Galois theory, commutative algebra, with applications to finite fields
Preface

This is the written notes for the course entitled “Galois theory and commutative algebra” given in the fall of 2004. However, this notes is not faithful to the one given in class as I found it necessary to rearrange some topics. For example, ring of algebraic integers was mentioned both in Galois theory and Dedekind domain during the semester and in this notes only one chapter is devoted to it. Another effort I am trying to make is putting more details to the examples and exercise.

The purpose of the course is to build a bridge between basic algebra core courses and advanced topics such as coding theory, algebraic number theory, and algebraic geometry. Hence we assume that the students have some basic background on ring theory and module theory.

The notes consists of three parts: Galois theory, introduction to commutative algebra, and applications to coding theory.

In the first part, Galois theory, we emphasize on the fundamental theory of Galois group, and some basic properties of fields such as normality, separability, and certain structures of their Galois group such as cyclic extensions. Throughout the first part, one of the main themes is finite field. We are also hoping to cover some basic properties for function fields with characteristic greater than 0. These are motivated by the fact that finite field is one of the most extensively used mathematical tools in other sciences and technology. On the other hand, function fields with characteristic greater 0 have attracting growing attention as they are used in various applications such as coding theory. We would like to point out that we omit some very classical topics in Galois theory such as ruler and compass constructions. It is because that the audience might have learned these topics from basic abstract algebra. If not, they can be found in most books contained Galois theory such as the one by Jacobson [Jac85] or the one by Hungerford [Hun80].

The topics to be considered in part two, introduction to commutative al-
algebra, besides some reviews, consists of primary decomposition, chain condition, Noetherian and Artinian rings, discrete valuations rings, and Dedekind domains. Hopefully they serve a preparation for learning algebraic number theory and algebraic curves which can be used for constructing geometric codes, mainly Goppa codes.

A Dedekind domain is an commutative domain in which every ideal is finitely generated, every nonzero prime ideal is a maximal ideal, and which is integrally closed in its fraction field.

In another description, an commutative domain $R$ is a Dedekind domain if and only if the localization of $R$ at each prime ideal $p$ of $R$ is a discrete valuation ring.

Some examples of Dedekind domains are the ring of integers, the polynomial rings $F[x]$ in one variable over any field $F$, and any other principal ideal domain. Not all Dedekind domains are principal ideal domains however. The most important examples of Dedekind domains, and historically the motivating ones, arise from algebraic number fields that we have considered before.

The study of Dedekind domains was initiated by Dedekind, who introduced the notion of ideal in a ring in the hopes of compensating for the failure of unique factorization into primes in rings of algebraic integers. While not all Dedekind domains are unique factorization domains, they all have a property closed to unique factorization: primary decomposition. This means every ideal can be uniquely factored as a product of primary ideals.

There is another example of Dedekind domains generalizing the example that $F[x]$ being a Dedekind domain. Let $C$ be any smooth algebraic curve over an algebraically closed field $F$. Then the ring of functions of $C$ over $F$ is also a Dedekind domain. We use that here as a motivation for learning elliptic curves, commutative algebra, and algebraic geometry. See the first two chapter of [Sil86] for a more detailed description of algebraic curves.
In last part on coding theory consists of student presentations

- James Fiedler: Hamming codes and hat game
- Mehmed Dagli: BCH codes
- Tim Zick: Perfect codes
- Theodore Rice: Greedy codes and games
- Key One Chung: Goppa codes
Basic notations

- \( \mathbb{Z} \): the ring of rational integers;
- \( \mathbb{Q} \): The field of rational numbers;
- \( F, E, K \): fields;
- \( F[X] \): the smallest ring containing both the field \( F \) and the set \( X \);
- \( F(X) \): the smallest field containing both the field \( F \) and the set \( X \); or the field of fractions of \( F[X] \);
- \( | \cdot | \): cardinality or order;
- \( \mathcal{O}_K \): the ring of integers of the field \( K \);
- \( \mathbb{F}_{p^n} \): a finite field of characteristic \( p^n \);
- \( \overline{F} \): an algebraic closure of the field \( F \);
- \( E/F \): the field \( E \) is an extension of the field \( F \);
- \( [E : F] \): degree of the field extension;
- \( \text{Gal}(E/F) \): The Galois group of the extension \( E/F \);
- \( \text{Inv}G \): the field of invariants of the automorphism group \( G \);
- \( T_E^F(u) \): trace of the element \( u \in E \);
- \( N_E^F(u) \): norm of the element \( u \in E \);
- \( R, A \): rings;
- \( M \): module;
- \( l(M) \): length of the module \( M \);
- \( a, b, c \): ideals;
- \( r(a) \), or \( \sqrt{a} \): the radical of the ideal \( a \);
- \( p \): prime ideals;
• \( q \): primary ideal;
• \( \mathfrak{M} \): maximal ideal;
• \( \mathfrak{N} \): the Nilradical of the ring;
• \( \mathfrak{R} \): the Jacobson radical of the ring;
• \( S^{-1}A \): ring of fractions with respect to the multiplicative set \( S \);
• \( A_p \): ring \( A \) localized at the prime ideal \( p \);
• \( \text{dim } A \): the dimension of ring \( A \);
• \( \text{Ann}(x) \): the annihilating ideal of element \( x \) in \( A \);
• \( \mathbb{A}^1_k \): the affine line over the field \( k \);
• \( \text{Spec}(A) \): the spectrum of the ring \( A \);
Contents

I  Galois theory ........................................ 13

1  Field extension ........................................ 15
   1.1 Field extension and examples ...................... 15
   1.2 Simple extension .................................. 20

2  Galois groups of field extensions ...................... 23
   2.1 Field isomorphism ................................ 23
   2.2 Splitting fields of a polynomial .................. 24
   2.3 Multiple roots .................................... 26
   2.4 Algebraic closure .................................. 28
   2.5 Galois groups ..................................... 29
   2.6 Galois extension ................................... 32
   2.7 Fundamental theorem of Galois theory .......... 33

3  Separability ........................................... 37
   3.1 Purely inseparable extensions .................... 37
   3.2 Separable extensions ................................ 39

4  Cyclic extensions ..................................... 45
   4.1 Trace and Norm ................................... 45
   4.2 Cyclic extension ................................... 46

5  Finite fields .......................................... 49
   5.1 Properties of finite fields ....................... 49
   5.2 Irreducible polynomials over \( \mathbb{F}_p \) ........... 51
II Commutative algebra 53

6 Rings and ideals-Review 55
6.1 Ideals ................................. 55
6.2 Local rings ............................ 56
6.3 Nilradical and Jacobson radical ............. 56
6.4 Rings and modules of fractions ............... 57
6.5 Nakayama’s lemma ........................ 58
6.6 Integral dependency ........................ 59
6.7 Integrally closed domains .................... 61

7 Primary decomposition 63
7.1 Primary ideals ........................... 63
7.2 Primary decomposition ...................... 64
7.3 Minimal primary decomposition .............. 64

8 Chain condition 67
8.1 Chain condition ........................... 67
8.2 Basic properties of Noetherian and Artinian rings .................. 68

9 Noetherian rings 73
9.1 Properties of Noetherian rings ............... 73
9.2 Primary decomposition for Noetherian rings .............. 76

10 Artinian Rings 79
10.1 Further properties of Artinian rings ............ 79
10.2 Local Artinian rings ...................... 80

11 Discrete valuation ring and Dedekind domains 83
11.1 Discrete valuation rings .................... 83
11.2 Dedekind domains ........................ 85

12 Algebraic integers 87
12.1 Algebraic integers form a ring and a Z-module ............ 87
12.2 Ring of integers of a number field is a Dedekind domain .................. 89
12.3 Primary decomposition for imaginary quadratic number fields 89
13 Algebraic curves
   13.1 Affine varieties and affine curves .......................... 91
   13.2 An example -Elliptic curve .................................. 92
   13.3 An example of singular algebraic curve ...................... 94
Part I

Galois theory
Chapter 1

Field extension

1.1 Field extension and examples

Definition 1.1.1. A field is a commutative division ring. The smallest natural number $p$ such that summation of $p$ copies of 1 yields 0 is called the characteristic of the field. Since a field contains no zero divisor, then such a $p$, if it exists, must be a prime integer. If there is no such natural number exists, the field is said to have characteristic 0. Give a field $F$, we use $|F|$ to denote the cardinality of $F$.

Example 1.1.1. Let $\mathbb{Q}$ be the set of all rational numbers, then $\mathbb{Q}$ is a field.

Example 1.1.2. $\mathbb{Z}/5\mathbb{Z} = \{0, 1, 2, 3, 4\}$ is a field. In particular, $\bar{a} + \bar{b} = \bar{a+b}$, and $\bar{a\bar{b}} = \bar{ab}$. Given $\bar{a} \in \mathbb{Z}/5\mathbb{Z}$ such that $\bar{a} \neq \bar{0}$. Pick any representative $a$ for $\bar{a}$ in $\mathbb{Z}$. It is easy to see $a$ is coprime to 5. Then there exist two integers $s$ and $t$ such that $as + 5t = 1$. Modulo 5, we have $\bar{as} = 1$ and $(\bar{a})^{-1} = \bar{s}$.

In general, given any prime number $p$, the ring $\mathbb{Z}/p\mathbb{Z}$ is a field with $p$ elements. We denote such a field by $\mathbb{F}_p$. Such a field is called a prime finite field.

Example 1.1.3. $\mathbb{Z}/10\mathbb{Z}$ is not a field as $\bar{2}$ is a zero divisor.

Example 1.1.4. Let $i$ be a primitive 4th root of unity such that $i^2 = -1$. The set $\{a + bi \mid a, b \in \mathbb{Q}\}$ is a vector space over $\mathbb{Q}$ of dimension 2. This set is a field. We only need to check every non-zero element is a unit. Given any $a, b \in \mathbb{Q}$ which are not simultaneously zero, then $(a + bi) \frac{a - bi}{a^2 + b^2} = 1$. Hence $a + bi$ is a unit. This field is denoted by $\mathbb{Q}(i)$. 
**Example 1.1.5.** Let $i$ as above, then the set $\{a + bi \mid a, b \in \mathbb{F}_5\}$ is not a field. It is because $(2 + i)(2 - i) = 0$.

**Exercise 1.1.1.** Let $S$ be an element such that $S^2 = -3$. Prove that $\{a + bS \mid a, b \in \mathbb{F}_5\}$ is a field. It is a field with $5^2$ elements, denoted $\mathbb{F}_5(S)$ or $\mathbb{F}_{5^2}$.

**Remark 1.1.1.** The difference between these two cases is that $x^2 = -1$ has two solutions in $\mathbb{F}_5$. However, there is no solution of $x^2 = -3$ in $\mathbb{F}_5$.

**Definition 1.1.2.** A field $F$ is called an extension (field) of the field $K$ if $F$ contains $K$ as a subfield. If $F$ is an extension of $K$, their relation is denoted by $F/K$. The degree of the field extension of $F$ over $K$, denoted by $[F : K]$ is the dimension of $F$ as a $K$-vector space. When $[F : K] < \infty$, $F$ is called a finite extension of $K$.

**Example 1.1.6.** The field $\mathbb{Q}(i)$ is a degree 2 extension of the field $\mathbb{Q}$.

**Example 1.1.7.** Any finite field $\mathbb{F}$ must have characteristic $p$ greater than 0. Hence $\mathbb{F}$ must contains $\mathbb{F}_p$ as a subfield.

**Example 1.1.8.** The field $\mathbb{F}_{5^2}$ is a degree 2 extension of $\mathbb{F}_5$.

**Remark 1.1.2.** Don’t confuse the ring $\mathbb{Z}/25\mathbb{Z}$ and the field $\mathbb{F}_{5^2}$. $\mathbb{Z}/25\mathbb{Z}$ is not even an integral domain.

**Proposition 1.1.1.** Let $F$ be a finite field with characteristic $p$. Then the cardinality of $F$ is a power of $p$.

**Proof.** Since $\mathbb{F}_p$ is a subfield of $F$ and hence $|F| = p^{|\mathbb{F}_p|}$. \qed

**Definition 1.1.3.** Let $R$ be a commutative integral domain with units, the set $\left\{ \frac{a}{b} \mid a, b \in R, b \neq 0 \right\}$ is a field. It is called the field of rational functions of $R$.

Let $F$ be a field and $x$ an indeterminant. Then the polynomial ring $F[x]$ is an integral domain. The quotient field of this ring, denoted by $F(x)$, is the set $\{ \frac{f(x)}{g(x)} \mid f(x), g(x) \in F[x], g(x) \neq 0 \}$.

**Exercise 1.1.2.** Let $F$ be a field and $x$ an indeterminant. Check that $F[x]$ is an integral domain and a principal ideal domain (P.I.D.).

**Example 1.1.9.** The field $\mathbb{Q}(x)$ is an extension of $\mathbb{Q}$ as every rational number is a constant function. $[\mathbb{Q}(x) : \mathbb{Q}] = \infty$.

\[^1\text{We will see all fields with 25 elements are isomorphic.}\]
The ring \( \mathbb{Q}[x] \) is a principle ideal domain. The polynomial \( x^2 + 1 \) is irreducible over \( \mathbb{Q} \). Hence the ideal \((x^2 + 1)\) is a prime ideal and hence a maximal one.

**Exercise 1.1.3.** The quotient \( \mathbb{Q}[x]/(x^2 + 1) \) is isomorphic to \( \mathbb{Q}(i) \).

**Theorem 1.1.1.** Let \( F \) be a field extension of \( E \) and let \( E \) be a field extension of \( K \). Then \( F \) is an extension of \( K \) and \([F : K] := [F : E][E : K] \). \([F : K] < \infty \) if and only if \([F : E] < \infty \) and \([E : K] < \infty \).

**Proof.** When \([F : K] < \infty \), then \( F \) is an \([F : E] \) dimensional vector space over \( E \) and \( E \) is an \([E : K] \) dimensional vector space over \( K \). Hence \( F \) is an \([F : K] = [F : E][E : K] \) dimensional vector space over \( K \). \( \square \)

**Exercise 1.1.4.** Let \( F := \{ a + \sqrt{2}b + \sqrt{3}c \mid a, b, c \in \mathbb{Q}(i) \} \). Prove that \( F \) is a field and \([F : \mathbb{Q}] = 6 \).

If \( F \) is an extension of the field \( K \) and \( X \) is a set in \( F \). Then we let \( K(X) \) (resp. \( K[X] \)) denote the intersection of all sub fields(subrings) of \( F \) which contain \( X \cup K \). To be more explicitly, if \( X \) is a finite set \( \{ u_1, u_2, \ldots, u_n \} \) then we write \( F(X) = F(u_1, \ldots, u_n) \) (resp. \( F[X] = F[u_1, \ldots, u_n] \)). If \( X = \{ u \} \), then \( X(u) \) is said to be a simple extension of \( K \). It is easy to see that the order of the elements \( u_i \) does not matter. Moreover, \( F(u_1, \ldots, u_{n-1})(u_n) = F(u_1, u_2, \ldots, u_n) \) (resp. \( F[u_1, \ldots, u_{n-1}][u_n] = F[u_1, u_2, \ldots, u_n] \)).

**Example 1.1.10.** Let \( X = \{ \sqrt{-3}, \sqrt{-2} \} \). Please describe \( \mathbb{F}_5(\sqrt{-3}, \sqrt{-2}) = \mathbb{F}_5(\sqrt{-3})(\sqrt{-2}) = \mathbb{F}_{5^2}(\sqrt{-2}) \). Now we would like to check whether \( \sqrt{-2} \) is in the field \( \mathbb{F}_{5^2} \) or not. This is equivalent to say we would like to know whether \( x^2 + 2 = 0 \) has any solution in \( \mathbb{F}_{5^2} \). We can check \( \pm 2\sqrt{-3} \) are the two solutions of this equation. Hence \( \mathbb{F}_5(\sqrt{-3}, \sqrt{-2}) = \mathbb{F}_5(\sqrt{-3}) = \mathbb{F}_5(\sqrt{-2}) \).

**Theorem 1.1.2.** If \( F \) is an extension field of \( K \), \( u, u_i \in F \), and \( X \subseteq F \), then

1. the subring \( K[u] \) consists of all elements of the form \( f(u) \) where \( f \) is a polynomial with coefficients in \( K \).

2. the subring \( K[u_1, \ldots, u_m] \) consists of all elements of the form \( g(u_1, \ldots, u_m) \) where \( g \in K[x_1, \ldots, x_n] \).

3. the subring \( K[X] \) consists of all elements of the form \( h(u_1, \ldots, u_n) \) where \( u_i \in X, n \) a positive integer, and \( h \in K[x_1, \ldots, x_n] \).
4. the subfield $K(u)$ (resp. $K(u_1, ..., u_m)$, $K(X)$) is the quotient field of the ring $K[u]$ (resp. $K(u_1, ..., u_m)$, $K[X]$).

Proof. We will only show the proof of 1 and it can be generalized to prove statement 2, 3, and 4.

1. All elements of the form $f(u)$ where $f(x) \in K[x]$ form a ring, denoted by $R'$. Since $K[u]$ is a ring contains $K \cap \{u\}$, hence it contains $R'$. Since $K \cap \{u\} \subset R'$, and $K[u]$ is the smallest ring contains $K \cap \{u\}$, hence $K[u] \subseteq R'$. So $R' = K[u]$.

Exercise 1.1.5. Let $X = \{i\}$. We have described before $\mathbb{Q}(i)$ (resp. $\mathbb{F}_5(\sqrt{-3})$) as a vector space over $\mathbb{Q}$ (resp. $\mathbb{F}_5$). Please describe the rings $\mathbb{Q}[i]$ and $\mathbb{F}_5[\sqrt{-3}]$. How about the field $\mathbb{Q}(i, \sqrt{2})$ and the ring $\mathbb{Q}[i, \sqrt{2}]$?

If $L$ and $M$ are subfields of a field $F$, the composite of $L$ and $M$ in $F$, denoted by $LM$ is the subfield generated by the set $L \cup M$.

Example 1.1.11. The composite of $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{2})$ is the field $\mathbb{Q}(i, \sqrt{2}) = \mathbb{Q}(\sqrt{2} + i)$.

Definition 1.1.4. Let $F$ be an extension field of $K$. An element $u$ of $F$ is said to be algebraic over $K$ provided that $u$ is a root of some nonzero polynomial $f \in K[x]$. An irreducible monic polynomial in $K[x]$ of degree $n \geq 1$ uniquely determined by the conditions that $f(u) = 0$ is called the minimal polynomial of $u$.

If $u$ is not a root of any nonzero $f \in K[x]$, $u$ is said to be transcendental over $K$. $F$ is said to be an algebraic extension of $K$ if every elements of $F$ is an algebraic extension over $K$. $F$ is said to be a transcendental extension extension if at least one element of $F$ is transcendental over $K$.

