$ nor $a$ is a unit.
We say a non-zero element \( a \in R \) is irreducible if it is not a unit and if it has no proper divisor.

We say that \( a, a' \in R \) are associates if \( a \) divides \( a' \) and \( a' \) divides \( a \). It is easy to show that if \( a, a' \) are associates then \( a = ua' \) for some unit \( u \in R \).

**Theorem 1.37.** Let \( R \) be an integral domain.

\[
\text{\( u \) is a unit } \iff (u) = (1) \\
\text{\( a, a \) are associates } \iff (a) = (a') \\
\text{\( a \) divides \( b \) } \iff (a) \supset (b) \\
\text{\( a \) is a proper divisor of \( b \) } \iff (1) \supseteq (a) \supseteq (b)
\]

**Theorem 1.38.** Let \( R \) be an integral domain. Then the following are equivalent.

(a) For every \( a \in R, a \neq 0 \) if \( a \) is not a unit then

\[
a = b_1 \cdots b_n
\]

where each \( b_i \) is irreducible.

(b) \( R \) does not contain an infinite increasing chain of principle ideals

\[
(a_1) \subset (a_2) \subset (a_3) \subset
\]

**Definition 1.39.** We say that an integral domain \( R \) is a **Unique Factorization Domain** (UFD) if

(i) Existence of factors is true for \( R \)

(ii) If \( a \in R \) and \( a = p_1 \cdots p_n \) and \( a = q_1 \cdots q_m \) where \( p_i, q_j \) are irreducible. Then \( m = n \) and after reordering \( p_i, q_j \) are associates for each \( i \).

**Definition 1.40.** Let \( R \) be an integral domain. \( p \in R \) is prime if \( p \neq 0 \) and \((\forall a, b \in R) \) if \( p \) divides \( ab \) then \( p \) divides \( a \) or \( p \) divides \( b \).

**Theorem 1.41.** Let \( R \) be an integral domain such that existence of factorization holds. Then \( R \) is a UFD if and only if every irreducible element is prime.
Theorem 1.42. Let $R$ be a UFD and let $a = p_1 \ldots p_n, b = q_1 \ldots q_m$ be prime factorizations. Then $a$ divides $b$ if and only if $m \geq n$ and after reordering $p_i, q_i$ are associates for all $i \leq n$.

Theorem 1.43. Let $R$ be a UFD and $a, b \in R$ such that at least one of $a \neq 0$ or $b \neq 0$ holds. Then there exists a greatest common divisor $d$ of $a, b$ such that

(i) $d$ divides $a$ and $b$

(ii) if an element $e$ divides $a$ and $b$ then $e$ divides $d$

Definition 1.44. Let $R$ be an integral domain. We say $R$ is a principle ideal domain (PID) if every ideal is principle.

Theorem 1.45. In an integral domain all prime elements are irreducible. In a PID all irreducible elements are prime.

Theorem 1.46. Every PID is a UFD

Lemma 1.47. Let $R$ be any ring. Then the union of an increasing chain of ideals is an ideal.

Theorem 1.48. Let $R$ be a PID

(a) Let $0 \neq p \in R$. Then $R/(p)$ is a field if and only if $p$ is irreducible.

(b) The maximal ideals of $R$ are those generated by irreducible elements.

2 Fields

Definition 2.1. Let $F$ be a field. And let $\alpha \in K$ such that $K \supseteq F$. We say that $\alpha$ is algebraic over $F$ if there is a polynomial over $F$ which is satisfied by $\alpha$. I.e. if

$$\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + \alpha = 0$$

for some $a_0, \ldots, a_{n-1} \in F$

We say that $\alpha$ is transcendental over $F$ if it is not algebraic over $F$. 
Lemma 2.2. Let \( F \subset K \) be fields with \( \alpha \in K \). Then if
\[
\varphi_\alpha : F[x] \to K \ f(x) \sim f(\alpha)
\]
we have \( \alpha \) is transcendental if and only if \( \varphi \) is injective. Or more specifically if the kernel of \( \varphi \) is 0.