Remark 1.1.3. It is a nontrivial fact that $\pi, e \in \mathbb{R}$ are transcendental over $\mathbb{Q}$. For proofs, please refer to [Jac85]

Theorem 1.1.3. Let $F$ be an extension field of $K$ and $E$ the set of all elements of $F$ which are algebraic over $K$. Then $E$ is a subfield of $F$.

Proof. Let $u$ and $v$ in $F$ be algebraic over $K$, then $K(u - v) \subset K(u, v) = K(u)(v)$ and if $v \neq 0$ $K(u^{-1}v) \subset K(u, v)$. Hence $u + v$ and $uv$ are also algebraic over $K$. Hence the set of all elements of $F$ which are algebraic over $K$ form a subfield.
Theorem 1.1.4. If $F$ is an extension field of $K$ and $u \in F$ is transcendental over $K$, then the field $K(u)$ is isomorphic to $K(x)$ where $x$ is an indeterminate.

Proof. The map $f(u) \mapsto f(x)$ gives the isomorphism. \hfill \Box

Theorem 1.1.5. If $F$ is an extension field of $K$ and $u \in F$ is algebraic over $K$, then

1. $K(u) = K[u].$
2. $K(u) \cong K[x]/(f)$ where $f$ is the minimal polynomial of $u$. Then $g(u) = 0$ if and only if $f$ divides $g$.
3. $[K(u) : K] = n.$
4. $\{1, u, \ldots, u^{n-1}\}$ is a basis of $K(u)$ over $K$.

Proof. Let $\phi : K[x] \rightarrow K[u]$ be the map sending $g(x)$ to $g(u)$. The kernel is generated by a single element $f$ since $K[x]$ is a P.I.D. Hence if there is any other polynomial $g$ such that $g(u) = 0$. Then $g \in \text{Ker}\phi$. Hence $f|g$. Now we claim $\{1, u, \ldots, u^{n-1}\}$ are linearly independent over $K$. Since $K[u]$ is an integral domain, and $K[x]/(f) \cong K[u]$, hence $(f)$ is a prime ideal and hence a maximal ideal. So $K[u]$ is a field.

The field $K(u)$ is the quotient field of $K[u]$. So $K[u] \subset K(u)$. On the other hand, $K(u)$ is the smallest field which contains $K$ and $u$. Hence $K(u) \subset K[u]$. Hence $K(u) = K[u]$. \hfill \Box

Corollary 1.1.1. Let $f(x)$ be a monic irreducible polynomial in $F[x]$. Let $u$ be any solution of $f(x) = 0$. Then $F(u)$ is isomorphic to $F[x]/(f(x))$.

Exercise 1.1.6. How many degree 2 irreducible polynomials in $\mathbb{F}_2$. How about degree $n$ then?

Exercise 1.1.7. $f(x) = x^3 + x^2 - 1$ is irreducible in $\mathbb{F}_5$. Let $u$ be a root of the equation $f(x) = 0$. Please write $u^4 + 1$ as a linearly combination of $\{1, u, u^2\}$ over $\mathbb{F}_5$. Please find the inverse of $u^2 + 1$ in $\mathbb{F}_5(u)$.

Exercise 1.1.8. Let $E = F(u)$ where $u$ is algebraic of odd degree. Show that $E = F(u^2)$.

Proof. $F(u^2)$ is a subfield of $F(u)$. Hence $[F(u) : F(u^2)] [F(u^2) : F] = [F(u) : F]$. Hence $[F(u^2) : F(u)]$ is either 1 or 2 and $[F(u) : F]$ is odd. Hence $[F(u^2) : F(u)] = 1$ and $[F(u^2) : F] = [F(u) : F]$. \hfill \Box
1.2 Simple extension

**Theorem 1.2.1.** If $F$ is a finite extension of the field $K$, then $F$ is finitely generated and algebraic over $K$.

*Proof.* Suppose $[F : K] = n < \infty$. Let \{u_1, \ldots, u_n\} be a basis of the $n$-dimensional vector space $F$ over $K$. Then $F = K(u_1, \ldots, u_n)$. Given any $u \in F$, $1, u, \ldots, u^n$ is linearly dependent over $K$. Hence $u$ is algebraic over $K$.

**Exercise 1.2.1.** Let $E$ be an extension field of the field $F$ such that i) $[E : F] < \infty$, and ii) for any two subfields $E_1$ and $E_2$ containing $F$, either $E_1 \supset E$ or $E_2 \supset E_1$. Show that $E$ has a primitive element over $F$.

*Proof.* We prove it by contradiction. Suppose $E$ is not a simple extension over $F$, then for any $u \in E$, $F(u) \subsetneq E$. Now we fix the choice for $u$ such that the index $[F(u) : F]$ obtains the maximum among all choice $u \in E$. is Pick $v \in E$ such that $v \notin F(u)$. Then we have either $F(v) \subseteq F(u)$ or $F(u) \subseteq F(v)$ by the assumption. The first circumstance won’t happen as $v \notin F(u)$ and the second circumstance implies $[F(v) : F] > [F(u) : F]$ which contradicts the choice of $u$. Hence $E$ is a simple extension. □

We will like to method a corollary of this exercise. However, to prove it we will need more properties of finite fields that we will obtain later.

**Corollary 1.2.1.** Any finite field is a simple extension over its prime field.

**Example 1.2.1.** In the field $\mathbb{C}$, $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{2})$ are isomorphic as vector spaces (both are 2-dimensional $\mathbb{Q}$ spaces), but not as fields. To prove $\mathbb{Q}(i, \sqrt{2}) = \mathbb{Q}(i + \sqrt{2})$.

*Proof.* As vector spaces, they are both two dimensional over $\mathbb{Q}$. Hence they are isomorphic. But as fields, if there is a field isomorphism $\phi : \mathbb{Q}(i) \rightarrow \mathbb{Q}(\sqrt{2})$ then the image of $\phi(i) = a + b\sqrt{2}$ satisfies that $(a + b\sqrt{2})^2 = -1$. This is impossible. Hence as fields they are not isomorphic. To prove the second statement, we first see that

$$(x - (i + \sqrt{2}))(x - (i - \sqrt{2}))(x - (-i + \sqrt{2}))(x - (-i - \sqrt{2})) = x^4 - 2x^2 + 9.$$ 

Hence $i + \sqrt{2}$ is a root of the over $\mathbb{Q}$ irreducible polynomial $x^4 - 2x^2 + 9$. By theorem 1.1.5, $[\mathbb{Q}(i + \sqrt{2}) : \mathbb{Q}] = 4$. Hence $(i + \sqrt{2}) + (i - \sqrt{2}) = 2i \in \mathbb{Q}(i + \sqrt{2})$. Similarly, $\sqrt{2} \in \mathbb{Q}(i + \sqrt{2})$. Hence $\mathbb{Q}(i, \sqrt{2}) = \mathbb{Q}(i + \sqrt{2})$. □
The next theorem indeed holds for any field which contains only infinitely many elements. But we will state and prove it for a specified case only.

If \( F \) is a finite extension of the field \( \mathbb{Q} \), then \( F \) is called an algebraic number field, or simply a number field.

Example 1.2.2. The fields \( \mathbb{Q}(i) \), \( \mathbb{Q}(\sqrt{2}, i) \) are algebraic number field.

Theorem 1.2.2. Let \( F \) be an algebraic number field. Then \( F \) is a simple extension of \( \mathbb{Q} \). In other words, there exists an element \( u \in F \) such that \( F = \mathbb{Q}(u) \).

Proof. Since \( [F : \mathbb{Q}] < \infty \), \( F \) is finitely generated over \( \mathbb{Q} \). By induction, it is sufficient to prove given any two \( u_1, u_2 \in F \), there exists an element \( u \in F \) such that \( K(u_1, u_2) = K(u) \). Let \( f, g \in \mathbb{Q}[x] \) be two relatively prime polynomials. Suppose \( \alpha_1, \ldots, \alpha_n \) and \( \beta_1, \ldots, \beta_m \) are the roots of these two polynomials respectively. Since they are relatively prime, they have no repeated roots. Choose \( t \in \mathbb{Q} \) such that \( a_i + t\beta_j \neq \alpha_1 + t\beta_1 \) for all \( j \neq 1 \) and all \( i \). Let \( u = \alpha_1 + t\beta_1 \). Consider \( f(u - tx) \). It is easy to see the solutions are \( u - tx = \alpha_i \). I.e. \( x = (\alpha_1 + t\beta_1 - \alpha_i)/t \). Hence the common roots of \( g(x) \) and \( f(u - tx) \) is \( \beta_1 \). On the other hand, the greatest common divisor of \( f(u - tx) \) and \( g(x) \), which is \( x - \beta_1 \), is a polynomial in \( \mathbb{Q}(u)[x] \) by the Euclidean algorithm. Hence \( \beta_1 \in \mathbb{Q}(u) \) and \( \alpha_1 = u - t\beta_1 \in \mathbb{Q}(u) \). Hence \( \mathbb{Q}(u) \subset \mathbb{Q}(\alpha_1, \beta_1) \subset \mathbb{Q}(u) \). \( \square \)
Chapter 2

Galois groups of field extensions

2.1 Field isomorphism

Suppose $E$ is an extension of $K$ and $F$ is an extension of field $L$, and $\sigma : K \to L$ is an isomorphism of fields. We will consider here under what condition $\sigma$ can be extended to an isomorphism from $E$ to $F$?

**Theorem 2.1.1.** Let $\sigma : K \to L$ be an isomorphism of fields, $u$ an element of some extension field of $K$ and $v$ an element of some extension field of $L$. Assume either

1. $u$ is transcendental over $K$ and $v$ is transcendental over $L$; or
2. $u$ is a root of an irreducible polynomial $f \in K[x]$ and $v$ is a root of $\sigma f \in L[x]$.

then $\sigma$ extends to an isomorphism of fields $K(u) \cong L(v)$ which maps $u$ to $v$.

**Proof.** In case 1, it is obvious as $K(u) \cong K[x]$.

In case 2, since $\sigma : K \to L$ is an isomorphism, the induced map

$$
\begin{align*}
K[x]/(f) & \to L(x)/(\sigma f) \\
g + (f) & \mapsto \sigma(g) + (\sigma f)
\end{align*}
$$

is also an isomorphism when $f$ is irreducible. $\square$
Corollary 2.1.1. Let $E$ and $F$ each be extension fields of $K$ and let $u \in E$ and $v \in F$ be algebraic over $K$. Then $u$ and $v$ are roots of the same irreducible polynomials $f \in K[x]$ if and only if there is an isomorphism of field $K(u) \cong K(v)$ which sends $u$ onto $v$ and is the identity on $K$.

Proof. “$\Rightarrow$” follows from theorem 2.1.1 when $\sigma = 1_K$.

“$\Leftarrow$” Let $\sigma : K(u) \cong K(v)$ be the isomorphism. Suppose the minimal irreducible polynomial satisfy by $u$ is $f = \sum_{0 \leq i \leq n} a_i x^i$. Then $\sigma a_i u^i = a_i v^i = 0$. Hence $v$ is also a root of the irreducible polynomial $f$.

Theorem 2.1.2. If $K$ is a field and $f \in K[x]$ polynomial of degree $n$, then there exists a simple extension field $F = K(u)$ of $K$ such that

1. $u \in F$ is a root of $f$;
2. $[K(u) : K] \leq n$, with equality holding iff it is irreducible in $K[x]$;
3. if $f$ is irreducible in $K[x]$, then $K(u)$ is unique up to an isomorphism which is the identity on $K$.
4. the number of such an extension is the same as the number of distinct roots of $f$.

Proof. Let $u$ be a root of $f$, then $[K(u) : K] \leq n$ as $1, u, \ldots, u^n$ are linearly dependent. If $f$ is irreducible, iff $1, u, \ldots, u^{n-1}$ are linearly independent, hence $[K(u) : K] = n$. The last two claims follow from the previous corollary.

This theorem explains why we later need to consider multiple roots and simple roots separately.

2.2 Splitting fields of a polynomial

Definition 2.2.1. Let $F$ be a field, $f(x)$ a monic polynomial in $F[x]$. Then an extension $E/F$ is called a splitting field over $F$ of $f(x)$ if

1. $f(x) = (x - r_1) \cdots (x - r_n)$ in $E[x]$ and
2. $E = F(r_1, \ldots, r_n)$, that is $E$ is generated by the roots of $f(x)$.
2.2. SPLITTING FIELDS OF A POLYNOMIAL

Example 2.2.1. Let \( f = x^3 - 1 \) and \( \omega \) a primitive cubic root of one. Then the splitting field of \( f \) over \( \mathbb{Q} \) is \( \mathbb{Q}(\omega) \).

Example 2.2.2. Let \( f = x^3 - 2 \). Then the splitting field of \( f \) over \( \mathbb{Q} \) contains \( \sqrt[3]{2}, \sqrt[3]{2}\omega \), where \( \omega = \frac{-1+\sqrt{3}}{2} \). Hence the splitting field of \( f \) is \( \mathbb{Q}(\sqrt[3]{2}, \omega) \).

Example 2.2.3. Let \( F = \mathbb{F}_2 \), and \( f = x^3 + x + 1 \). \( f \) is irreducible over \( \mathbb{F}_2 \). Put \( r_1 = x + (f(x)) \in F[x]/(f) \) so \( F(r_1) \) is a field and \( x^3 + x + 1 = (x+r_1)(x^2+ax+b) \in F(r_1)[x] \). Moreover, we can check that \( a = r_1, b = 1+r_1^2 \).

The element of \( F(r_1) \) can be written as \( c + dr_1 + er_1^2 \), where \( c, d, e \in F \). Substituting these in \( x^2 + r_1x + 1 + r_1^2 \) we get \( (r_1^2)^2 + r_1(r_1^2) + 1 + r_1^2 = r_1^4 + r_1^3 + 1 + r_1^2 = 0 \) as since \( r_1^3 = r_1 + 1 \) and \( r_1^4 = r_1^2 + r_1 \). Hence \( E = F(r_1) \) is the splitting field of \( x^3 + x + 1 \).

Example 2.2.4. Let \( F = \mathbb{Q} \) and let \( f = x^p - 1 \). The degree of its splitting field over \( \mathbb{Q} \) is \( p - 1 \).

Proof. Let \( \mu_p = e^{2\pi i/p} \), then in \( \mathbb{Q}(\mu_p) \),

\[
x^p = \prod_{i=1}^{p} (x - \mu_p^i).
\]

\[\square\]

Theorem 2.2.1. Any monic polynomial \( f(x) \in F[x] \) of positive degree has a splitting field \( E/F \).

Proof. We prove it by induction. Suppose the statement is true for any polynomial of degree \( < n \). Let \( f \) be a monic irreducible polynomial of \( F[x] \). Let \( u \) be a solution of \( f \), then let \( E' = F(u) \) be an intermediate field. Then, \( f \) factors over \( E' \) as several irreducible components, and each component has degree less than \( n \). By our assumption, each component has a splitting field then the composition of splitting fields obtained above is a splitting field for \( f \). \[\square\]

Theorem 2.2.2. Let \( f(x) \) be a polynomial over a field \( F \). Splitting fields for \( f(x) \) are \( F \)-isomorphic.

Proof. We use Proposition 1.1.5. \[\square\]
2.3 Multiple roots

We factor $f(x)$ in its splitting field as

$$f(x) = (x - r_1)^{k_1} \cdots (x - r_s)^{k_s}$$

so that $k_i > 0$ and $r_i \neq r_j$ if $i \neq j$. We call $k_i$ the multiplicity of the root $r_i$. If $k_i = 1$ then $r_i$ is called a simple root.

**Lemma 2.3.1.** Let $f(x)$ be a monic polynomial of positive degree in $F[x]$. Then all the roots of $f$ in any splitting field $E/F$ are simple if and only if $\gcd(f, f')$ has degree 0.

**Proof.** Let $f(x) = (x - r_1)^{k_1} \cdots (x - r_s)^{k_s}$, then

$$f' = \sum_{i=1}^{s} k_i (x - r_1)^{k_1 - 1} \cdots (x - r_i)^{k_i - 1} \cdots (x - r_s)^{k_s} \in F[x]$$

and

$$(x - r_1)^{k_1 - 1} \cdots (x - r_s)^{k_s - 1} \mid \gcd(f, f')$$

So $\gcd(f, f')$ has degree 0 iff $k_i = 1$ for $i = 1, \ldots, s$. □

**Corollary 2.3.1.** If $f(x)$ is an irreducible polynomial with degree at least 1, then $\gcd(f, f')$ has degree greater than 0 iff $f' = 0$.

It is easy to see that every irreducible polynomial over a characteristic 0 field has only simple roots.

**Corollary 2.3.2.** Let $F$ be a field with characteristic $p > 0$. Let $f(x)$ be an irreducible polynomial with degree at least 1. Then $f' = 0$ iff $f(x) = \sum_{i=1}^{n} a_i x^{pi}$.

In a characteristic $p$ case (odd or even), we have

$$ (x + y)^p^e = x^{p^e} + y^{p^e} \quad (2.1)$$

$$ (x - 1)^{p^e} = x^{p^e} - 1 = (x - 1)^{p^e}. \quad (2.2)$$

**Exercise 2.3.1.** Determine a splitting field over $\mathbb{F}_p$ of $x^{p^e} - 1$ for any natural number $e$.

**Solution:** The splitting field is $\mathbb{F}_p$ itself as $x^{p^e} - 1 = (x - 1)^{p^e}$. 
Lemma 2.3.2. If $F$ has characteristic $p > 0$ and $a \in F$, then $x^p - a$ is either irreducible in $F[x]$ or it is a $p$th power in $F[x]$.

Proof. If $x^p - a$ is not irreducible, then $\gcd(f, f') = f$. Suppose $(x^p - a) = g(x)h(x)$ where $g(x)$ is monic of degree $k$ and $1 \leq k \leq p - 1$. Let $E$ be a splitting field over $F$ of $x^p - a$ and let $b \in E$ be a root of $g$. Then $b^p = a$. Hence $x^p - a = x^p - b^p = (x - b)^p = g(x)h(x)$. Hence $g(x) = (x - b)^k$ and $b^k \in F$. Since $k$ and $p$ are coprime, there exist $u$ and $v$ such that $uk + vp = 1$, hence $b = (b^k)^u(b^p)^v \in F$.

Example 2.3.1. Let $F = \mathbb{F}_p(t)$ be a function field, we claim that $t$ is not a $p$th power in this field. If yes, we have $t = (f(t)/(gt))^p$ where $f(t) = a_0 + a_1t + \cdots + a_nt^n$ and $g(t) = b_0 + \cdots + b_mt^m$. Hence we have

$$(b_0^p + b_1t^p + \cdots + b_mt^mp)t = a_0^p + a_1^pt^p + \cdots + a_n^pt^n$$

However, $1, t, t^2, \ldots$ are independent over $\mathbb{F}_p$. Hence all $b_i = 0$, impossible. Now let $f(x) = x^p - t$, it is irreducible over $\mathbb{F}_p$. Let $E$ be the splitting field of $f$. Then $f$ has multiple roots as $f'(x) = 0$.

Definition 2.3.1. A polynomial in $F[x]$ is separable if its irreducible factors have distinct roots. A field is said to be perfect if every irreducible polynomial in $F[x]$ is separable.

By Lemma 2.3.1, any field with characteristic 0 is perfect. We will now discuss when a field with characteristic $p$ is perfect.

Theorem 2.3.1. A field $F$ of characteristic $p \neq 0$ is perfect if and only if $F = F^p$, the field of $p$th powers of the elements of $F$.

Proof. If $F \neq F^p$, then there is an $a \in F - F^p$. Then $f(x) = x^p - a$ is irreducible and have multiple roots. Hence $F$ is not perfect. If let $f(x)$ be an inseparable irreducible polynomial in $F[x]$. Then $(f(x), f'(x)) \neq 1$ and this implies that $f(x) = a_0 + a_1x^p + a_2x^{2p} + \cdots$ and one of these $a_i$ is not a $p$th root. For otherwise, $f(x)$ will be a $p$th power, contrary to the irreducibility of $f(x)$. Hence $F \neq F^p$.

Corollary 2.3.3. Every finite field $\mathbb{F}$ is perfect.
Proof. Since $x^p = y^p$ implies $(x - y)^p$, the map
\[
F \rightarrow \mathbb{F}^p \\
x \mapsto x^p
\]
is one to one and hence is also an isomorphism.

Exercise 2.3.2. Let $F$ be imperfect of characteristic $p$. Show that $x^p - a$ is irreducible if $a \not\in F^p$.

Proof. If $x^p - a = (x - \alpha)^p = f(x)g(x)$ with $\deg f > 0, \deg g > 0$. I.e. $f(x) = (x - \alpha)^{p^i} \in F[x]$. Hence $\alpha^{p^i} \in F$ and $\alpha^{p^i - n_1} \in F$. Let $p_i = (p^i, n_1)$ then $i < n$. By the Euclidean algorithm we know $\alpha^{p_i} \in F$. Hence $\alpha^{p^i - 1} \in F$. I.e. $a \in F^p$.

2.4 Algebraic closure

Theorem 2.4.1. The following conditions on a field are equivalent.

1. Every nonconstant polynomial $f \in F[x]$ has a root in $F$;

2. every nonconstant polynomial $f \in F[x]$ splits over $F$; every irreducible polynomial in $F[x]$ has degree 1;

3. there is no algebraic extension field of $F$ (except itself);

4. there exists a subfield $K$ of $F$ such that $F$ is algebraic over $K$ and every polynomial in $K[x]$ splits in $F[x]$.

A field that satisfies the equivalent conditions of theorem 2.4.1 is said to be algebraically closed.

Example 2.4.1. The field of complex numbers is algebraically closed as every nonconstant polynomial $f(x) \in \mathbb{C}[x]$ has at least a root in $\mathbb{C}$.

Theorem 2.4.2. If $F$ is an extension field of $K$, then the following conditions are equivalent.

1. $F$ is algebraic over $K$ and $F$ is algebraically closed;

2. $F$ is a splitting field over $K$ of the set of all polynomials in $K[x]$. 
Any extension field $F$ of a field $K$ that satisfies the equivalent conditions of theorem 2.4.2 is called an algebraic closure of $K$.

**Theorem 2.4.3.** Every field $K$ has an algebraic closure. Any two algebraic closure of $K$ are $K$-isomorphic.

**Proof.** C.f. Theorem 3.6 Page 259 of Hungerford [Hun80].

**Example 2.4.2.** Let $\overline{\mathbb{Q}}$ denote an algebraic closure of $\mathbb{Q}$, then $\overline{\mathbb{Q}} \subseteq \mathbb{C}$ as by the above theorem $\overline{\mathbb{Q}}$ does not contain any transcendental elements over $\mathbb{Q}$.

### 2.5 Galois groups

Let $E$ be an extension of a field $F$ and let $G$ be the set of automorphisms of $E$ which fix $F$; that is the set of automorphisms $\eta$ of $E$ such that $\eta(a) = a$ for all $a \in F$. We also called such an automorphism of $E$ to be an $F$-automorphism of $E$. The set of $F$-automorphisms form a group $G$ and is called the Galois group of $E$ over $F$, denoted by Gal($E/F$).

**Example 2.5.1.** Let $E = F(u)$ where $u^2 = a \in F$ and $a$ is not a square. The $\{1, u\}$ is a basis for $E$ over $F$. Gal($E/F$) = $< \sigma >$ is of order 2 where $\sigma(a + bu) = a - bu, a, b \in F$.

**Exercise 2.5.1.** Find the Galois group Gal($\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$).

**Solution:** We have discussed in section 1.2 that $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is a simple extension. Explicitly, $E = \mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$. The minimal polynomial of $\sqrt{2} + \sqrt{3}$ is given by

$$(x - \sqrt{2} + \sqrt{3})(x - \sqrt{2} + \sqrt{3})(x - \sqrt{2} + \sqrt{3})(x - \sqrt{2} + \sqrt{3}) = x^4 - 10x^2 + 1$$

There are 4 $\mathbb{Q}$-automorphisms of $E$ which are specified by

$\sigma_1(\sqrt{2} + \sqrt{3}) = \sqrt{2} + \sqrt{3}, \sigma_2(\sqrt{2} + \sqrt{3}) = \sqrt{2} - \sqrt{3},$

$\sigma_3(\sqrt{2} + \sqrt{3}) = -\sqrt{2} + \sqrt{3}, \sigma_4(\sqrt{2} + \sqrt{3}) = -\sqrt{2} - \sqrt{3}.$

Indeed the Galois group Gal($E/\mathbb{Q}$) = $< \sigma_2, \sigma_3 > = \mathbb{Z}_2 \oplus \mathbb{Z}_2$.

**Example 2.5.2.** Let $F$ be imperfect of characteristic $p$ and let $a \in F - F^p$. Then exercise 2.3.2 says $f(x) = x^p - a$ is irreducible. Moreover

$$x^p - a = (x - u)^p.$$ Let $E$ be a splitting field of $f(x)$. So the Galois group Gal($E/F$) = 1.
Example 2.5.3. Let $F$ be a field and let $E = F(t)$ where $t$ is transcendental over $E$. Any automorphism $\sigma$ will send $t$ to another generator of the field extension $u$ of $E/F$. Moreover, $u$ is a generator of $E/F$ if and only if

$$u = \frac{at + b}{ct + d}, \quad ad - bc \neq 0.$$  

Hence $\text{Gal}(E/F) = PGL_2(F)$ where $PGL_2(F)$ is the group of invertible $2 \times 2$ matrices with entries in $F$ modulo nonzero scalar matrices.

Exercise 2.5.2. Let $E$ be a splitting field of $x^3 - 2$ over $\mathbb{Q}$. Prove that the Galois group $\text{Gal}(E/F)$ is isomorphic to $S_3$.

Now let $G$ be any group of automorphisms of a field $E$. Let

$$\text{Inv}G = \{a \in E \mid g(a) = a, g \in G\}$$

i.e. $\text{Inv}G$ are the set of elements of $E$ which are not moved by any $g \in G$. Then from

$$g(a + b) = g(a) + g(b), \quad g(ab) = g(a)g(b), \quad g(1) = 1, \quad g(a^{-1}) = g(a)^{-1},$$

we see that $\text{Inv}G$ is a subfield of $E$, called the $G$-invariants or $G$-fixed subfield of $E$.

Given two automorphism groups $G_1$ and $G_2$ of $E$ and two subfields $F_1$ and $F_2$ of $E$, according to the definitions above, it is easy to verify the following properties:

1. If $G_1 \supset G_2$, then $\text{Inv}G_1 \subset \text{Inv}G_2$;
2. $F_1 \supset F_2$, then $\text{Gal}(E/F_1) \subset \text{Gal}(E/F_2)$;
3. $\text{Inv}(\text{Gal}(E/F)) \supset F$;
4. $\text{Gal}(E/\text{Inv}G) \supset G$.

Theorem 2.1.2 implies

Lemma 2.5.1. Let $E/F$ be a splitting field of a separable polynomial contained in $F[x]$. Then $|\text{Gal}(E/F)| = [E : F]$. 

Lemma 2.5.2 (Artin’s Lemma). Let $G$ be a finite group of automorphisms of a field $E$ and let $F = \text{Inv}_G$. Then

$$[E : F] \leq |G|.$$  

Proof. Let $n = |G|$. We only need to show that any $m(> n)$ elements of $E$ are linearly dependent over $F$. Let $G = \{1, g_2, \ldots, g_m\}$ and let $u_1, \ldots, u_m$, be $m(> n)$ elements of $E$. Then by linear algebra we know the system of $n$

\[\sum_{i=1}^{m} g_i(u_j)x_i = 0\]  

(2.3)  

have nontrivial solutions. Suppose among all of them, $(a_1, \ldots, a_m)$ has the least number of nonzero entries. Without loss of generality, we may assume $a_1 = 1$. Now we claim all $a_i \in F$. If all $a_i \in \text{Inv}_G$ then it is done. If not, we suppose $a_i \notin \text{Inv}_G$. We may assume $g_k(a_2) \neq a_2$. Now we applied $g_k$ to the system (2.3) to get $\sum_{j=1}^{m} (g_k g_i)(u_j)g_k(b_j) = 0$. Since $(g_k g_1, \ldots, g_k g_n)$ is a permutation of $(g_1, \ldots, g_n)$, we know $(1, g_k(b_2), \ldots, g_k(b_m))$ is also a solution of (2.3). Hence $(0, b_2 - g_k(b_2), \ldots, b_m - g_k(b_m))$ is also a nontrivial solution (as the second entry $a_2 - g_k(a_2) \neq 0$) with even fewer nonzero entries than the original one. \hfill \Box

Exercise 2.5.3. Let $E = \mathbb{F}_p(t)$ where $t$ is transcendental over $\mathbb{F}_p$. Let $\sigma(t) = t + 1$ and $G = \langle \sigma \rangle$. Determine $F = \text{Inv}(G)$ and show that $[E : F] = p$.

Proof. Since the characteristic is $p$, so $\sigma^p = \text{id}$. Hence $|G| = p$. By Artin’s lemma $[E : \text{Inv}_G] \leq p$. Every $f(t) \in F_p[t]$ satisfies $f(t) = f(t + 1)$ implies that $f(t) - f(0)$ is a multiple of $g(t) = t(t-1) \cdots (t-p+1)$. Such a polynomial $g(t)$ is a minimal polynomial which is invariant under $G$. By induction, $f(t)$ is a polynomial of $g$. It follows that $\text{Inv}_G = \mathbb{F}_p(g)$.

Now we show $1, t, \ldots, t^{p-1}$ is linearly independent over $\text{Inv}_G$. If not there are $a_i(g) \in \mathbb{F}_p[g]$ such that $\sum_{i=1}^{p-1} a_i(g) t^i = 0$. We may assume that not every $a_i(g)$ is a multiple of $g$ (after dividing by a high enough power of $g$). Then $\sum_{i=1}^{p-1} a_i(g) t^i \mod g = 0$. After modulo by $g$, the left hand side is a degree at most $p - 1$ polynomial in $t$ which is won’t equal to zero, the right hand side. Hence $[E : \text{Inv}_G] \geq p$. Hence $[E : \text{Inv}_G] = p$. \hfill \Box

Definition 2.5.1. An extension $E/F$ is called normal (algebraic) extension if every irreducible polynomial in $F[x]$ which has a root in $E$ is a product of linear factors in $E[x]$. 
Example 2.5.4. Let be a root of $x^3 - 2$. Then $\mathbb{Q}(u)/\mathbb{Q}$ is not a normal extension. (As the splitting field of $x^3 - 2$ has degree 6 over $\mathbb{Q}$).

Exercise 2.5.4. Let $F$ be a field of characteristic $p$, $a$ an element of $F$ not of the form $b^p - b$, $b \in F$. Determine the Galois group over $F$ of a splitting field of $x^p - x - a$.

Solution: Let $f(x) = x^p - x - a$. Then $f'(x) = -1 \neq 0$. Hence $x^p - x - a$ only has simple roots. By the assumption on $a$, $x^p - x - a$ does not have any root over $F$. On the other hand, if $u$ is a root of $f(x)$, then $f(u + 1) = (u + 1)^p - (u + 1) - a = u^p - u - a = 0$. So $f(x) = (x - u)(x - u - 1) \cdots (x - u - p + 1)$. Hence $E = F(u)$ is a splitting field for $f(x)$. $\text{Gal}(E/F) = \langle \sigma \rangle$ where $\sigma(u) = u + 1$.

2.6 Galois extension

Theorem 2.6.1. Let $E$ be an extension field of a field $F$. Then the following conditions on $E/F$ are equivalent.

1. $E$ is a splitting field over $F$ of a separable polynomial $f(x)$.

2. $F = \text{InvG}$ for some finite group of automorphisms of $E$.

3. $E$ is finite dimensional normal and separable over $F$.

Moreover, if $E$ and $F$ are as in (1) and $G = \text{Gal}(E/F)$ then $F = \text{InvG}$ and if $G$ and $F$ are as in (2), then $G = \text{Gal}(E/F)$.

Proof. (1) $\Rightarrow$ (2). Let $G = \text{Gal}(E/F)$ and $F' = \text{InvG}$. Then $F'$ is a subfield of $E$ containing $F$. Hence $E$ is a splitting field over $F'$ of $f(x)$ as well as over $F$ and $G = \text{Gal}(E/F')$. Hence by lemma 2.5.1 we know $[F' : F] = 1$. It follows that $F = \text{Inv}(\text{Gal}(E/F'))$

(2) $\Rightarrow$ (3). By Artin’s lemma we have $[E : F] \leq |G|$, so $E$ is of finite dimensional over $F$. Let $f(x)$ be an irreducible polynomial in $F[x]$ having a root $r$ in $E$. Let $\{r_1, r_2, \ldots, r_m\}$ be the orbit of $r$ under the action of the group $G$. Thus this set is the set of distinct elements of the form $g(r)$. Hence if $\xi \in G$, then the set $((\xi(r_1), \ldots, \xi(r_m)))$ is a permutation of $(r_1, \ldots, r_m)$. We have $f(r) = 0$ which implies $f(r_i) = 0$. Then $f$ is divisible by $x - r_i$, $i = 1, \ldots, m$. Hence $f$ is divisible by $\prod_{i=1}^{m}(x - r_i)$. Since $\xi g(x) = g(x)$ for any $\xi \in G$, so the coefficients of $g(x)$ are $G$-invariant, i.e. $g(x) \in F[x]$. Hence
2.7. **FUNDAMENTAL THEOREM OF GALOIS THEORY**

Let $f(x) = g(x)$ (as $f$ is irreducible) is a product of distinct linear factors in $E[x]$. It follows $E$ is separable and normal over $F$ and (3) holds.

(3) $\Rightarrow$ (1). We assume $E = F(r_1, ..., r_k)$ where $r_i$ are all algebraic over $F$ with minimal polynomial $f_i(x)$. Then $E$ is the splitting field of $f = \prod_i f_i(x)$ and $f$ is separable.

Moreover, we know by Artin’s lemma that $[E : F] \leq |G|$ and $\text{Gal}(E/F) = [E : F]$. Since $G \subset \text{Gal}(E/F)$ and we know $G = \text{Gal}(E/F)$.

**Definition 2.6.1.** If an extension $E/F$ satisfies one (and hence all) of the above equivalent conditions, then $E$ is said to be *Galois over $F$.*

**Exercise 2.6.1.** Let $E = \mathbb{Q}(u)$ where $u$ is a root of $f(x) = x^3 + x^2 - 2x - 1 = 0$. Verify that $u' = u^2 - 2$ is also a root of $f(x) = 0$, Determine $\text{Gal}(E/\mathbb{Q})$ and show that $E$ is normal over $\mathbb{Q}$.

### 2.7 Fundamental theorem of Galois theory

**Theorem 2.7.1 (Fundamental theorem of Galois theory).** Let $E$ be a Galois extension field of a field $F$. Let $G = \text{Gal}(E/F)$. Let $\Gamma = \{H\}$, the set of subgroups of $G$, and $\Sigma$, the set of intermediate fields between $E$ and $F$. The maps $H \mapsto \text{Inv}_H, K \mapsto \text{Gal}(E/K), H \in \Gamma, K \in \Sigma$ are inverses and so are bijective. Moreover, we have the following

1. $H_1 \supset H_2 \Leftrightarrow \text{Inv}_{H_1} \subset \text{Inv}_{H_2}$;
3. $H$ is normal in $G \Leftrightarrow \text{Inv}_H$ is normal over $F$. In this case

\[
\text{Gal}(\text{Inv}_H/F) \cong G/H.
\]

**Proof.** The bijection between this two sets $\Gamma$ and $\Sigma$ follows from theorem 2.6.1. Claim 1) follows directly from the definition of $\text{Inv}_H$.


3). If $H \in \Gamma$ and $K = \text{Inv}_H$ is the corresponding invariants. Then for any $\gamma \in G$, $\text{Inv}_H \gamma^{-1} = \gamma(K)$. Hence $H$ is normal then for any $\gamma \in G, \gamma(\text{Inv}_H) = \text{Inv}_H$. Hence every $\gamma \in G$ maps $\text{Inv}_H$ to itself.
So we consider $\gamma|_{K=\text{Inv}H}$ which gives the restriction homomorphism from $\text{Gal}(E/F)$ to $\text{Gal}(\text{Inv}H/F)$. The kernel of this map are those elements in $G$ which are identity on $K$, by the correspondence, they are in $H$. Hence $G/H \cong \text{Gal}(\text{Inv}H/F)$. The image $\overline{G}$ is a group of automorphisms in $\text{Inv}H$ and $\text{Inv}G = F$. Hence theorem 2.6.1 implies that $K/\text{Inv}(G)$ is a normal extension. Conversely, if $K$ is normal over $F$. Let $a \in K$ and let $f(x)$ be the minimal polynomial of $a$ over $F$. Then over $K$, $f(x) = \prod(x - a_i)$, where $a_1 = a$. If $\gamma \in G$ then $f(\gamma(a)) = 0$ implies that $\gamma(a) = a_i$ for some $a_i$. The $\gamma(a) \in K$. I.e. $\gamma(K) \subset K$, so $H$ is normal in $G$.

\[\square\]

**Example 2.7.1.** Let $f = x^{17} - 1 \in \mathbb{Q}[x]$. Let $E$ be a splitting field of $f(x)$. Determine the Galois correspondence for this case.