Definition 2.3. Let \( F \subset K \) be fields with \( \alpha \in K \). Further let
\[
\varphi_\alpha : F[x] \to K \ f(x) \sim f(\alpha)
\]
We then know that \( \ker(\varphi_\alpha) \) is principle as \( F[x] \) is a principle ideal domain. So in particular it is generated by a single element \( f_\alpha(x) \in F[x] \).

But because \( K \) is a field we must have \( f_\alpha(x) \) is irreducible (because otherwise \( K \) would have a zero divisor) Hence \( f_\alpha(x) \) is the only irreducible polynomial in \( (f_\alpha(x)) \) (because every element of the ideal is a multiple of \( f_\alpha(x) \)) and we call \( f_\alpha \) the Irreducible Polynomial for \( \alpha \) over \( F \).

Definition 2.4. Let \( F(\alpha) \) be the smallest field containing both \( \alpha \) and \( F \). Similarly let \( F(\alpha_1, \ldots, \alpha_n) \) be the smallest field containing \( \alpha_1, \ldots, \alpha_n \) and \( F \).

Lemma 2.5. Recall that \( F[\alpha] \) is the ring
\[
\{\Sigma a_n\alpha^n : a_n \in F\}
\]
and is the smallest ring containing both \( F \) and \( \alpha \). We then have \( F(\alpha) \) is isomorphic to the field of fractions of \( F[\alpha] \).

In particular we have that if \( \alpha \) is transcendental then \( F[x] \to F[\alpha] \) is an isomorphism and hence \( F(\alpha) \) is isomorphic to the field \( F(x) \) of rational functions.

Theorem 2.6. (a) Suppose that \( \alpha \) is algebraic over \( F \) and let \( f(x) \) be its irreducible polynomial over \( F \). The map \( F[x]/(f) \to F[\alpha] \) is an isomorphism and \( F[\alpha] \) is a field. Thus \( F[\alpha] = F(\alpha) \).

(b) More generally let \( \alpha_1, \ldots, \alpha_n \) be algebraic elements of a field extension \( K \) of \( F \). Then \( F[\alpha_1, \ldots, \alpha_n] = F(\alpha_1, \ldots, \alpha_n) \).

Theorem 2.7. Let \( \alpha \) be an algebraic over \( F \) and let \( f(x) \) be its irreducible polynomial. Suppose \( f(x) \) has degree \( n \). Then \( (1, \alpha, \ldots, \alpha^{n-1}) \) is a basis for \( F[\alpha] \) as a vector space over \( F \).
Theorem 2.8. Let $\alpha \in K$ and $\beta \in L$ be algebraic elements of two extensions of $F$. There is an isomorphism of fields

$$\sigma : F(\alpha) \to F(\beta)$$

which is the identity on $F$ and which sends $\alpha \mapsto \beta$ if and only the irreducible polynomials for $\alpha$ and $\beta$ over $F$ are equal.

Definition 2.9. Let $K, K'$ be field extensions of $F$. An isomorphism

$$\varphi : K \to K'$$

which restricts to the identity on $F$ is called an Isomorphism of field extensions of an $F$-isomorphism

Theorem 2.10. Let $\varphi : K \to K'$ be an isomorphism of field extensions of $F$ and let $f(x)$ be a polynomial with coefficients in $F$. Let $\alpha$ be a root of $f$ in $K$ and let $\alpha' = \varphi(\alpha)$ be its image in $K'$. Then $\alpha'$ is also a root of $f$.

Definition 2.11. Let $K$ be a field extension of a field $F$. We can always regard $K$ as a vector space over $F$ where addition is field addition and multiplication by $F$ is simply multiplication.

We say that the degree of $K$ as an extension of $F$ is the dimension of the vector space (denoted $[K : F]$).

Extensions of degree 2 are called quadratic, of degree are called cubic, etc.

The term degree comes from the case when $K = F(\alpha)$ for an algebraic $\alpha$ over $F$ and so $(1, \alpha, \ldots, \alpha^{n-1})$ form a basis for the vector space (where $n$ is the degree of the irreducible polynomial).

In this case we also call the degree the degree of $\alpha$ over $F$.

Theorem 2.12. If $\alpha$ is algebraic over $F$ then $[F(\alpha) : F]$ is the degree of the irreducible polynomial of $\alpha$.

Theorem 2.13. Let $F \subset K \subset L$ be fields. Then $[L : F] = [L : K][K : F]$. These are called towers of field extensions.

Corollary 2.14. Let $K$ be an extension of $F$ of finite degree $n$ and let $\alpha \in K$. Then $\alpha$ is algebraic over $F$ and it’s degree divides $n$. 
Corollary 2.15. Every irreducible polynomial in \( \mathbb{R}[x] \) has degree 1 or 2

Theorem 2.16. Let \( K \) be an extension of \( F \). The elements of \( K \) which are algebraic over \( F \) form a subfield of \( K \).

Definition 2.17. We say that an extension \( K \) of \( F \) is an algebraic extension (and \( K \) is algebraic over \( F \)) if every element of \( K \) is algebraic over \( F \).

Theorem 2.18. Let \( F \subset K \subset L \) be fields. If \( L \) is algebraic over \( K \) and \( K \) is algebraic over \( F \), then \( L \) is algebraic over \( F \).

Theorem 2.19. Let \( F \) be a field. Let \( F' = F[x]/I \). Then \( I = (f) \) for some \( f \in F[x] \) and \( F' \) is a field if and only if the \( (f) \) is irreducible.

Corollary 2.20. Let \( F \) be a field and let \( f \in F[x] \) be irreducible. Then \( K = F[x]/(f) \) is a field extension of \( F \) and the residue of \( x \) is a root of \( f \) in \( K \).

Theorem 2.21. Let \( F \) be a field and let \( f(x) \) be a monic polynomial in \( F[x] \) of positive degree. Then there is a field extension \( K \) of \( F \) such that \( f(x) \) factors into linear factors over \( K \).

Theorem 2.22. Let \( f, g \in F[x] \) and let \( K \) be a field extension of \( F \).

\( (a) \) Division with remainder of \( g \) by \( f \) gives the same answer whether carried out in \( F[x] \) or in \( K[x] \).

\( (b) \) \( f \) divides \( g \) in \( K[x] \) if and only if \( f \) divides \( g \) in \( F[x] \).

\( (c) \) The monic greatest common divisor \( d \) of \( f, g \) is the same whether computed in \( K[x] \) or in \( F[x] \).

\( (d) \) If \( f \) and \( g \) have a common root in \( K \), then they are not relatively prime in \( F[x] \). Conversely if \( f \) and \( g \) are not relatively prime in \( F[x] \) then there exists an extension field \( L \) in which they have a common root.

\( (e) \) If \( f \) is irreducible in \( F[x] \) and \( f \) and \( g \) have a common root in \( K \) then \( f \) divides \( g \) in \( F[x] \).

Definition 2.23. Let \( F \) be a field and let \( f \in F[x] \). If

\[
f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0
\]

is an irreducible polynomial in \( F[x] \), then by Theorem 2.22, \( \deg(f) \) is the degree of the extension \( \mathbb{F}_p, a \mathbb{F}_p, \mathbb{F}_q, \mathbb{F}_r \).
then we define

\[ f'(x) = na_nx^{n-1} + (n-1)a_{n-1}x^{n-2} \cdots a_1 \]

Where we interpret \( n \) as the image of \( n \in \mathbb{Z} \) under the unique ring homomorphism \( \mathbb{Z} \to F \).

It can be shown that things like the product rule hold for these formal derivatives.

Lemma 2.24. Let \( F \) be a field and let \( f(x) \in F[x] \). Let \( \alpha \in F \) be a root of \( f(x) \). Then \( \alpha \) is a multiple root, i.e. that \( (x - \alpha)^2 \) divides \( f(x) \) if and only if \( \alpha \) is a root of \( f(x) \) and of \( f'(x) \).

Theorem 2.25. Let \( f(x) \in F[x] \) where \( F \) is a field. Then there exists a field extension \( K \) of \( F \) in which \( f \) has a multiple root if and only if \( f \) and \( f' \) are not relatively prime.