**Solution:** Let $\mu_{17} = e^{2\pi i / 17}$, then

$$f(x) = x^{17} - 1 = \prod_{i=1}^{17}(x - \mu_{17}^i).$$

Let $\sigma(\mu)_{17} = \mu_{17}^3$, then $G = \text{Gal}(E/\mathbb{Q})$ is cyclic and is generated by $\sigma^i$. The order $|\text{Gal}(E/\mathbb{Q})| = 16$.

Since $G$ cyclic, it is easy to determine the set of all subgroups of $G$ as $H = \{< \sigma >, < \sigma^2 >, < \sigma^4 >, < \sigma^8 >, < \sigma^{16} > \}$.

Each subgroup $G_a = < \sigma^a >$ is also cyclic and hence

$$\text{Inv}G_a = \left\{ \sum_{i=1}^{16/a} \sigma^a(x) \mid x \in E \right\}$$

$$= \mathbb{Q}\left(\sum_{i=1}^{16/a} \sigma^a(\mu_{17})\right).$$

Let $x_1 = \sum_{i=1}^{16/a} \sigma^a(\mu_{17}) = \mu_{17} + \mu_{17}^2 + \cdots + \mu_{17}^{16} \in \mathbb{Q}.$

Let $x_2 = \sum_{i=1}^{16/2} \sigma^{a2}(\mu_{17}) = \mu_{17}^2 + \mu_{17}^4 + \mu_{17}^6 + \cdots + \mu_{17}^{16}.$

Let $x_4 = \sum_{i=1}^{16/4} \sigma^{a4}(\mu_{17}) = \mu_{17}^4 + \mu_{17}^8 + \mu_{17}^{12} + \mu_{17}^{16}.$

Let $x_8 = \sum_{i=1}^{16/8} \sigma^{a8}(\mu_{17}) = \mu_{17}^8 + \mu_{17}^{16}.$

Then $\text{Inv} < \sigma^i > = Q(x_i)$.

Hence there are 3 intermediate fields between $\mathbb{Q}$ and $E$. Explicitly

$$\mathbb{Q} = \mathbb{Q}(x_1) \subset \mathbb{Q}(x_2) \subset \mathbb{Q}(x_4) \subset \mathbb{Q}(x_8) \subset \mathbb{Q}(\mu_{17}) = E.$$
2.7. FUNDAMENTAL THEOREM OF GALOIS THEORY

Exercise 2.7.1. Let $K = \mathbb{F}_2$ and let $F = \mathbb{F}_2(t)$. Describe the separable closure and purely inseparable closure of $F$ over $K$.

Solution: By example 2.5.3 we know

$$G = \text{Gal}(F/K) = PGL(2, \mathbb{F}_2) = \langle \sigma_1, \sigma_2 \rangle \cong S_3,$$

where $\sigma_1(t) = 1/t$, $\sigma_2(t) = t + 1$. The group $G$ has 6 subgroups, which are

$$\Gamma = \{ \{id\}, \langle \sigma_1 \rangle, \langle \sigma_2 \rangle, \langle \sigma_1 \sigma_2 \rangle, \langle \sigma_1 \sigma_2 \sigma_1 \rangle, G \}.$$

$$\begin{align*}
\text{Inv}\{id\} & = F_2(t) \\
\text{Inv} \langle \sigma_1 \rangle & = F_2(t^2 + 1) \\
\text{Inv} \langle \sigma_2 \rangle & = F_2(t(t + 1)) \\
\text{Inv} \langle \sigma_1 \sigma_2 \rangle & = F_2(t^2) \\
\text{Inv} \langle \sigma_1 \sigma_2 \sigma_1 \rangle & = F_2(t^2(t + 1)) \\
\text{Inv} G & = F_2
\end{align*}$$
CHAPTER 2. GALOIS GROUPS OF FIELD EXTENSIONS
Chapter 3

Separability

3.1 Purely inseparable extensions

**Definition 3.1.1.** Let $F$ be an extension field of $K$. An algebraic element $u \in F$ is purely inseparable over $K$ if its irreducible polynomial $f$ in $K[x]$ factors in $F[x]$ as $f = (x - u)^m$. $F$ is a purely inseparable extension of $K$ if every elements of $F$ is purely inseparable over $K$.

**Example 3.1.1.** Let $K = \mathbb{F}_p(t)$ and $y^2 = t$. Then the minimal polynomial of $y$ over $K$ is $X^2 - t$. The element $y$ is separable over $K$ is $Char(K) = p \neq 2$. $Char(K) = 2$, $y$ is purely inseparable over $K$.

**Theorem 3.1.1.** Let $F$ be an extension field of $K$. Then $u \in F$ is both separable and purely inseparable over $K$ if and only if $u \in K$.

**Proof.** If $u \in K$, then the minimal irreducible polynomial of $u$ over $K$ is $x - u$. Hence $u$ is both separable and purely inseparable. It is easy to prove the converse by definitions.

**Lemma 3.1.1.** Let $F$ be an extension field of $K$ with $charK = p \neq 0$. If $u \in F$ is algebraic over $K$, then $u^p$ is separable over $K$ for some $n \geq 0$.

**Proof.** We use induction. Let $f(x)$ be the irreducible polynomial of $u$ over $K$. If $deg f = 1$ or $f$ has no repeated roots, then $u$ is separable. Otherwise, we have $f' = 0$, hence $f$ is a polynomial in $x^p$. Therefore, $u^p$ is algebraic of degree less than $u$ over $K$. Hence we can use induction $(u^p)^p^m$ is separable over $K$ for some $m \geq 0$. 

37
CHAPTER 3. SEPARABILITY

Theorem 3.1.2. If $F$ is an algebraic extension field of a field $K$ of characteristic $p \neq 0$, then the following statements are equivalent.

1. $F$ is purely inseparable over $K$;
2. the irreducible polynomial of any $u \in F$ is of the form $x^{p^n} - a \in K[x]$; if $u \in F$, then $u^{p^n} \in K$ for some $n \geq 0$;
3. If $u \in F$, then $u^{p^n} \in K$ for some $n \geq 0$;
4. the only elements of $F$ which are separable over $K$ are the elements of $K$ itself;
5. $F$ is generated over $K$ by a set of purely inseparable elements.

Proof. $1) \Rightarrow 2)$. Given any $u \in F$, the irreducible polynomial is $f = (x - u)^{m}$. $f' = 0$ and hence $m = p^rm'$ and $(p, m') = 1$. Hence $(x^{p^r} - u^{p^r})^{m} \in K$. Since the coefficient of $X^{p^r(m'-1)}$ is $u^{p^r}$. If $m' \neq 1$, then $u^{p^r} \in K$ and $f = (x^{p^r} - u^{p^r})^{m'}$ is not irreducible. Hence $m' = 1$.

$2) \Rightarrow 3) \Rightarrow 4) \Rightarrow 5)$ trivial, $4) \Rightarrow 3)$ (implies by Lemma 3.1.1).

$3) \Rightarrow 1)$ If $u \in F$, then $u^{p^n} \in K$ for some $n \geq 0$. Then $g(x) = x^{p^n} - u^{p^n} \in K[x]$ satisfies by $u$. Hence the minimal polynomial of $u$ is a divisor of $g(x)$, and $u$ is purely inseparable.

$5) \Rightarrow 3)$ Suppose $u_i$ is purely inseparable and by $3)$ we know $u_i^{p^{n_i}} \in K$. If $u = u_iu_j$ then $u^{p^{n_i+n_j}} \in K$. If $u = au_i + bu_j, a, b \in K$, then $(au_i + bu_j)^{p^{n_i+n_j}} = a^{p^{n_i+n_j}}u_i^{p^{n_i+n_j}} + b^{p^{n_i+n_j}}u_j^{p^{n_i+n_j}} \in K$. By induction, we know every element in $F$ is purely inseparable.

Corollary 3.1.1. If $F$ is a finite dimensional purely inseparable extension field of $K$ and $\text{char} \, K = p \neq 0$, then $[F : K] = p^n$ for some $n \geq 0$.

Proof. Suppose $F = K(u_1, \cdots, u_n)$ and by the above theorem, all $u_i$ are purely inseparable over $K$. Then $[K(u_i) : K] = p^{e_i}$ for some $i \geq 0$. The the composition of $K(u_i)$ also has $p$-power degree over $K$.

Lemma 3.1.2. Let $E$ be an extension of the field $F$. If $u$ is separable (resp. purely inseparable) over $F$, then $u$ is separable (resp. purely inseparable) over $E$.\]
3.2. SEPARABLE EXTENSIONS

Proof. Let \( f(x) \) be the monic minimal polynomial of \( u \) over \( F \) and let \( f' \) be the monic minimal polynomial of \( u \) over \( E \). Then \( f'|f \). If \( u \) is separable over \( F \), then \( f \) has only simple roots; and so if \( f' \). If \( u \) is purely inseparable over \( F \), then by Theorem 3.1.2, \( f \) has only one single root; and so is \( f' \).

Exercise 3.1.1. If \( u \in F \) is separable over \( K \) and \( v \in F \) is purely inseparable over \( K \), then \( K(u, v) = K(u + v) \). If \( uv \neq 0 \), then \( K(u, v) = K(uv) \).

Proof. We only need to consider characteristic \( p > 0 \) case.

By theorem 3.1.2, there is an large enough \( n \) such that \( v^p \in K \). Hence \((u + v)^p = u^p + v^p \) (resp. \((uv)^p = u^p v^p \)). So \( u^p \in K(u + v) \) (resp. \( u^p \in K(uv) \)). By Lemma 3.1.2, \( u \) is also separable over \( K(u^p) \). We consider \( x^p - u^p \in K(u^p)[x] \) and \( x^p - u^p = (x - u)^p \in K(u^p)[x] \). Hence \( u \) is both separable and purely inseparable over \( K(u^p) \). By Theorem 3.1.1, \( u \in K(u^p) = K(u + v) \) (resp. \( u \in K(u^p) = K(uv) \)). It follows \( v \in K(u + v) \) (resp. \( v \in K(uv) \)).

Exercise 3.1.2. If \( charK = p \neq 0 \) and \( p \mid [F : K] < \infty \), then \( F \) is separable over \( K \).

3.2 Separable extensions

Lemma 3.2.1. If \( F \) is an extension field of \( K \), \( X \) is a subset of \( F \) such that \( F = K(X) \) and every element of \( X \) is separable over \( K \), then \( F \) is a separable extension of \( K \).

Proof. If \( v \in F \), there exists \( u_1, \ldots, u_n \in X \) such that \( v \in K(u_1, \ldots, u_n) \). I.e. Let \( f_i \) be the irreducible polynomials of \( u_i \). The \( v \) is in the splitting field of the polynomial \( f = \prod f_i \) which is separable. Hence \( E \) is normal and separable. So \( v \) is separable.

Theorem 3.2.1. Let \( F \) be an algebraic extension of \( K \), \( S \) the set of all elements of \( F \) which are separable over \( K \), and \( P \) the set of all elements of \( F \) which are purely inseparable over \( K \).

1. \( S \) is a separable extension field of \( K \)
2. \( F \) is purely inseparable over \( S \)
3. \( P \) is a purely inseparable extension over \( K \).
40

CHAPTER 3. SEPARABILITY

4. \( P \cap S = K \).

5. \( F \) is separable over \( P \) if and only if \( F = SP \).

6. If \( F \) is normal over \( K \), then \( S \) is Galois over \( K \), \( F \) is Galois over \( P \) and \( \text{Gal}(F/K) \cong \text{Gal}(F/P) \cong \text{Gal}(S/K) \).

Proof. 1) follows from lemma 3.2.1.

2) Let \( u \in F \), the \( u^{p^n} \in S \) for some \( n \), by property 3 of theorem 3.1.2 we know \( F \) is purely inseparable over \( K \).

3) use same argument as that for 5) \( \Rightarrow \) 3) of theorem 3.1.2.

4) theorem 3.1.1

5) If \( F \) is separable over \( P \), then \( F \) is separable over \( PS \). Since \( F \) is purely inseparable over \( S \), hence \( F \) is purely inseparable over \( PS \). Hence \( F = PS \).

6) Let \( G = \text{Gal}(F/K) \). Inv\( G \supset P \). Let \( u \in \text{Inv}G \), let \( f \in K[x] \) be the minimal polynomial of \( u \). Since \( F \) is normal, then all roots of \( f \in F \). Suppose there is another root \( v \neq u \) of \( f \). Then \( \sigma : u \mapsto v \) induces an element in \( \text{Gal}(F/K) \) which will be fix \( u \). Hence Inv\( G \subset P \) and Inv\( G = P \).

By Galois theorem, we know \( F/P = F/\text{Inv}G \) is Galois and \( G = \text{Gal}(F/P) \). Now since every \( \sigma \in \text{Gal}(F/K) = \text{Gal}(F/P) \) must sending separable elements to separable elements. Hence \( \sigma \rightarrow \sigma|_S \) defines a homomorphism \( \theta : \text{Gal}(F/P) \rightarrow \text{Gal}(S/K) \). Since \( F \) is normal over \( S \) (as \( F \) is purely inseparable over \( S \)), hence \( \theta \) surjective. Since \( F/P \) is Galois, hence \( \theta \) is one-to-one. Hence \( \text{Gal}(S/K) = \text{Gal}(F/P) \). Now if \( u \in S \) is fixed by \( \text{Gal}(S/K) \) then it is also in \( P \) which is fixed by \( \text{Gal}(F/K) \). Hence \( u \in S \cap P = K \).

We will call \( P \) (resp. \( S \)) the purely inseparable (resp. separable) closure of \( F \) over \( K \).

Corollary 3.2.1. If \( F \) is separable over \( E \) and \( E \) is separable over \( K \), then \( F \) is separable over \( K \).

Proof. Let \( S \) be the maximal separable extension of \( K \) contain in \( F \), then \( E \subset S \). \( F \) is purely inseparable over \( S \). Since \( F \) is separable over \( E \), it is separable over \( S \). Hence \( F = S \). \( \square \)

Corollary 3.2.2. Let \( F \) be an algebraic extension of \( K \) and \( \text{char}K = p \neq 0 \). If \( F \) is separable over \( K \), then \( F = KF^{p^n} \) for each \( n \geq 1 \). If \( [F : K] < \infty \) and \( F = KF^p \), then \( F \) is separable over \( K \). In particular, \( u \in F \) is separable over \( K \) iff \( K(u^p) = K(u) \).
Proof. We first prove the last claim. If $u$ is separable over $K$, $K(u)/K(u^p)$ is separable as $K(u)/K$ is separable. $K(u)/K(u^p)$ is purely inseparable as it is generated by $u$ which purely inseparable over $F(u^p)$. Hence $K(u) = K(u^p)$.

If $K(u) = K(u^p)$, then by induction $K(u) = K(u^{p^n})$. Now for large enough $n$, we have $u^{p^n}$ being separable over $K$. Hence $u$ is separable over $K$.

Now we prove the first statement.

It follows naturally that if $F/K$ is separable, then $F = KF = KF^{p^n}$ for all $n \geq 1$.

If $[F : K] < \infty$, and $F = KF^p$. Iteratively, $F = KF^{p^n} = S$. Hence $F$ is separable over $K$.

\[ \square \]

**Definition 3.2.1.** Let $F/K$ be an algebraic extension and $S$ be the largest subfield of $F$ separable over $K$. Then $[S : K]$ is called the *separable degree* of $F$ over $K$, denoted by $[F : K]_s$. The dimension $[F : S]$, denoted by $[F : K]_i$, is called the *inseparable degree* of $F$ over $K$.

\[ [F : K]_i = 1, \text{ or } [F : K]_s = [F : K] \text{ iff } F \text{ is separable over } K. \ [F : K]_s = 1 \text{ or } [F : K]_i = [F : K] \text{ iff } F \text{ is purely inseparable over } K. \ [F : K] = [F : K]_s[F : K]_i. \]

**Lemma 3.2.2.** Let $F$ be an extension field of $E$ and $E/K$ an extension and $N/K$ is a normal extension containing $F$. If $r$ is the cardinality of distinct $E$-monomorphism $F \to N$ and $t$ is the cardinality of distinct $K$-monomorphism $E \to N$, then $rt$ is the cardinality of distinct $K$-monomorphism $F \to N$. 
CHAPTER 3. SEPARABILITY

Proof. Suppose \( r, t < \infty \). Let \( \tau_1, \ldots, \tau_r \) be all the distinct \( E \)-monomorphism \( F \to N \) and \( \sigma_1, \ldots, \sigma_t \) be the distinct monomorphism \( E \to N \). Each \( \sigma_i \) extends to a \( K \)-automorphism of \( N \). Each composition \( \sigma_i \tau_j \) is a \( K \)-monomorphism of \( F \to N \). If \( \sigma_i \tau_j = \sigma_a \tau_b \), then \( \tau_a^{-1} \sigma_i \tau_j = \tau_b \). Hence \( \sigma_a^{-1} \sigma_i | E = id \). Hence \( a = i \). Since \( \sigma_i \) is injective, hence \( \sigma_i \tau_j = \sigma_i \tau_b \) implies \( \tau_j = \tau_b \). So all \( \sigma_j \tau_j \) \( K \)-monomorphism are distinct. On the other hand, let \( \sigma : F \to N \) be a \( K \)-monomorphism. Then \( \sigma|_E = \sigma_i \) for some \( i \). Then \( \sigma^{-1} \sigma|_E = id \). Hence \( \sigma^{-1} \sigma = \tau_j \) for some \( j \). So \( \sigma = \sigma_i \tau_j \). \( \square \)

Proposition 3.2.1. Let \( F/K \) be a finite extension and \( N/K \) be normal which contains \( F \). Then the number of distinct \( K \)-monomorphisms of \( F \to N \) is \( [F : K]_s \).

Proof. Let \( S \) be the maximal separable extension of \( K \) contained in \( F \). Every \( K \)-monomorphism \( S \to N \) extends to a \( K \)-automorphism of \( N \) and by restriction a \( K \)-monomorphism \( F \to N \). We only need to worry \( \text{char} K = p \neq 0 \) and suppose \( \tau, \sigma \) are two \( K \)-monomorphism \( F \to N \) such that \( \tau|_S = \sigma|_S \). If \( u \in F \), then \( w^o \in S \), hence \( \tau(w^o) - \sigma(w^o) = (\sigma(u) - \tau(u))^o = 0 \) hence \( \tau(u) = \sigma(u) \). So \( \sigma|_S = \tau|_S \). So it suffice to prove when \( F/K \) is separable.