Theorem 2.26. Let \( f \) be an irreducible polynomial in \( F[x] \). Then \( f \) has no multiple roots in any field extension of \( F \) unless the derivative \( f' \) is the zero polynomial. In particular if \( F \) has characteristic 0, then \( f \) has no multiple root.

Definition 2.27. Let \( K \) be a field extension of \( F \). Let \( \alpha_1, \ldots, \alpha_n \) be a sequence of elements of \( K \). We say that \( \alpha_1, \ldots, \alpha_n \) are Algebraically Dependent if there is a polynomial \( f \in F[x_1, \ldots, x_n] \) such that \( f(\alpha_1, \ldots, \alpha_n) = 0 \). We say \( \alpha_1, \ldots, \alpha_n \) are algebraically independent otherwise.

Lemma 2.28. Let \( F \subseteq K \). \( \alpha_1, \ldots, \alpha_n \) are algebraically independent if and only if the substitution map \( \varphi : F[x_1, \ldots, x_n] \to K \) which takes \( f(x_1, \ldots, x_n) \) to \( f(\alpha_1, \ldots, \alpha_n) \) has \( \ker(\varphi) = 0 \).

Corollary 2.29. If \( \alpha_1, \ldots, \alpha_n \) are algebraically independent over \( F \) then \( F(\alpha_1, \ldots, \alpha_n) \) is isomorphic to \( F(x_1, \ldots, x_n) \) the field of rational functions in \( x_1, \ldots, x_n \).

Definition 2.30. An extension of the form \( F(\alpha_1, \ldots, \alpha_n) \) where \( \alpha_1, \ldots, \alpha_n \) are algebraically independent is called a Pure Transcendental extension.

Definition 2.31. A transcendence basis for a field \( K \) of \( F \) is a set of elements \( \alpha_1, \ldots, \alpha_n \) such that \( K \) is algebraic over \( F(\alpha_1, \ldots, \alpha_n) \).
Theorem 2.32. Let \((\alpha_1, \ldots, \alpha_m)\) and \((\beta_1, \ldots, \beta_n)\) be elements in a field extension \(K\) of \(F\) which are algebraically independent. If \(K\) is algebraic over \(F(\beta_1, \ldots, \beta_n)\) then \(m \leq n\) and \((\alpha_1, \ldots, \alpha_m)\) can be completed to a transcendence basis for \(K\) by adding \(n - m\) many of the \(\beta_i\).

Corollary 2.33. Any two transcendence basis for a field extension \(F \subseteq K\) have the same number of elements.

2.1 Finite Fields

Definition 2.34. We say that \(q = p^r = |K|\) is the order of a field \(K\). When dealing with finite fields \(p\) will always be a prime and \(q\) will be the order of the field we are talking about.

Fields with \(q = p^r\) elements are often denoted \(\mathbb{F}_q\).

Theorem 2.35. Let \(p\) be a prime and let \(q = p^r\) be a power of \(p\) with \(r \geq 1\). Let \(K\) be a field with order \(q\).

(a) There exists a field of order \(q\)

(b) Any two fields of order \(q\) are isomorphic.

(c) Let \(K\) be a field of order \(q\). The multiplicative group \(K^\times\) of nonzero elements of \(K\) is a cyclic group of order \(q - 1\).

(d) The elements of \(K\) are roots of the polynomial \(x^q - x\). This polynomial has distinct roots and it factors into linear factors in \(K\)

(e) Every irreducible polynomial of degree \(r\) in \(\mathbb{F}_p[x]\) is a factor of \(x^q - x\). The irreducible factors of \(x^q - x\) in \(\mathbb{F}_p[x]\) are precisely the irreducible polynomials in \(\mathbb{F}_p[x]\) whose degree divides \(r\).

(f) A field \(K\) of order \(q\) contains a subfield of order \(q' = p^k\) if and only if \(k\) divides \(r\).

Corollary 2.36. Let \(K\) be a finite field. Then there is an element \(a \in K\) such that for all \(b \in K, b \neq 0\) there is an \(n \in \omega\) such that \(a^n = b\).

Definition 2.37. A generator for the cyclic group \(\mathbb{F}_p^\times\) is called an primitive element modulo \(p\).
Theorem 2.38. Let $p$ be a prime and let $q = p^r$.

(a) The polynomial $x^q - x$ has no multiple root in any field $L$ of characteristic $p$.

(b) Let $L$ be a field of characteristic $p$ and let $K$ be the set of roots of $x^q - x$ in $L$. Then $K$ is a subfield of $L$.

Theorem 2.39. Let $L$ be a field of characteristic $p$, and let $q = p^r$. Then in the polynomial ring $L[x, y]$, we have $(x + y)^q = x^q + y^q$.

Lemma 2.40. Let $k$ be an integer dividing $r$, say $r = ks$, and let $q = p^r$, $q' = p^k$. Then $x^{q'} - x$ divides $x^q - x$.

Definition 2.41. A field $F$ is algebraically closed if every polynomial $f(x) \in F[x]$ has a root in $F$.

Theorem 2.42 (Fundamental Theorem of Algebra). Every nonconstant polynomial with complex coefficients has a complex root.

Definition 2.43. Let $F$ be a field. $\overline{F}$ is an algebraic closure of $F$ if

- $\overline{F}$ is algebraically closed
- $\overline{F}$ is algebraic over $F$.

Corollary 2.44. Let $F$ be a subfield of $\mathbb{C}$. Then the subset $\overline{F}$ of $\mathbb{C}$ consisting of all numbers algebraic over $F$ is an algebraic closure of $F$.

Theorem 2.45. Every field $F$ has an algebraic closure and if $K_1, K_2$ are algebraic closures of $F$ there is an isomorphism $\varphi : K_1 \rightarrow K_2$ which is the identity map on $F$.

Corollary 2.46. Let $\overline{F}$ be an algebraic closure of $F$, and let $K$ be any algebraic extension of $F$. Then there is a subextension $K' \subset \overline{F}$ which is isomorphic to $K$.

Lemma 2.47. Let $f(x)$ be a complex polynomial. Then $|f(x)|$ takes on a minimum value at some point $x_0 \in \mathbb{C}$.
2.2 Field Extensions

Definition 2.48. If $K$ is a field extension of $F$ we say $K/F$.

Definition 2.49. An $F$-automorphism of $K$ is an automorphism of $K$ which is the identity on $F$.

Definition 2.50. The group of all $F$-automorphisms of $K$ is called the Galois Group of the field extension $(G(K/F))$.

Theorem 2.51. For any finite extension $K/F$ the order of $|G(K/F)|$ divides the degree $[K : F]$ of the field extension.

Definition 2.52. A finite field extension $K/F$ is called a Galois Extension if

$|G(K/F)| = [K : F]$ 

Definition 2.53. Let $G$ be a group of automorphisms of $K$. The set of elements fixed by every element of $G$ is called the fixed field of $G$

$K^G = \{ \alpha \in K : \varphi(\alpha) = \alpha \text{ for all } \varphi \in G \}$

Corollary 2.54. Let $K/F$ be a Galois extension with Galois group $G = G(K/F)$. The fixed field of $G$ is $F$.

Definition 2.55. Let $f(x) \in F[x]$ be a nonconstant monic polynomial. A splitting field for $f(x)$ over $F$ is an extension $K$ of $F$ such that

(i) $f(x)$ factors into linear factors in $K : f(x) = (x - \alpha_1) \cdots (x - \alpha_n)$ with $\alpha_i \in K$

(ii) $K$ is generated by the roots of $f(x) : K = F(\alpha_1, \ldots, \alpha_n)$

Theorem 2.56. If $K$ is a splitting field of a polynomial $f(x)$ over $F$ then $K$ is a Galois extension of $F$. Conversely, every Galois extension is a splitting field of some polynomial $f(x) \in F[x]$.

Corollary 2.57. Every finite extension is contained in a Galois extension.

Corollary 2.58. Let $K/F$ be a Galois extension and let $L$ be an intermediate field: $F \subset L \subset K$. Then $K/L$ is a Galois extension too.
Theorem 2.59.  (a) Let $K$ be an extension of a field $F$, let $f(x)$ be a polynomial with coefficients in $F$ and let $\sigma$ be an $F$-automorphism of $K$. If $\alpha$ is a root of $f(x)$ in $K$ then $\sigma(\alpha)$ is also a root.