We proceed by induction on \( n = [F : K] = [F : K]_s \). The case \( n = 1 \) is trivial. Choose \( u \in F - K \), if \( [K(u) : K] < n \), then we apply \( K(u) = E \) to the above lemma. If \( [K(u) : K] = n \), then \( F = K(u) \) and \( [F : K] \) is the degree of the irreducible polynomial \( f \in K[x] \) of \( u \). Every \( K \)-monomorphism \( \sigma : F \to N \) is completely determined by \( v = \sigma(u) \) minimal polynomial (separable) of \( u \) over \( K \) is \( n \). Since \( v \) is a root of \( f \), there are at most \( [F : K] \) of them. Since \( f \) splits completely in \( N \) is separable, hence there are exactly \( [F : K] \) of them. \( \square \)

Corollary 3.2.3. If \( F/E \) and \( E/K \), then \( [F : E]_s [E : K]_s = [F : K]_s \) and \( [F : E]_s [E : K]_i = [F : K]_i \).

Proof. It follows from lemma 3.2.2 and prop 3.2.1. \( \square \)

Corollary 3.2.4. Let \( f \in K[x] \) be an irreducible monic polynomial over \( K \), \( F \) a splitting field of \( f \) over \( K \) and \( u_1 \) a root of \( f \). Then

1. every root of \( f \) has multiplicity \( [K(u_1) : K]_i \) so that in \( F(x) \),
\[
f = ((x - u_1) \ldots (x - u_n))^{[K(u_1) : K]}.
\]
2. \( u_1^{K(u_1) : K} \) is separable over \( K \).
Proof. Assume $\text{char} K = p \neq 0$. 1) for $\sigma_i : u_1 \mapsto u_i$ is a $K$-isomorphism of $F$. Hence $(x - u_1)^{r_1}...(x - r_n)^{r_n} = f = \sigma f = (x - \sigma(u_1))^{r_1}...(x - \sigma(u_n))^{r_n}$.

Since $u_i$ are distinct, by the unique factorization in $K[x]$ we know $r_i = r$ are all the same and hence $[K : F] = \text{deg} f = nr$. Since there are $n$ distinct $K$-monomorphism $K(u_1) \to F$ and hence $[K(u_1) : K]_s = n$. It follows $[K(u_1) : K]_i = r$.

Since $r$ is a power of $p$, $u_i^r$ are all distinct, then $(x - u_1^r)...(x - u_n^r) \in K[x]$ satisfied by $u_1^r$, and hence it is separable over $K$. 
\qed
Chapter 4

Cyclic extensions

4.1 Trace and Norm

**Definition 4.1.1.** Let $F$ be a finite extension of $K$ and $\overline{K}$ an algebraic closure of $K$ containing $F$. Let $\sigma_1, \ldots, \sigma_r$ be all the distinct $K$-monomorphism $F \to \overline{K}$. If $u \in F$, the norm of $u$, denoted by $N^K_F(u)$ is defined by

$$N^K_F(u) = (\sigma_1(u) \cdots \sigma_r(u))^{[f:K]}.$$

The trace of $u$, denoted by $T^K_F(u)$ is the element

$$T^K_F(u) = [f : K]_i(\sigma_1(u) + \cdots + \sigma_r(u)).$$

By definition, we can track that $N^K_F(u), T^K_F(u) \in K$.

**Theorem 4.1.1.** If $F$ is a finite dimensional Galois extension of $K$ and

$$Gal(F/K) = \{\sigma_1, \ldots, \sigma_n\},$$

then for $u \in F$

$$N^K_F(u) = \sigma_1(u) \cdots \sigma_r(u);$$
$$T^K_F(u) = \sigma_1(u) + \cdots + \sigma_r(u).$$

**Proof.** When $F/K$ is Galois, then $F$ is separable over $K$. Hence $[F : K]_i = 1$. \[\square\]

**Theorem 4.1.2.** Let $F/K$ be a finite extension. Then for all $u, v \in F$:
1. \( N_K^F(u)N_K^F(v) = N_K^F(uv) \) and \( T_K^F(u) + T_K^F(v) = T_K^F(u + v) \);

2. if \( u \in K \), then \( N_K^F(u) = [F : K]u \) and \( T_K^F(u) = [F : K]u \);

3. \( N_K^F(u) \) and \( T_K^F(u) \) are elements of \( K \). More precisely
   \[
   N_K^F(u) = ((-1)^n a_0)^{[F : K(u)]} \in K, T_K^F(u) = -[F : K(u)]a_{n-1} \in K,
   \]
   where \( f = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in K[x] \) is the irreducible polynomial of \( u \);

4. if \( E \) is an intermediate field, then
   \[
   N_K^E(N_E^F(u)) = N_K^F(u), T_K^E(T_E^F(u)) = T_K^F(u).
   \]

### 4.2 Cyclic extension

**Definition 4.2.1.** Let \( S \) be a nonempty set of automorphisms of a field \( F \). \( S \) is linearly independent provided that for any \( a_1, \ldots, a_n \in F \) and \( \sigma_1, \ldots, \sigma_n \in S \):

\[
a_1\sigma_1(u) + \cdots + a_n\sigma_n(u) = 0, \forall u \in F
\]

then \( a_i = 0 \) for every \( i \).

**Lemma 4.2.1.** If \( S \) is a set of distinct automorphisms of a field \( F \), then \( S \) is linearly independent.

**Proof.** If not there exist nonzero \( a_i \in F \) and distinct \( \sigma_i \in F \) such that

\[
a_1\sigma_1(u) + \cdots + a_n\sigma_n(u) = 0, \forall u \in F \tag{4.1}
\]

such an \( n > 1 \). Among all choose one with \( n \) minimal. Since \( \sigma_1 \) and \( \sigma_2 \) are distinct, there exists \( v \in F \) with \( \sigma_1(v) \neq \sigma_2(v) \). Apply (4.1) to \( uv \) we have

\[
a_1\sigma_1(u)\sigma_1(v) + \cdots + a_n\sigma_n(u)\sigma_n(v) = 0 \tag{4.2}
\]

Multiply (4.1) by \( \sigma(v) \) gives:

\[
a_1\sigma_1(u)\sigma_1(v) + \cdots + a_n\sigma_n(u)\sigma_1(v) = 0 \tag{4.3}
\]

The difference of (4.4) and (4.2) is a relation

\[
a_1[\sigma_2 - \sigma_1(v)]\sigma_2(u) + \cdots + a_n[\sigma_n(v) - \sigma_1(v)]\sigma_n(u) = 0, \forall u \in F \tag{4.4}
\]

Not all the coefficients are zero and this contradicts the minimality of \( n \). \( \square \)
4.2. CYCLIC EXTENSION

Definition 4.2.2. Let \( E/F \) is said to be cyclic (resp. abelian) if \( F/K \) is algebraic and Galois and \( \text{Gal}(F/F) \) is a cyclic (resp. abelian) group.

Example 4.2.1. Any finite field with characteristic \( p \) is a cyclic extension over \( \mathbb{F}_p \).

Theorem 4.2.1. Let \( F \) be a cyclic extension field of \( K \) of degree \( n \), \( \sigma \) a generator of \( \text{Gal}(F/K) \). Then

1. \( T_K^F(u) = 0 \) if and only if \( u = v - \sigma(v) \) for some \( v \in F \).

2. (Hilbert's theorem 90) \( N_K^F(u) = 1 \) if and only if \( u = v\sigma(v)^{-1} \) for some nonzero \( v \in F \).

Proof. \( T(u) = u + \sigma u + \cdots + \sigma^{n-1} u \) and \( T u = u(\sigma u) \cdots (\sigma^{n-1} u) \).

1) It is easy to prove that when \( u = v - \sigma v \) then \( Tu = 0 \). Now we prove the converse. Suppose \( Tu = 0 \). Since \( \sigma, \cdots, \sigma^n \) are linearly independent, there exists a \( z \in F \) such that \( Tz \neq 0 \). Let \( w = Tz^{-1}z \). Then \( Tw = 1 \). Now let

\[
v = uw + (u + \sigma u)(\sigma w) + (u + \sigma u + \sigma^2 u)(\sigma^2 w) + \cdots + (u + \sigma u + \cdots + \sigma^{n-2} u)(\sigma^{n-2} w),
\]

then we can check \( v - \sigma v = u \).

2) It is also easy to verify that if \( u = \sigma(v)^{-1}v \) then \( Tu = 1 \). Conversely, if \( N(u) = 1 \), then there exists \( y \in F \) such that the element \( v \) given by

\[
v = uy + (u\sigma u)\sigma y + \cdots + (u\sigma u \cdots \sigma^{n-2} u)\sigma^{n-2} y + (u\sigma u \cdots \sigma u^{-1})\sigma^{n-1} y
\]

is nonzero. The last summand is indeed \( N(u)\sigma^{n-1} y = \sigma^{n-1} y \). We can verify that \( u^{-1}v = \sigma v \). Hence \( u = v\sigma v^{-1} \).

Proposition 4.2.1. Let \( F/K \) be a cyclic extension of degree \( n = mp^t \) where \( 0 \neq \text{Char} K = p \) and \( (m, p) = 1 \). Then there exists a chain of intermediate fields \( F \supset E_0 \supset E_1 \supset \cdots \supset E_t = K \) such that \( F/E_0 \) is cyclic of degree \( m \) and for each \( 0 \leq i \leq t \), \( E_{i-1} \) is a cyclic extension of \( E_i \) of degree \( p \).

Proposition 4.2.2. Let \( K \) be a field of characteristic \( p \neq 0 \). \( F \) is a cyclic extension field of \( K \) of degree \( p \) if and only if \( F \) is a splitting field over \( K \) of an irreducible polynomial of the form \( x^p - x - a \in K[x] \). In this case \( F = K(u) \) where \( u \) is any root of \( x^p - x - a \).
Proof. If $F/K$ is a cyclic extension of degree $p$, let $\text{Gal}(F/K) = \langle \sigma \rangle$. Let $u \in F - K$, then $f(x) = (x - u) \cdots (x - \sigma^{p-1}u) \in K[x]$ is irreducible. Now $T^F_K(1) = [F : K]1 = p = 0$. Hence $1 = v - \sigma v$. Now $\sigma u = u + 1$. Hence $\sigma u^p = (u + 1)^p = u^p + 1 = u^p - u + \sigma u$. Hence $\sigma u^p - u = u^p - u = a \in K$. Now let $u = -v$, it is easy to see $u \notin K$. $\sigma u = -\sigma v = 1 - v = 1 + u$, hence $\sigma^i u = i + u$. The irreducible polynomial for $u$ is $f(x) = (x - u)(x - 1 - u) \cdots (x - p - 1 - u)$. Now $f(x + u) = x(x - 1) \cdots (x - p - 1) = x^p - x$. Hence $f(x) = (x - u)^p - (x - u) = x^p - u^p - x + u = x^p - x + a$.

Conversely, we assume that $F = K(u)$ where $u$ is a root of an irreducible polynomial of the form $f(x) = x^p - x - a$. $\sigma(u) = u + 1$ is an automorphism on $F$ whose degree is $p$. Let $G = \langle \sigma \rangle$. Then $\text{Inv}G = K$. On the other hand since $f(x) = (x - u)(x - (u + 1)) \cdots (x - (u + p - 1))$ is irreducible and $p$ is a prime number, we know $\deg f = p$ won’t be a multiple of $\text{char}(K)$. Hence all the $p$ roots of $f$ are distinct. Hence $[F : K] = p$ by Theorem 2.1.2. So $F$ is a cyclic extension of $K$ of degree $p$. \qed
Chapter 5

Finite fields

5.1 Properties of finite fields

Any finite extension of the prime field \( \mathbb{F}_p \) is called a finite field.

Lemma 5.1.1. If \( F \) is a finite extension over \( \mathbb{F}_p \), then \( F \) has \( p^n \) elements for some exponent \( n \).

Proof. Suppose \([ F : \mathbb{F}_p ] = n\), then as a vector space \( F \), it is \( n \) dimensional over \( \mathbb{F}_p \).

Lemma 5.1.2. For any natural number \( n \), there is a finite field with \( p^n \) elements.

Proof. Let \( f(x) = x^{p^n} - x \in \mathbb{F}_p[x] \). Now let \( F \) be the splitting field of \( f(x) \). Now \( f(x)' = -1 \neq 0 \), then \( f(x) \) has distinct roots. We are going to prove all these roots form a field. It is easy to see of \( a^{p^n} = a \) and \( b^{p^n} = b \), then \( (a - b)^{p^n} = a^{p^n} - b^{p^n} = a - b \) and \( (ab^{-1})^{p^n} = ab^{-1} \). Since \( f \) has degree \( p^n \) and all roots are distinct, then all these roots for a field of cardinality \( p^n \).

Lemma 5.1.3. Any two fields of the same number of elements are isomorphic.

Proof. Given a field \( F \) with \( p^n \) elements, we consider \( F^\times \) the nonzero elements. Since \( F \) is a field, \( f^\times \) form an abelian group of order \( p^n \). Hence for any \( a \in F \), \( a^{p^n-1} = 1 \). i.e. \( a^{p^n} = a \) for every \( a \in F \). Hence \( F \) is a splitting field of \( x^{p^n} - x \) over \( \mathbb{F}_p \). It follows that any two such fields are isomorphic.
Lemma 5.1.4. Given any finite field $F$ with $p^n$ elements. Then $\sigma : a \mapsto a^p$ is an automorphism of $F$. $\text{Gal}(F/\mathbb{F}_p)$ is cyclic generated by $\sigma$ or order $n$.

Proof. 1) Now give two elements $x$ and $y$ in $E$ we know $(x \pm y)^p = x^p \pm y^p$ and $(xy)^p = x^py^p$ and $\sigma(x^{-1}) = x^{-p} = (\sigma(x))^{-1}$.

2) $\sigma^i(x) = \sigma^{i-1}(x^p) = x^p$. Since any $a$ in $F$ with $p^n$ elements satisfying $a^{p^n} = a$, we know $\sigma^n = \text{id}$. Hence the order of $\sigma$ is exactly $n$. Now $[F : \mathbb{F}_p] = n$ is normal separable, hence $\#\text{Gal}(F/\mathbb{F}_p) = [F : \mathbb{F}_p]$ and it follows $\text{Gal}(F/\mathbb{F}_p) = \langle \sigma \rangle$.

Corollary 5.1.1. The subgroup of $\mathbb{F}_{p^n}$ are all $\mathbb{F}_{p^m}$ where $m | n$.

Proof. We apply the fundamental theorem of Galois theorem.

Since $\text{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) = \langle \sigma \rangle$. Hence $\Gamma$ the set of all subgroups of $\text{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ are $\{< \sigma^m >\}$ for some natural number $m$ dividing $n$. Now $\text{Inv}(< \sigma^m >) = \mathbb{F}_{p^n}$ and $\text{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_{p^m}) = < \sigma^m >$ of order $n/m$.

More over since each element in $\Gamma$ is normal, we have

$$\text{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)/\text{Gal}(\mathbb{F}_{p^m}/\mathbb{F}_{p^m}) = \text{Gal}(\mathbb{F}_{p^m}/\mathbb{F}_p).$$

Exercise 5.1.1. Let $F$ be a finite field and $f(x)$ an irreducible polynomial in $F[x]$. Show that if the roots $r_1, ..., r_n$ of $f(x)$ are suitably order then the Galois group $G_f$ consisting of the powers of $(12 \cdots n)$.

Proof. Suppose $F$ is a field of $p^n$ elements. Let $u$ be a root of $f(x)$, then $[F(u) : F] = n$ and $u^{p^n} \notin F$. Now we claim $x^{p^n}$ is also a root of $f$ since $\sigma^m(f(u)) = f(\sigma^m(u)) = f(u^{p^m})$.

is the splitting field of the polynomial $f$ as $F(u)$ is finite. Similarly $\sigma^{2m}(u) = u^{p^{2m}}$ is also a root of $f(x)$. We label all the roots as $u, u^{p^m}, u^{2p^m}, ..., u^{(p-1)m}$, then $\text{Gal}(E/F)$ acts on the roots as powers of $(12 \cdots n)$.

Given a prime finite field $\mathbb{F}_p$, let $\bar{\mathbb{F}}_p$ be an algebraic closure of $\mathbb{F}_p$, which as defined in section 2.4.

Theorem 5.1.1. $\text{Gal}(\bar{\mathbb{F}}_p/\mathbb{F}_p) = \langle \sigma_p \rangle \cong \mathbb{Z}$.

Proof. It follows from Lemma 5.1.4.
5.2 Irreducible polynomials over $\mathbb{F}_p$

Example 5.2.1. There are 2 degree 1 irreducible polynomials over $\mathbb{F}_2$, namely $x$ and $x+1$. Moreover $x(x-1) = x^2 - x$. There is only 1 degree 2 irreducible polynomial over $\mathbb{F}_2$, namely $x^2 + x + 1$. Moreover $x(x-1)(x^2 + x + 1) = x^4 - x$.

Exercise 5.2.1. Find the number of degree $d$ irreducible polynomials in $\mathbb{F}_p$.

Sol: Let $N(d)$ denote the number of irreducible polynomials over $\mathbb{F}_p$. Consider the factorization of $x^{p^n} - x = 0$ which is the splitting polynomial of $\mathbb{F}_{p^n}$. Since $\mathbb{F}_{p^n}$ is separable, so all irreducible factors of $x^{p^n} - x$ have only simple roots. We know there has no irreducible factor with degree larger than $n$ since every root is in $\mathbb{F}_{p^n}$. Hence we get

$$\sum_{n=1}^{n} N(n)n = p^n.$$ 

So $N(n)$ are given by a recursive formula. Exact formula for $N(n)$ is available by using some basis function in number theory.
Part II

Commutative algebra
Chapter 6
Rings and ideals-Review

In this section, in stead to give a full treatment of rings, modules, and integral domains, we will only recall only some special topics relevant to our discussion in the next few sections. For full details of the basic ring or module theory, please refer to either [Jac85], [Hun80], or [AM69].

6.1 Ideals

Any ring $A$ will be commutative with unit 1 unless specified. Let $a$ be an ideal of $A$, then $\phi : A \to A/a$ is a surjective ring homomorphism.

Proposition 6.1.1. There is a one-to-one order-preserving correspondence between the ideals $b$ of $A$ which contain $a$ and the ideals $\bar{b}$ of $A/a$, given by $\bar{b} = \phi^{-1}(b)$.

Let $f : A \to B$ be a ring homomorphism.

If $a$ is an idea in $A$, then $f(a)$ is not necessary an ideal in $B$. We define the extension $a^e$ of $a$ to $e$ the ideal $Bf(a)$ generated by $f(a)$ in $B$.

Let $b$ be an ideal in $B$, then $f^{-1}(b)$ is an ideal in $A$. This ideal is called the contraction $b^c$ of $b$. Let $b$ be a prime ideal in $B$, then $f^{-1}(b)$ is a prime ideal in $A$. But if $b$ is maximal in $B$, $f^{-1}(b)$ may not be maximal.

Example 6.1.1. $A = \mathbb{Z}, B = \mathbb{Q}, a = 0$. Consider the embedding $f : \mathbb{Z} \to \mathbb{Q}$. The ideal 0 is maximal in $\mathbb{Q}$, however $0^c = 0$ is not maximal in $\mathbb{Z}$.

Theorem 6.1.1. Every ring $A \neq 0$ has at least one maximal ideal.
6.2 Local rings

A ring with exactly one maximal ideal \( M \) is called a local ring. The field \( k = A/\mathfrak{M} \) is called the residue field of \( A \).

Example 6.2.1. \( \mathbb{Z}/p^n\mathbb{Z} \) for any prime \( p \) and any natural number \( n \) is a local ring with residue field \( \mathbb{F}_p \).

Example 6.2.2. Any field will be a local ring with 0 being the only maximal ideal. The residue field of a field is itself.

Proposition 6.2.1. 1. Let \( A \) be a ring with \( \mathfrak{M} \neq (1) \) be an ideal of \( A \) such that every \( x \in A - \mathfrak{M} \) is a unit. Then \( A \) is a local ring and \( \mathfrak{M} \) is its maximal ideal.

2. Let \( A \) be a ring and \( \mathfrak{M} \) a maximal ideal of \( A \), such that every element of \( 1 + \mathfrak{M} \) is a unit in \( A \), then \( A \) is a local ring.

Proof. 1. Every ideal \( \neq (1) \) consists of non-units, hence is contained in \( \mathfrak{M} \). Hence \( \mathfrak{M} \) is the only maximal ideal of \( A \).

2. Let \( x \in A - x \), since \( \mathfrak{M} \) is maximal, the ideal generated by \( x \) and \( \mathfrak{M} \) is \( (1) \), hence \( xy + m = 1 \) for some \( y \in A, m \in \mathfrak{M} \). Now \( xy=1-m \) is a unit. Hence it follows from 1. \( A \) is local. \( \square \)

6.3 Nilradical and Jacobson radical

Proposition 6.3.1. The set \( \mathfrak{N} \) of all nilpotent elements in a ring \( A \) is an ideal, and \( A/\mathfrak{N} \) has no nilpotent element \( \neq 0 \).

Proof. Since \( A \) is commutative, if \( x \) is nilpotent, then \( ax \) for any \( a \in A \) is nilpotent. If \( x, y \in \mathfrak{N} \) such that \( x^n = y^m = 0 \) then \( (x + y)^{n+m+1} = 0 \). Hence \( \mathfrak{N} \) is an ideal. Now consider \( a + \mathfrak{N} \) for \( a \notin \mathfrak{N} \). If it is nilpotent, then \( a^n \in \mathfrak{N} \) for some \( n \), so \( a \) itself is nilpotent. \( \square \)

The ideal \( \mathfrak{N} \) is called the nilradical of \( A \).

Example 6.3.1. \( A = \mathbb{Z}/9\mathbb{Z}, \mathfrak{N} = \{0, 3, 6\} = (3) \).

Example 6.3.2. \( A = \mathbb{Z}/12\mathbb{Z}, \mathfrak{N} = \{0, 6\} \).

Proposition 6.3.2. The nilradical \( \mathfrak{N} \) is the intersection of all the prime ideals of \( A \).
6.4. Rings and Modules of Fractions

Proof. Let \( \mathfrak{N} \) be the intersection of all prime ideals of \( A \). If \( f \in A \) is nilpotent, then for any prime ideal \( \mathfrak{a} \) \( f^n \in \mathfrak{a} \), for some \( n > 0 \). Hence \( f \in \mathfrak{a} \). So \( \mathfrak{N} \subseteq \mathfrak{N}' \). If \( f \notin \mathfrak{N} \), then let \( \Sigma \) be the set of ideals \( \mathfrak{a} \) with the property \( n > 0 \Rightarrow f^n \notin \mathfrak{a} \). \( 0 \notin \Sigma \) is nonempty. The \( \Sigma \) has a maximal element, called \( b \). If \( x, y \notin b \), then \( b + (x) \) and \( b + (y) \) strictly contain \( b \) hence not in \( \sigma \); hence \( f^m \in b + (x), f^n \in b + (y) \) for some \( n, m > 0 \). Then \( f^{m+n} \in b + (xy) \) hence \( b + (xy) \) is not in \( \Sigma \) and therefor \( xy \notin b \). Hence \( b \) is prime. It is a contradiction. \( \square \)

Definition 6.3.1. Let \( \mathfrak{a} \) be an ideal of \( A \), the radical of \( \mathfrak{a} \), denoted by \( \sqrt{\mathfrak{a}} = \{ f \in A | f^n \in \mathfrak{a} \text{ for some } r > 0 \} \). The set \( \sqrt{\mathfrak{a}} \) is an ideal itself.

Example 6.3.3. \( (x^2) \) is an ideal of \( k[x] \), then \( \sqrt{(x^2)} = (x) \). \( (x, y^2) \) is an ideal of \( k[x, y] \), then \( \sqrt{(x, y^2)} = (x, y) \).

Definition 6.3.2. The Jacobson radical \( \mathfrak{R} \) of \( A \) is the intersection of all maximal ideals of \( A \).

Example 6.3.4. In \( \mathbb{Z} \), maximal ideals are \( (p) \) for primes \( p \). Then the Jacobson radical of \( \mathbb{Z} \) is the zero ideal 0.

Proposition 6.3.3. \( x \in \mathfrak{R} \iff 1 - xy \) is a unit in \( A \) for all \( y \in A \).

Proof. If \( 1 - xy \) is not a unit, then it belongs to a maximal ideal \( m \). Since \( x \in M, xy \in m \), hence it implies \( 1 \in m \), which violates the definition of maximal ideal.

If \( x \in m \) for some maximal ideal \( m \), then \( m \) and \( x \) generate 1, i.e. \( xy + m = 1 \). Hence \( 1 - xy \) is not a unit. \( \square \)

Let \( A = \mathbb{F}_2[x, y]/(x^2 - y) \) where \( x, y \) are indeterminant. Find the nilradical of \( A \) and Jacobson radical of \( A \).

Exercise 6.3.1. In the ring \( A[x] \), the nilradical is equal to the Jacobson radical.

6.4 Rings and modules of fractions

A multiplicatively closed set of a ring \( A \) is a subset \( S \) of \( A \) such that \( 1 \in S \) and \( S \) is closed under multiplication. Then for the order pairs \( (a, s), a \in A, s \in S \), the following relation is an equivalent relation

\[ (a, s) \sim (b, t) \iff u( at - bs ) = 0, \text{ for some } u \in S. \]
Let $S^{-1}A$ denote the equivalent classes of $(a, s)$. It is called the ring of fractions respect to $S$. We can think of the class $(a, s)$ as $\frac{a}{s}$.

There is a ring homomorphism from $f : A \to S^{-1}A$ by sending $a \mapsto (a, 1)$.

**Example 6.4.1.** The following sets are multiplicative

- $S = \{a^k\}_{k=0}^\infty$, where $a \in A$.
- $S = A - p$ where $p$ is a prime ideal of $A$.
- $S = A^x$

**Example 6.4.2.** $A = \mathbb{Z}$, $S = \{2^k\}_{k=0}^\infty$, then $S^{-1}\mathbb{Z} = \{\frac{m}{2^n}, m, n \in \mathbb{Z}, n \geq 0\}$. Denote this new ring as $\mathbb{Z}[1/2]$ (means 2 is invertible here.) For any prime $p \in \mathbb{Z}$ different from 2, $(p)$ is a prime ideal of $\mathbb{Z}[1/2]$.

**Example 6.4.3.** $A = \mathbb{Z}$. If $S = A - (2)$, then $S^{-1}\mathbb{Z} = \{\frac{m}{n}, m, n \in \mathbb{Z}, n = 1 \mod 2\}$. This ring has only one maximal ideal $(2)$ and hence is a local ring. Its residue field is $\mathbb{F}_2$.

**Proposition 6.4.1.** Let $p$ be a prime ideal of $A$, let $S = A - p$. Then $A_p = S^{-1}A$ is a local ring with the maximal ideal $\mathfrak{M} = \{\frac{a}{b}, a \in p, b \in S\}$.

The process of passing from $A$ to $A_p$ is called the localization of $A$ at $p$.

### 6.5 Nakayama’s lemma

**Proposition 6.5.1.** Let $M$ be a finite generated $A$-module, and let $a$ be an ideal of $A$, and let $\phi$ be an $A$-module endomorphism of $M$ such that $\phi(M) \subseteq aM$. The $\phi$ satisfies an equation of the form

$$\pi^n + a_1\pi^{n-1} + \cdots + a_n = 0, a_i \in a.$$

**Corollary 6.5.1.** Let $M$ be a finitely generated $A$-module and let $a$ be an ideal of $A$ such that $aM = M$. Then there exist $x \equiv 1 \mod a$ such that $xM = 0$.

**Theorem 6.5.1 (Nakayama’s lemma).** Let $M$ be a finitely generated $A$-module and $a$ an ideal of $A$ contained in the Jacobson radical $\mathcal{R}$ of $A$. Then $aM = M$ implies that $M = 0$.

**Proof.** By the previous corollary we have $xM = 0$ for some $x \equiv 1 \mod \mathcal{R}$. By Proposition 6.3.3 $x$ is a unit in $A$, hence $M = 0$. \qed
6.6 Integral dependency

Let $B$ be a ring and $A$ be a subring of $B$. An element of $B$ is said to be integral over $A$ if $x$ is a root of a monic polynomial with coefficients in $A$, that is $x$ satisfies an equation of the form

$$x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0, \quad a_i \in A.$$  \hfill (6.1)

**Example 6.6.1.** When $A = \mathbb{Z}$, $B = \mathbb{Q}$, any $a \in \mathbb{Q}$ which is integral over $\mathbb{Z}$ satisfies a minimal polynomial $x - a \in \mathbb{Z}[x]$. Hence $a \in \mathbb{Z}$.

**Example 6.6.2.** When $A = \mathbb{Z}$ and $B = \mathbb{Z}[i]$, then every $a + bi \in \mathbb{Z}[i]$ is integral over $A$ as it satisfies $x^2 - 2ax + (a^2 + b^2) = 0$.

**Proposition 6.6.1.** The following are equivalent:

1. $x \in B$ is integral over $A$;
2. $A[x]$ is a finitely generated $A$-module;
3. $A[x]$ is contained in a subring $C$ of $B$ such that $C$ is a finitely generated $A$-module;
4. There exists a faithful $A[x]$-module $M$ which is finitely generated as an $A$-module.

**Proof.**

1 $\Rightarrow$ 2: $A[x]$ is generated by $1, x, \ldots, x^{n-1}$.

2 $\Rightarrow$ 3: take $C = A[x]$.

3 $\Rightarrow$ 4: Take $M = C$, which is a faithful $A[x]$-module as $yC = 0 \Rightarrow y \cdot 1 = 0$.

4 $\Rightarrow$ 1: Since $M$ is an $A[x]$-module, we have $xM \subseteq M$. Since $M$ is faithful, then we have $x^n + a_1x^{n-1} + \cdots + a_n = 0$ for some $a_i \in A$.

**Corollary 6.6.1.** Let $x_i, 1 \leq i \leq n$ be elements of $B$, each integral over $A$. Then the ring $A[x_1, \cdots, x_n]$ is a finitely generated $A$-module.

**Proof.** By induction on $n$. When $n > 1$, let $A_r = A[x_1, \ldots, x_r]$. Then by hypothesis, $A_{n-1}$ is a finitely generated $A$-module, say generated by $b_1, \ldots, b_m$. $A_n = A_{n-1}[x_n]$ is a finitely generated $A_{n-1}$-module and an $A$-module generated by $b_1, \ldots, b_m, b_1x_n, \ldots, b_mx_n$. \hfill \qed
The elements $C$ of $B$ which are integral over $A$ form a subring of $B$ containing $A$. The set $C$ is called the integral closure of $A$ in $B$. If $C = A$, then $A$ is said to be integrally closed in $B$. If $C = B$, then the ring $B$ is said to be integral over $A$.

For example, $\mathbb{Z}$ is integrally closed in $\mathbb{Q}$, and $\mathbb{Z}[i]$ is integral over $\mathbb{Z}$.

**Proposition 6.6.2.** Let $A \subseteq B$ be rings, $B$ integral over $A$.

1. If $b$ is an ideal of $B$ and $a = b^c = A \cap b$, then $B/b$ is integral over $A/a$.

2. If $S$ is a multiplicatively closed subset of $A$, then $S^{-1}B$ is integral over $S^{-1}A$.

**Proof.** If $x \in B$ we have $x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$, $a_i \in A$. Reduce by $b$ we have we have $x \mod b$ satisfied a monic equation with coefficients in $A/a$. Hence $x \mod b$ is integral over $A/a$.

Let $x/s \in S^{-1}B$, $x \in B$, $s \in S$. Then the equation above gives

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

which shows that $x/s$ is integral over $S^{-1}A$. \hfill \square

**Example 6.6.3.** Since $\mathbb{Z}[i]$ is integral over $\mathbb{Z}$, pick $S = \mathbb{Z} - (2)$ a multiplicative set in $\mathbb{Z}$, then $S^{-1}\mathbb{Z}[i] = \{b/s \mid b \in \mathbb{Z}[i], s \in \mathbb{Z} - (2)\} = S^{-1}\mathbb{Z} + iS^{-1}\mathbb{Z}$. This ring has only one maximal ideal $(1+i)$ hence is local. By the above proposition, $S^{-1} + iS^{-1}\mathbb{Z}$ is integral over $S^{-1}\mathbb{Z}$.

**Proposition 6.6.3.** Let $A \subseteq B$ be integral domains and suppose $B$ is integral over $A$. Then $B$ is a field if and only if $A$ is a field.

**Proof.** If $B$ is a field, then for any $x \in A$, $x^{-1} \in B$, and hence $x^{-1}$ is integral over $A$. So it satisfies

$$x^{-n} + a_{n-1}x^{1-n} + \cdots + a_0 = 0, \ a_i \in A.$$ 

So $x^{-1} = -a_{n-1} - a_{n-2}x - \cdots - a_0x^{n-1} \in A$. So $A$ is a field.

If $A$ is a field and $x \in B$ is integral over $A$ and satisfies

$$x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0, \ a_i \in A, a_0 \neq 0$$

then

$$x^{-n} + \frac{a_1}{a_0}x^{1-n} + \cdots + \frac{1}{a_0} = 0.$$ 

Since $A$ is a field, we have $x^{-1}$ is integral over $A$ and hence $x^{-1} \in B$ since $B$ is integral over $A$. So $B$ is also a field. \hfill \square
Corollary 6.6.2. Let $A \subseteq B$ be rings, and $B$ be integral over $A$. Let $q$ be a prime ideal of $B$ and let $p = q^c = a \cap A$. Then $q$ is maximal if and only if $p$ is maximal.

Proof. $B/q$ is integral over $A/p$, and both rings are integral domains. Then it follows from Proposition 6.6.3.

Proposition 6.6.4. Let $A \subseteq B$ be rings, and $B$ be integral over $A$. Let $q$ and $q'$ be prime ideals of $B$ such that $a \subseteq q'$ and $q^c = q'^c = p$. Then $q = q'$.

Proof. By Proposition 6.6.2 we know $B_p$ is integral over $A_p$. Let $\mathfrak{M}$ be the extension of $p$ in $A_p$ and let $n, n'$ be the extension of $q, q'$ respectively in $B_p$. Then $\mathfrak{M}$ is maximal ideal of $A_p$; $n \subseteq n'$ and $n^c = n'^c = \mathfrak{M}$. By Proposition 6.6.3 we know both $n$ and $n'$ are maximal, hence $n = n'$. So $q = q'$.

Theorem 6.6.1. Let $A \subseteq B$ be rings and suppose $B$ is integral over $A$. Let $p$ be a prime ideal of $A$. Then there exists a prime ideal $q$ of $B$ such that $q \cap A = p$.

Proof. By Proposition 6.6.2, $B_p$ is integral over $A_p$ and the diagram

\[
\begin{array}{ccc}
A & \rightarrow & B \\
\alpha \downarrow & & \downarrow \beta \\
A_p & \rightarrow & B_p
\end{array}
\]

is commutative. Let $n$ be the maximal ideal of $B_p$; then $\mathfrak{M} = n \cap A_p$ is maximal by Proposition 6.6.3, hence is the unique maximal ideal of the local ring $A_p$. If $q = \beta^{-1}(n)$, then $q$ is prime and we have $q \cap A = \alpha^{-1}(\mathfrak{M}) = p$.

Definition 6.6.1. An integral domain is said to be integrally closed if it is integrally closed in its field of fractions. For example, $\mathbb{Z}$ is integrally closed.

6.7 Integrally closed domains

Proposition 6.7.1. Let $A \subseteq B$ be rings, $C$ the integral closure of $A$ in $B$. Let $S$ be a multiplicatively closed subset of $A$. Then $S^{-1}C$ is the integral closure of $S^{-1}A$ in $S^{-1}B$. 
Proof. By Proposition 6.6.2, $S^{-1}C$ is integral over $S^{-1}A$. Then element $b/s \in S^{-1}B$ which is integral over $S^{-1}A$ satisfies

$$(b/s)^n + (a_{n-1}/s_{n-1})(b/s)^{n-1} + \cdots + a_0/s_0 = 0,$$

for some $a_i \in A, s_i \in S$. Let $t = s_{n-1}s_{n-2}\cdots s_0$ and multiply the above equation by $(st)^n$ throughout. Then the above equation becomes an equation of integral dependence over $A$. Hence $bt \in C$ and $b/s = bt/st \in S^{-1}C$. 

Proposition 6.7.2. Let $A$ be an integral domain. Then following are equivalent.

1. $A$ is integrally closed;

2. $A_p$ is integrally closed for each prime ideal $p$;

3. $A_M$ is integrally closed for each maximal ideal $M$.

Proof. Let $K$ be the field of fractions of $A$, let $C$ be the integral closure of $A$ in $K$. Let $f : A \to C$ be the identity mapping of $A$ onto $C$. Then $A$ being integrally closed is equivalent to $f$ being surjective, and by the previous Proposition $A_p$ (resp. $A_M$) being integrally closed, is equivalent to $f_p$ (resp. $f_M$) is surjective. 


Chapter 7

Primary decomposition

7.1 Primary ideals

Example 7.1.1. In \( \mathbb{Z} \), the ideal \((12) = (2^2) \cap (3)\). The ideal \((3)\) is prime and \((2^2)\) is not.