(b) Let $K$ be a field extension generated over $F$ by elements $\alpha_1, \ldots, \alpha_r$ and let $\sigma$ be an $F$-automorphism of $K$. If $\sigma$ fixes each of the generators $\alpha_i$ then $\sigma$ is the identity automorphism.

(c) Let $K$ be a splitting field of a polynomial $f(x)$ over $F$. The Galois group $G(K/F)$ operates faithfully on the set $\{\alpha_1, \ldots, \alpha_r\}$.

Theorem 2.60 (The Main Theorem). Let $K$ be a Galois extension of a field $F$ and let $G = G(K/F)$ be its Galois group. The function

$$H \mapsto K^H$$

is a bijective map from the set of subgroups of $G$ to the set of intermediate fields $F \subset L \subset K$. Its inverse is

$$L \mapsto G(K/L)$$

This correspondence has the property that if $H = G(K/L)$ then

$$[K : L] = |H| \text{ hence } [L : F] = [G : H]$$

Theorem 2.61 (Existence of a primitive element). Let $K$ be a finite extension of a field $F$ of characteristic 0. there is an element $\gamma \in K$ such that $K = F(\gamma)$.

Definition 2.62. We call an element $\gamma \in K$ such that $F(\gamma) = K$ a primitive element for $K$ over $F$.

Theorem 2.63. Let $G$ be a finite group of automorphisms of a field $K$ and let $F$ be its fixed field. Let $\{\beta_1, \ldots, \beta_r\}$ be the orbit of an element $\beta = \beta_1 \in K$ under the action of $G$. Then $\beta$ is algebraic over $F$, it’s degree over $F$ is $r$ and its irreducible polynomial over $F$ is $g(x) = (x - \beta_1) \cdots (x - \beta_r)$. Further note that $r$ divides $|G|$.

Corollary 2.64. Let $K/F$ be a Galois extension. Let $g(x)$ be an irreducible polynomial in $F[x]$. If $g$ has one root in $K$ then it factors into linear factors in $K[x]$. 
Theorem 2.65. Let $G$ be a group of order $n$ of automorphisms of a field $K$ and let $F$ be its fixed field. Then $[K : F] = n$.

Corollary 2.66. Let $G$ be a finite group of automorphisms of a field $K$ and let $F$ be its fixed field. Then $K$ is a Galois extension of $F$ and its Galois group is $G$.

Definition 2.67. Let $\varphi : F \rightarrow \overline{F}$ be an isomorphism. Then $\varphi$ extends to an isomorphism $F[x] \rightarrow \overline{F}[x]$ by

$$\sum a_n x^n \mapsto \sum \overline{a_n} x^n$$

where $\overline{a_n} = \varphi(a_n)$. We denote by $\overline{f}(x)$ the image of $f(x)$ under this map.

Lemma 2.68. Let $f(x) \in F[x]$ be an irreducible polynomial. Let $\alpha$ is a root of $f(x)$ in an extension field $K$ of $F$ and let $\overline{\alpha}$ be a root of $\overline{f}(x)$ in an extension field $\overline{K}$ of $\overline{F}$. Then there is a unique isomorphism

$$\varphi_1 : F(\alpha) \rightarrow \overline{F}(\overline{\alpha})$$

which restricts to $\varphi$ on the subfield $F$ and which sends $\alpha$ to $\overline{\alpha}$.

Theorem 2.69. Let $\varphi : F \rightarrow \overline{F}$ be an isomorphism of fields. Let $f(x) \in F[x]$ be nonconstant and let $\overline{f}(x)$ be the corresponding polynomial in $\overline{F}[x]$. Let $K$ and $\overline{K}$ be the splitting fields for $f(x)$ and $\overline{f}(x)$. Then there is an isomorphism $\psi : K \rightarrow \overline{K}$ which restricts to $\varphi$ on $F$.

Corollary 2.70. Any two splitting fields of $f(x) \in F[x]$ are isomorphic.

Theorem 2.71. Let $K$ be the splitting field of a polynomial $f(x) \in F[x]$. Then $K$ is a Galois extension of $F$. That is $|G(K/F)| = [K : F]$.