Recall, given an ideal \( a \) of \( A \), the radical of \( a \), denoted by \( r(a) = \sqrt{a} = \{ x \in A \mid x^n \in a, \text{ for some } n > 0 \} \).

Proposition 7.1.1. \( r(a) \) is the intersection of all prime ideals of \( A \) which contains \( a \).

Proof. \( f : A \to A/\alpha \) sending \( r(a) \) to the nilradical of \( A/\alpha \) which consists of nilpotent elements of \( A/\alpha \). The nilradical \( R \) is the intersection of prime ideals of \( A/\alpha \). Hence \( r(a) = f^{-1}(R) \) is the intersection of prime ideals of \( A \) containing \( a \).

An ideal \( a \) in a ring \( A \) is primary if \( a \neq A \) and if

\[ xy \in a \Rightarrow \text{either } x \in a \text{ or } y^n \in a \text{ for some } n > 0. \]

In other words, if \( ab \in \alpha \), then either \( a \in \alpha \) or \( b \in r(\alpha) \). Equivalently

\[ \alpha \text{ is primary } \iff A/\alpha \neq 0 \text{ and every zero divisor in } A/\alpha \text{ is nilpotent}. \]

Proposition 7.1.2. If \( a \) is primary, then \( r(a) \) is the smallest prime containing \( a \).
CHAPTER 7. PRIMARY DECOMPOSITION

Proof. The smallest part is clear as \( r(\mathfrak{a}) \) is the intersection of all prime ideals containing \( \mathfrak{a} \). We only need to show it is a prime ideal. If \( xy \in r(\mathfrak{a}) \), then \( (xy)^n \in \mathfrak{a} \) for some \( n > 0 \). If \( x^n \not\in \mathfrak{a} \) and because \( \mathfrak{a} \) is primary, hence \( y^n \in r(\mathfrak{a}) \) and hence \( y \in r(\mathfrak{a}) \).

Example 7.1.2. If \( k \) is a field and \( x \) and \( y \) are two variables, then \( (x, y^2) \) is primary in \( A = k[x, y] \) as the zero divisors of \( A/(x, y^2) = A[y]/(y^2) \) are nilpotent. Moreover \( (x, y) \) is a maximal ideal as \( A/(x, y) = k \) is a field. we have \( (x, y^2) = (x^2, xy, y^2) \subseteq (x, y^2) \subseteq (x, y) \).

Example 7.1.3. Let \( A = k[x, y, z]/(xy - z^2) \), let \( \bar{x}, \bar{y}, \bar{z} \) be the images of \( x, y, z \) in \( A \). Then \( \mathfrak{p} = (\bar{x}, \bar{z}) \) is prime as \( A/\mathfrak{a} = A[\bar{y}] \) is an integral domain. But \( \mathfrak{p}^2 = (\bar{x}\bar{z}, x^2, z^2) \) is not primary as \( \bar{x}\bar{y} = \bar{z}^2 \in \mathfrak{p}^2 \), but \( \bar{x} \not\in \mathfrak{p}^2 \) and \( \bar{y} \not\in r(\mathfrak{p}^2) = \mathfrak{p} \). Hence \( \mathfrak{p}^2 \) is not primary. So not all powers of prime ideals are primary.

Proposition 7.1.3. Let \( \mathfrak{a} \) be an ideal in \( A \), if \( r(\mathfrak{a}) = \mathfrak{M} \) is a maximal ideal, then \( \mathfrak{a} \) is primary. Consequently, every power of a maximal ideal is primary.

Proof. Since \( r(\mathfrak{a}) \) is the intersection of all prime ideals containing \( \mathfrak{a} \) and it ends up with a maximal ideal, hence only one prime ideal, which is \( \mathfrak{M} \) containing \( \mathfrak{a} \). Now \( f : A \to A/\mathfrak{a} \) maps \( r(\mathfrak{a}) \) to the nilradical of \( A/\mathfrak{a} \). It implies \( A/\mathfrak{a} \) is has also only one prime ideal \( \text{nil}(A/\mathfrak{a}) \). So every element in \( A/\mathfrak{a} \) is either a unit or a zero divisor which is nilpotent. So \( \mathfrak{a} \) is primary.

7.2 Primary decomposition

An ideal \( \mathfrak{a} \) is said to have a primary decomposition if \( \mathfrak{a} \) is a finite intersection of primary ideals.

Example 7.2.1. \( (x^2, xy) = (x) \cap (x, y)^2 \) is a primary decomposition of \( (x^2, xy) \). It is because \( (x) \) is prime and \( (x, y) \) is maximal, hence \( (x, y)^2 \) is primary.

Example 7.2.2. Every ideal in \( \mathbb{Z} \) has a primary decomposition. It is because every ideal is principal, so can be written as \( (n) = \prod p_i^{d_i} \) where \( p_i \) are distinct primes. Then \( (n) = \bigcap_{i=1}^n (p_i^{d_i}) \) and each \( (p_i^{d_i}) \) is primary.

7.3 Minimal primary decomposition

Lemma 7.3.1. Let \( \mathfrak{a}_i (1 \leq i \leq n) \) be \( \mathfrak{p} \)-primary, then \( \mathfrak{a} = \bigcap_{i=1}^n \mathfrak{a}_i \) is wp-primary.
7.3. MINIMAL PRIMARY DECOMPOSITION

Proof. $r(\cap_{i=1}^{n}a_i) = \cap r(a_i) = p$. Now we need to show $a$ is primary. If $xy \in a, y \notin a$, then for some $i$ we have $xy \in a_i$ and $y \notin a_i$, hence $x \in p$, since $a_i$ is primary.

Definition 7.3.1. Let $a$ and $b$ be two ideals of a ring $A$, then we use $(a : b)$ to denote the following set $\{x \in A \mid xb \in a\}$. When $b = (x)$ is a principal ideal then $(a : b)$ is denoted by $(a : x)$.

Example 7.3.1. In $A = \mathbb{Z}$, let $a = (2)$ and $b = (3)$, then $((2) : 3) = (2)$ and $((4) : 2) = (2)$.

Example 7.3.2. $(0 : x) = \text{Ann}(x)$.

Lemma 7.3.2. Let $a$ be a $p$-primary ideal, $x \in A$. Then

1. if $x \in a$, then $(a : x) = (1)$;

2. if $x \notin a$ then $(a : x)$ is $p$-primary, and therefore $r(a : x) = p$.

3. if $x \notin p$ then $(a : x) = a$

Proof. 1) is easy.

2) $(a : x) = \{y \in A \mid xy \in a\}$, since $a$ is primary, $y \in r(a) = p$. So $a \subseteq (a : x) \subseteq p$, so by the previous lemma, $(a : x)$ is $p$-primary.

3) Follows from the definition.

Given a primary decomposition of an ideal $a = \cap_{i=1}^{n}a_i$ where $a_i$ are primary, it is said to be minimal if the following two conditions are satisfied.

1. The $r(a_i)$ are all distinct.

2. $a_i \not\subseteq \cap_{j \neq i}a_j (1 \leq i \leq n)$.

Proposition 7.3.1. Any primary decomposition can be reduced to a minimal one.
Chapter 8

Chain condition

8.1 Chain condition

Definition 8.1.1. A module $A$ is said to satisfied the ascending chain condition (a.c.c) on submodules (or to be Noetherian) if every chain $A_1 \subset A_2 \subset \cdots$ of submodules of $A$, there is an integer $n$ such that $A_i = A_n$ for all $i \geq n$.

A module $B$ is said to satisfied the descending chain condition (d.c.c) on submodules (or to be Artinian) if every chain $A_1 \supset A_2 \supset \cdots$ of submodules of $A$, there is an integer $n$ such that $A_i = A_n$ for all $i \geq n$.

For example, the $\mathbb{Z}$-module $\mathbb{Z}$ satisfied the ascending chain condition but not the descending chain condition on the submodules.

If a ring $R$ is considered as a left [resp. right] module over itself, then it is easy to see that the submodules of $R$ are the left [resp. right] ideals of $R$. So we can speak of chain conditions on left or right ideals.

Definition 8.1.2. A ring $R$ is left [resp. right] Noetherian if $R$ satisfies the ascending chain condition on left [resp. right] ideals. $R$ is said to be Noetherian if $R$ is both left and right Noetherian.

A ring $R$ is left [resp. right] Artinian if $R$ satisfies the descending chain condition on left [resp. right] ideals. $R$ is said to be Artinian if $R$ is both left and right Artinian.

Example 8.1.1. A division ring $D$ is both Noetherian and Artinian since the only left and right ideals are $D$ and 0.

Example 8.1.2. Every commutative principal ideal ring is Noetherian. Special cases including $\mathbb{Z}$, $\mathbb{Z}_n$, and $F[x]$ with $F$ a field.
Example 8.1.3. The ring $\text{Mat}_n D$ of all $n \times n$ matrices over a division ring is both Noetherian and Artinian.

Example 8.1.4. The ring of all $2 \times 2$ matrices \( \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \) such that $a \in \mathbb{Z}$ and $b, c \in \mathbb{Q}$ is right Noetherian but not left Noetherian.

Example 8.1.5. The ring of all $2 \times 2$ matrices \( \begin{pmatrix} d & r \\ 0 & s \end{pmatrix} \) such that $d \in R$ and $s, r \in \mathbb{R}$ is right Artinian but not left Artinian.

Example 8.1.6. If $I$ is a nonzero ideal in a principal ideal domain $R$, then the ring $R/I$ is both Noetherian and Artinian.

Example 8.1.7. The ring $k[x_1, x_2, \ldots]$ is not Noetherian nor Artinian. But its field of fraction is both Noetherian and Artinian. Hence a subring of a Noetherian ring need not be Noetherian.

Let $\Sigma$ be a set of partially ordered by a relation $\leq$.

Proposition 8.1.1. The following conditions are equivalent:

1. Every increasing sequence $x_1 \leq x_2 \leq \cdots$ in $\sigma$ is stationary;

2. Every nonempty subset of $\sigma$ has a maximal element;

Proof. 1) $\Rightarrow$ 2) If 2) fails then there is a nonempty subset $T$ of $\sigma$ with no maximal element, and we can construct inductively a non-terminating strictly increasing sequence in $T$.

2) $\Rightarrow$ 1) The set $(x_m)$ has a maximal element, say $x_n$. Hence $(x_m)$ is stationary. $\square$

8.2 Basic properties of Noetherian and Artinian rings

Let $A$ be a commutative ring with unity and let $M$ be an abelian group whose binary operation is written additively. Suppose $M$ is an $A$-module.

Proposition 8.2.1. The group $M$ is a Noetherian $A$-module if and only if every submodule of $M$ is finitely generated.
8.2. BASIC PROPERTIES OF NOETHERIAN AND ARTINIAN RINGS

Proof. Let $N$ be a submodule of $M$, and let $\Sigma$ be the set of all finitely generated submodules of $N$. Then $\Sigma$ is nonempty as $0 \in \Sigma$, and therefore has a maximal element, say $N_0$. If $N_0 \neq N$, consider the submodule $N_0 + Ax$ where $x \in N - N_0$; this is finitely generated and strictly contains $N_0$. Hence $N_0 = N$.

Let $M_1 \subset M_2 \subset \cdots$ be an ascending chain of submodules of $M$. Then $N = \cup_{n=1}^{\infty} M_n$ is a submodule of $M$, hence is finitely generated by $x_1, \ldots, x_r$. Say $x_i \in M_{n_i}$, and let $n = \max_{i=1}^{r} n_i$; then each $x_i \in M_n$, hence the chain is stationary.

Because of this result, Noetherian modules are more important than Artinian modules.

Proposition 8.2.2. Let $0 \rightarrow M' \xrightarrow{\alpha} M \xrightarrow{\beta} M'' \rightarrow 0$ be an exact sequence of $A$-modules. Then

1. $M$ is Noetherian if and only if $M'$ and $M''$ are Noetherian;

2. $M$ is Artinian if and only if $M'$ and $M''$ are Artinian.

Proof. We shall prove 1) and the proof of 2) is similar.

⇒ An ascending chain of submodules of $M'$ (or $M''$) gives rise to a chain in $M$, hence is stationary.

⇐ Let $(L_n)_{n \geq 1}$ be an ascending chain of submodules; then $(\alpha^{-1}(L_n))$ is a chain in $M'$ and $(\beta(L_n))$ is a chain in $M''$. For large enough $n$ both these chains are stationary, and it follows that the chain $(L_n)$ is stationary. □

Corollary 8.2.1. If $M_i (1 \leq i \leq n)$ are Noetherian (resp. Artinian) $A$-modules, so is $\bigoplus_{i=1}^{n} M_i$.

Proof. Applies the above Proposition to

$$0 \rightarrow M_n \xrightarrow{\alpha} \bigoplus_{i=1}^{n} M_i \xrightarrow{\beta} \bigoplus_{i=1}^{n-1} M_i \rightarrow 0.$$ 

The result follows from induction. □

Proposition 8.2.3. Let $A$ be a Noetherian (resp. Artinian ring). $M$ a finitely generated $A$-module. Then $M$ is Noetherian (resp. Artinian).

Proof. $M$ is a quotient of $A^n$ for some $n$. The results from Corollary 8.2.1 and Proposition 8.2.2. □
Proposition 8.2.4. Let $A$ be a Noetherian (resp. Artinian), $a$ an ideal of $A$. Then $A/a$ is a Noetherian (Artinian) ring.

Proof. By Proposition 8.2.2, $A/a$ is Noetherian (resp. Artinian) as an $A$-module, hence also as an $A/a$-module. □

A chain of submodules of a module $M$ is a sequence $(M_i)(0 \leq i \leq n)$ of submodules of $M$ such that

$$M = M_0 \supset M_1 \supset \cdots \supset M_n = 0$$

strict inclusions.

The length of the chain is $n$. A composition series of $M$ is a maximal chain, that is one in which no extra submodules can be inserted: which is equivalent to say each $M_{i-1}/M_i(1 \leq i \leq n)$ is simple.

Proposition 8.2.5. Suppose that $M$ has a composition series of length $n$. Then every composition series of $M$ has length $n$, and every chain in $M$ can be extended to a composition series.

Proof. Let $l(M)$ be the least length of a composition series of a module $M$. ($l(M) = \infty$ if $M$ has no composition series.)

i) $N \subset M \implies l(N) < l(M)$. Let $(M_i)$ be a composition series of $M$ of minimum length and consider $N_i = N M_i$ of $N$. Since $N_{i-1}/N_i \subset M_{i-1}/M_i$ and the latter is a simple module, we have either $N_{i-1}/N_i = M_{i-1}/M_i$ or $N_{i-1} = N_i$; hence removing repeated terms, we have a composition series of $N$, so that $l(N) \leq l(M)$. If $l(N) = l(M) = n$, then $N_{i-1}/N_i = M_{i-1}/M_i$ for each $i$; hence $M_i = N_i$ and $N = M$.

ii) Any chain in $M$ has length $\leq l(M)$. Let $M = M_0 \supset M_1 \supset \cdots$ be a chain of length $k$. By i) we have $l(M) > l(M_1) > \cdots l(M_k) = 0$ hence $l(M) \geq k$.

iii) Consider any composition series of $M$. If it has length $k$, then $k \geq l(M)$. Hence $k = l(M)$. For any chain, if its length is $l(M)$ then it must be a composition series by ii); if its length is $< l(M)$, it is not a composition series, hence not maximal. So new terms can be inserted until length is $l(M)$. □

Proposition 8.2.6. $M$ has a composition series if and only if $M$ satisfies both chain conditions.

Proof. $\Rightarrow$ All chains in $M$ are of bounded length, hence both a.c.c and d.c.c.

$\Leftarrow$ Construct a composition series of $M$ as follows. Since $M = M_0$ satisfies the maximum condition by Proposition 8.1.1, it has a maximal submodule
8.2. BASIC PROPERTIES OF NOETHERIAN AND ARTINIAN RINGS

$M_1 \subset M_0$. Similarly $M_1$ has a maximal submodule $M_2 \subset M_1$, and so on. Thus we have a strictly descending chain $M_0 \supset M_1 \supset \cdots$ which is d.c.c. must be finite, and hence is a composition series of $M$.

A module satisfying both a.c.c and d.c.c is called a modules of finite length. $l(M)$ is called the length of $M$. The Jordan-Hölder theorem applies to modules of finite length: if $(M_i)_{i=0}^n$ and $(M'_i)_{i=0}^n$ are any two composition series of $M$, there is a one-to-one correspondence between the set of quotients $(M_{i-1}/M_i)_{1 \leq i \leq n}$ and $(M'_{i-1}/M'_i)_{1 \leq i \leq n}$ such that the corresponding quotient is isomorphic.

**Proposition 8.2.7.** The length $l(M)$ is an additive function on the class of all $A$-modules of finite length.

**Proof.** If $0 \rightarrow M' \xrightarrow{\alpha} M \xrightarrow{\beta} M'' \rightarrow 0$ is an exact sequence, then $l(M) = l(M') + l(M'')$. Take the image under $\alpha$ of any composition series of $M'$ and the inverse image under $\beta$ of any composition series of $M''$, these fits together to give a composition series of $M$.

**Example 8.2.1.** Let $M$ be a Noetherian $A$-module and let $\mathfrak{a}$ be the annihilator of $M$ in $A$. Prove that $A/\mathfrak{a}$ is a Noetherian ring.
Chapter 9

Noetherian rings

9.1 Properties of Noetherian rings

A ring is said to be Noetherian if it satisfies the following three equivalent conditions:

1. Every nonempty set of ideals has a maximal element.
2. Every ascending chain of ideals in $A$ is stationary.
3. Every ideal in $A$ is finitely generated.

**Proposition 9.1.1.** If $A$ is Noetherian and $\phi$ is a homomorphism of $A$ onto a ring $B$, then $B$ is Noetherian.

*Proof.* This follows from Proposition 8.2.4 since $B \cong A/\text{Ker}(\phi)$. \hfill $\square$

**Proposition 9.1.2.** Let $A$ be a subring of $B$; suppose that $A$ is Noetherian and that $B$ is finitely generated as an $A$-modules. Then $B$ is Noetherian.