Lemma 2.72. With the notation of the previous lemma, the number of isomorphisms $\psi : K \rightarrow \overline{K}$ extending $\varphi$ is equal to $[K : F]$.

Definition 2.73. Since any two splitting fields $K$ of $f(x) \in F[x]$ are isomorphic, the Galois group $G(K/F)$ depends, up to isomorphism, only on $f$. It is often referred to as the Galois group of the polynomial over $F$.

Corollary 2.74. Let $K/F$ be a finite field extension. the following are equivalent.
(i) $K$ is a Galois extension of $F$.

(ii) $K$ is the splitting field of an irreducible polynomial $f(x) \in F[x]$.

(ii') $K$ is the splitting field of a polynomial $f(x) \in F[x]$.

(iii) $F$ is the fixed field for the action of the Galois group $G(K/F)$ on $K$.

(iii') $F$ is the fixed field for an action of a finite group of automorphisms of $K$.

**Theorem 2.75 (Main Theorem).** Let $K$ be a Galois extension of a field $F$ and let $G = G(K/F)$ be its Galois group. The function

$$H \mapsto K^H$$

is a bijective map from the set of subgroups of $G$ to the set of intermediate fields $F \subset L \subset K$. Its inverse function is

$$L \mapsto G(K/L)$$

This correspondence has the property that if $H = G(K/L)$ then

$$[K : L] = |H| \text{ and } [L : F] = [G : H]$$

**Theorem 2.76.** Let $K/F$ be a Galois extension and let $L$ be an intermediate field. Let $H = G(K/L)$ be the corresponding subgroup of $G = G(K/F)$. Then

(a) Let $\sigma$ be an element of $G$. The subgroup of $G$ which corresponds to the conjugate subfield $\sigma L$ is the conjugate subgroup $\sigma H \sigma^{-1}$. In other words

$$G(K/\sigma L) = \sigma H \sigma^{-1}.$$  

(b) $L$ is a Galois extension of $F$ if and only if $H$ is a normal subgroup of $G$. When this is so, then $G(L/F)$ is isomorphic to the quotient group $G/H$.

**Definition 2.77.** Let $F \subseteq \mathcal{C}$ be a subfield of $\mathcal{C}$ which contains a primitive $p$th root of unity $\zeta_p = e^{2\pi i/p}$.

**Lemma 2.78.** If $\alpha$ is a root of $f(x) = x^p - a$ then $\alpha, \zeta_p \alpha, \zeta_p^2 \alpha, \ldots, \zeta_p^{p-1} \alpha$ are the roots of $f(x)$. So the splitting field of $x^p - a$ is generated by a single root $K = F[\alpha]$.
Theorem 2.79. Let $F \subseteq \mathbb{C}$ and let $F$ contain a $p$th root of unity. Further let $a \in F$ be an element which is not a $p$th power in $F$. Then the splitting field of $f(x) = x^p - a$ has degree $p$ over $F$ and its Galois group is a cyclic group of order $p$.

Theorem 2.80. Let $F$ be a subfield of $\mathbb{C}$ which contains a $p$th root of unity $\zeta_p$ and let $K/F$ be a Galois extension of degree $p$. Then $K$ is obtained by adjoining a $p$th root to $F$.

Theorem 2.81. Let $p$ be a prime integer and let $\zeta_p = e^{2\pi i/p}$. For any subfield $F$ of $\mathbb{C}$ the Galois group of $F(\zeta_p)$ over $F$ is a cyclic group.

Let’s consider the Galois group of a product of polynomials $f(x)g(x)$ over $F$. Let $K'$ be a splitting field of $fg$. Then $K'$ contains a splitting field of $K$ of $f$ and $F'$ of $g$. So we have the following diagram.

\[
\begin{array}{ccc}
K' & \cup & F' \\
\cup & K & \cup
\end{array}
\]

Theorem 2.82. With the above notation, let $G = G(K/F)$ and $H = G(F'/F)$ and $G = G(K'/F)$.

(i) $G$ and $H$ are quotients of $G$.

(ii) $G$ is isomorphic to a subgroup of the product $G \times H$. 