*Proof.* By Proposition 8.2.3, $B$ is a Noetherian $A$-module. Hence it is a Noetherian $B$-module. \hfill $\square$

**Theorem 9.1.1 (Hilbert Basis Theorem).** If $A$ is Noetherian, then the polynomial ring $A[x]$ is Noetherian.

*Proof.* Let $a$ be an ideal in $A[x]$. The leading coefficients of the polynomials in $a$ form an ideal $\iota$ in $A$. Since $A$ is Noetherian, $\iota$ is finitely generated, say by $a_1, \ldots, a_n$. For $i = 1, \ldots, n$ there is a polynomial $f_i \in A[x]$ of the form

\[ f_i = a_i x^r + \text{lower terms} \]
$f_i = a_i x_i r_i + \text{(lower terms)}$. Let $r = \max_{i=1}^r r_i$. The $f_i$ generate an ideal $\mathfrak{a}' \subset \mathfrak{a}$ in $A[x]$. Let $f = ax^m + \text{(lower terms)}$ be any element of $\mathfrak{a}$; we have $a \in \mathfrak{a}$. If $m \geq r$, write $a = \sum_{i=1}^n u_i a_i$ where $u_i \in A$; then $f - \sum u_i f_i x^{m-r_i}$ is in $\mathfrak{a}$ and has degree $< m$. Proceeding in this way, we can go on subtracting elements of $\mathfrak{a}'$ from $f$ until we get a polynomial $g$ of degree $< r$. Hence $f = g + h$, $h \in \mathfrak{a}'$. Let $M$ be the $A$-module generated by $1, x, \ldots, x^{r-1}$; then $\mathfrak{a} = (a M) + \mathfrak{a}'$. Now $M$ is finitely generated $A$-module. Hence is Noetherian. So $\mathfrak{a}$ is finitely generated and is Noetherian.

**Corollary 9.1.1.** If $A$ is Noetherian so if $A[x_1, \ldots, x_n]$.

Recall that an $A$-algebra $B$ is a ring $B$ together with a ring homomorphism $f : A \to B$. A ring homomorphism $f : A \to B$ is finite and $B$ is a finite $A$-algebra, if $B$ is a finitely generated as an $A$-module. The homomorphism $f$ is of finite type and $B$ is a finitely generated $A$-algebra, if there exists a finite set of elements $x_1, \ldots, x_n$ in $B$ such that every elements of $B$ can be written as a polynomial in $x_1, \ldots, x_n$ with coefficients in $f(A)$; or equivalently there is an $A$-algebra homomorphism from a polynomial ring $A[t_1, \ldots, t_n]$ to $B$.

**Corollary 9.1.2.** Let $B$ be a finitely generated $A$-algebra. If $A$ is Noetherian, then so is $B$. In particular, every finitely generated ring, and every finitely generated algebra over a field is Noetherian.

**Proof.** The ring $B$ is a finitely generated $A$-algebra, then $B$ is a homomorphic image of a polynomial ring $A[x_1, \ldots, x_n]$, which is Noetherian by Corollary 9.1.1.

We know let $x_i$, $1 \leq i \leq n$ be elements of $B$ each integral over $A$. The ring $A[x_1, \ldots, x_n]$ is a finitely generated $A$-module. Consequently, the set $C$ of elements of $B$ which are integral over $A$ is a subring of $B$ containing $A$. This ring $C$ is called the integral closure of $A$ in $B$. If $C = A$ then we said $A$ is algebraically closed in $B$. If $C = B$ then the ring $B$ is said to be integral over $A$.

**Proposition 9.1.3.** Let $A \subseteq B \subseteq C$ be rings. Suppose that $A$ is Noetherian, that $C$ is finitely generated as an $A$-algebra and that $C$ is finitely generated as a $B$-module. Then $B$ is finitely generated as an $A$-algebra.
9.1. PROPERTIES OF NOETHERIAN RINGS

Proof. Let \( x_1, \ldots, x_m \) generated \( C \) as an \( A \)-algebra, and let \( y_1, \ldots, y_n \) generated \( C \) as a \( B \)-module. The there exist expressions of the form

\[
x_i = \sum_j b_{ij}y_j \quad (b_{ij} \in B) \quad (9.1)
\]

\[
y_iy_j = \sum_k b_{ijk}y_k \quad (b_{ijk} \in B).
\]

Let \( B \) be the algebra generated over \( A \) by the \( b_{ij} \) and \( b_{ijk} \). Since \( A \) is Noetherian, so is \( B \), and \( A \subseteq B_0 \subseteq B \).

An element of \( C \) is a polynomial in the \( X_i \) with coefficients in \( A \). Substituting (9.2) and making repeated use of (9.2) show that each element of \( C \) is a linear combinations of the \( y_i \) with coefficients in \( B_0 \), and hence \( C \) is finitely generated as a \( B_0 \)-module. Since \( B_0 \) is Noetherian, and \( B \) is a submodule of \( C \), it follows that \( B \) is finitely generated as a \( B_0 \)-module. Since \( B_0 \) is finitely generated as an \( A \)-algebra, it follows that \( B \) is finitely generated as an \( A \)-module.

Proposition 9.1.4. Let \( K \) be a field and \( E \) is a finitely generated \( K \) algebra. If \( E \) is a field, then it is a finite algebraic extension of \( K \).

Proof. Let \( E = K[x_1, \ldots, x_n] \). If \( E \) is not algebraic over \( E \) then we can renumber \( x_i \) so that \( x_1, \ldots, x_r \) are algebraically independent over \( K \) and each \( x_{r+1}, \ldots, x_n \) is algebraically over the field \( F = K(x_1, \ldots, x_r) \). Hence \( E \) is an algebraic extension over \( F \) and therefore finitely generated as an \( F \)-module. So apply the previous Proposition to \( F \subseteq F \subseteq E \), it follows that \( F \) is finitely generated as a \( K \)-algebra, say \( F = K[y_1, \ldots, y_s] \) where \( y_i = f_i/g_i, f_i, g_i \in K[x_1, \ldots, x_r] \).

There are infinitely many polynomials in \( K[x_1, \ldots, x_r] \), hence there is an irreducible polynomial \( h \) which is coprime to all \( g_i \) and the element \( h^{-1} \) of \( F \) could not be a polynomial in \( y_i \). This is a contradiction. Hence \( E \) is algebraic over \( K \), therefore, finite algebraic.

Corollary 9.1.3. Let \( k \) be a field, \( A \) a finitely generated \( k \)-algebra. let \( \mathfrak{M} \) be a maximal ideal of \( A \). The the field \( A/\mathfrak{M} \) is a finite algebraic extension of \( K \). In particular, if \( K \) is algebraically closed then \( A/\mathfrak{M} = K \).

Proof. Take \( E = A/\mathfrak{M} \) in the previous Proposition.
9.2 Primary decomposition for Noetherian rings

We are going to show every ideal in a Noetherian ring has a primary decomposition.

An ideal \( a \) is said to be irreducible if \( a \) is the intersection of two ideals, i.e. \( a = b \cap c \) then either \( a = b \) or \( a = c \).

**Example 9.2.1.** In the ring \( \mathbb{Z} \), every ideal is principal. Hence \( (n) \cap (m) = (\text{lcm}(n, m)) \). Hence every ideal \( (p) \) is irreducible if an only if \( p \) is a prime.

Similarly, for the any principal ideal domain, and ideal \( a = (f) \) is irreducible if and only if the element \( f \) is not a product of two non-units.

**Proposition 9.2.1.** In a Noetherian ring, every ideal is a finite intersection of irreducible ideals.

**Proof.** If not, let \( \Sigma \) be the set of all ideals in \( A \) which are not finite intersection of ideals. By assumption, \( \Sigma \) is nonempty. Since \( A \) is a Noetherian ring (hence every nonempty set of ideals contains a maximal one), we assume \( a \) is a maximal ideal in \( \Sigma \). \( a \) itself won’t be irreducible by the assumption, so it can be written as intersection of two ideals \( b \) and \( c \) such that both \( b \) and \( c \) contain \( a \) as a proper subset. It follows \( b \) and \( c \) are not in \( \Sigma \) so they can be written as finite intersection of irreducible ideals. So is \( a \), which contradicts the choice of \( a \).

**Exercise 9.2.1.** Every irreducible ideal in a Noetherian ring is primary.

**Proof.** We look at the quotient ring \( A/\mathfrak{a} \) and suppose now \( 0 \) is irreducible and we want to show that it is primary. Let \( xy = 0 \) and suppose \( y \neq 0 \). The chain of annihilators

\[
\text{Ann}(x) \subseteq \text{Ann}(x^2) \subseteq \cdots
\]

is stationary, so we have \( \text{Ann}(x^i) = \text{Ann}(x^n) \) when \( i \geq n \). Now consider the intersection \( (x^n) \cap (y) \). If \( a \in (x^n) \cap (y) \) then \( a = cx^n = by \in \text{Ann}(x) \), i.e. \( byx = 0 = cx^n x = cx^{n+1} \) So \( c \in \text{Ann}(x^{n+1}) = \text{Ann}(x^n) \), hence \( cx^n = a = 0 \). So \( (x^n) \cap (y) = 0 \). As \( 0 \) is irreducible and \( y \neq 0 \), hence \( x^n = 0 \) so \( 0 \) is primary.

**Theorem 9.2.1.** In a Noetherian ring \( A \) every ideal has a primary decomposition.

**Proposition 9.2.2.** In a Noetherian ring \( A \), every ideal \( \mathfrak{a} \) contains a power of its radical.
9.2. PRIMARY DECOMPOSITION FOR NOETHERIAN RINGS

Proof. Let \( x_1, \ldots, x_k \) generate \( r(a) \): say \( x_i^{n_i} \in a(1 \leq i \leq k) \). Let \( m = \sum_{i=1}^{k} (n_i - 1) + 1 \). Then \( r(a)^m \) is generated by products \( x_i^{r_i} \cdots x_k^{r_k} \) with \( r_i = m \); so we have some \( r_i \geq n_i \) for at least one index \( i \). Hence \( r(a)^m \subseteq a \).

Corollary 9.2.1. In a Noetherian ring the nilradical is nilpotent.

Proof. Take \( a = 0 \) in the previous proposition.

Corollary 9.2.2. Let \( A \) be Noetherian, \( M \) a maximal ideal of \( A \), \( a \) any ideal of \( A \), then the following are equivalent.

1. \( a \) is \( M \)-primary.
2. \( r(a) = M \).
3. \( M^n \subseteq a \subseteq M \) for some \( n > 0 \).

Proof. 1) \( \iff \) 2) \( \Rightarrow \) 3) \( \Rightarrow \) 2) by taking radicals.

Example 9.2.2. In \( A = k[x, y] \), the ideal \( (x^2, xy) = (x) \cap (y) = (x) \cap (x^2, y) \) has two different primary decompositions. Both of them are minimal.

Theorem 9.2.2. Let \( a \neq (1) \) be an ideal in a Noetherian ring. Then the prime ideals which belong to \( a \) are precisely the prime ideals which occur in the set \( (a : x)(x \in A) \).

Proof. Passing to \( A/\mathfrak{a} \) we may assume \( a = 0 \). Let \( \cap_{i=1}^{m} a_i = 0 \) be a minimal primary decomposition of the zero ideals, and \( \mathfrak{p}_i \) be the radical of \( a_i \). Let \( \mathfrak{b}_i = \cap_{j \neq i} a_i \neq 0 \). Then from Lemma 7.3.2 we have \( r(\text{Ann}(x)) = \mathfrak{p}_i \) for any \( x \neq 0 \) in \( \mathfrak{b}_i \), so \( \text{Ann}(x) \subseteq \mathfrak{p}_i \). Since \( a_i \) is \( \mathfrak{p}_i \)-primary, there exists an integer \( m \) such that \( \mathfrak{p}_i^m \subseteq a_i \), and therefore, \( \mathfrak{b}_i \mathfrak{p}_i^m \subseteq \mathfrak{b}_i \cap \mathfrak{p}_i^m \subseteq a_i \cap \mathfrak{b}_i = 0 \). Let \( m \geq 1 \) be the smallest integer such that \( \mathfrak{b}_i \mathfrak{p}_i^m = 0 \), and let \( x \) be a non-zero element in \( \mathfrak{b}_i \mathfrak{p}_i^{m-1} \). Then \( \mathfrak{p}_i x = 0 \), therefore for such an \( x \) we have \( \text{Ann}(x) \supseteq \mathfrak{p}_i \) and hence \( \text{Ann}(x) = \mathfrak{p}_i \). Conversely, if \( \mathfrak{p}_x \) is prime, then \( \mathfrak{p}_x = r(\text{Ann}(x)) = \cap (a_i : x) = \cap_{x \notin a_i} \mathfrak{p}_i \) and hence \( \mathfrak{p}_x = \mathfrak{p}_i \) for some \( i \), so \( \mathfrak{p}_x \) is a prime ideal belongs to 0. \( \square \)
Chapter 10

Artinian Rings

10.1 Further properties of Artinian rings

An Artinian ring is one satisfying the d.c.c on ideals.

**Proposition 10.1.1.** In an Artinian ring $\mathcal{A}$ every prime ideal is maximal.

**Proof.** Let $p$ be a prime ideal Consider $\mathcal{A}/p = B$. If $x \in B$ be nonzero, then $(x) \subseteq (x^2) \subseteq \cdots$ which is stationary so $x^n = y^{n+1}y$ for some $y \in B$. Since $B$ is an integral domain, hence $xy = 1$ so $x$ has an inverse in $B$, so $B$ is a field and hence $p$ is maximal. \qed

**Corollary 10.1.1.** In an Artinian ring, the nilradical $\mathfrak{N}$ is equal to the Jacobson radical $\mathfrak{R}$.

**Proposition 10.1.2.** An Artinian ring has only a finite number of maximal ideals.

**Proof.** Consider the set of finite intersection of maximal ideals which are also maximal ideals. This set has a minimal element $\mathfrak{M}_1 \cap \mathfrak{M}_2 \cap \cdots \mathfrak{M}_n$, hence for any maximal ideal $\mathfrak{M}$ it contains $\mathfrak{M}_1 \cap \mathfrak{M}_2 \cap \cdots \mathfrak{M}_n$, so $\mathfrak{M} = \mathfrak{M}_i$ for some $i$. \qed

**Proposition 10.1.3.** The Jacobson radical $\mathfrak{R}$ of an Artinian ring is nilpotent.

**Proof.** Consider the descending chain $\mathfrak{R} \supseteq \mathfrak{R}^2 \supseteq \mathfrak{R}^3 \supseteq \cdots \mathfrak{R}^k = \mathfrak{R}^{k+1} = a \supseteq \cdots$ which is stationary. If $a \neq 0$ and let $\Sigma$ to be the set of all ideals in
A such that \( a, b \neq 0, a \in \Sigma \). So \( \sigma \) contains a minimal element, denoted by \( c \), then pick a nonzero element in \( c \). By the minimality of \( c \) we have \( (x) = c \). Similarly we have \( a(x) = (x) \). Hence \( yx = x \) for some \( y \in a \in \mathcal{R} \). By induction we know \( x = yx = y^kx \) for any \( k \). Since \( y \in \mathcal{R} \) so \( x = y^kx = 0 \). This contradicts the choice of \( x \), so \( a = 0 \). \( \square \)

In a ring \( A \), a chain of prime ideals is a finite strictly increasing prime ideals \( p_0 \subset p_1 \subset \cdots \subset p_n \). The \textit{dimension} of a ring \( A \), denoted by \( \dim A \), is the supremum of the lengths of all chains of primes ideals in \( A \).

Example 10.1.1. When \( A = \mathbb{Z} \), \( \dim \mathbb{Z} = 1 \) as \( 0 \subset (p) \).

Example 10.1.2. When \( A = k \) is a field, then \( \dim A = 0 \).

Example 10.1.3. When \( A = k[x_1, \ldots, x_n] \) where \( x_i \) are algebraically independent over \( k \). Then \( \dim A = n \) as \( (0) \subset (x_1) \subset (x_1, x_2) \subset \cdots \subset (x_1, \ldots, x_n) \).

Theorem 10.1.1. The ring is Artinian if and only if \( A \) is Noetherian and has dimension 0.

\textit{Proof}. If \( A \) is Artinian, then \( \dim A = 0 \) and since \( \mathcal{R} \) is nilpotent, we have \( (\prod_{i=1}^n M_i)^k = 0 \) for some big enough \( k \) and where \( M_i \) are all the distinct maximal ideals. Hence being Artinian implies being Noetherian.

If \( A \) has dimension one, then every prime ideal is maximal. Since \( A \) is Noetherian, \( 0 \) has a primary decomposition, say \( 0 = \cap_{i=1}^n q_i \). Since \( r(q_i) = M_i \) is maximal, so we have \( M_i^{n_i} \subset q_i \). Hence \( 0 = \cap_{i=1}^n M_i^{n_i} \supset \prod_{i=1}^n M_i^{n_i} \). Hence being Noetherian implies being Artinian. \( \square \)

10.2 Local Artinian rings

In a local Artinian ring \( A \), since the maximal ideal is nilpotent, hence every element in \( A \) is either a unit or being nilpotent.

**Proposition 10.2.1.** Let \( A \) be a Noetherian local ring with maximal ideal \( \mathcal{M} \) then one of the following two properties hold.

1. \( \mathcal{M}^n \neq \mathcal{M}^{n+1} \) for all \( n \);
2. \( \mathcal{M}^n = 0 \) for some \( n \) and \( A \) is an Artinian local ring.

\textit{Proof}. If \( \mathcal{M}^n = \mathcal{M}^{n+1} \) then by the Nakayama’s lemma 6.5.1, we have \( \mathcal{M}^n = 0 \). In this case, \( \mathcal{M}^n \) contains in any prime ideal \( p \). By taking radical we know \( \mathcal{M} \) is identical to \( p \). Hence \( \dim A = 0 \) and \( A \) is Artinian. \( \square \)
Proposition 10.2.2. Any Artinian ring $A$ is isomorphic to a direct product of a finite number of local Artinian ring.

Proof. Let $\mathfrak{M}_i, 1 \leq i \leq n$ be the list of all distinct maximal ideals of $A$, then for some big enough $k$ $\prod \mathfrak{M}_i^k = 0$. Hence the map $A \rightarrow \prod A/\mathfrak{M}_i^k$ is surjective as $\mathfrak{M}_i^k$ are pairwise coprime and is injective as $\cap \mathfrak{M}_i^k = 0$. So we have an isomorphism.

Example 10.2.1. Let $A = \mathbb{Z}$ and $S = \mathbb{Z} - (p)$ for some prime $p$, then $S^{-1}\mathbb{Z}$ is a local Noetherian ring, but it is not Artinian as its dimension is 1.

Example 10.2.2. Let $k$ be a field and let $A = k[x_1, x_2, ...]/(x_1^2, x_2^2, ..., x_n^2)$, then this ring has only one prime ideal which is the image of $(x_1, x_2, ...)$. So this ring has dimension 0. But it is neither Noetherian or Artinian.

Proposition 10.2.3. Let $A$ be a local Artinian ring and let $\mathfrak{M}$ be its maximal ideal. Let $A/\mathfrak{M}$ be its residue field. Then the following statements are equivalent.

1. $A$ is a principal ideal;

2. The maximal ideal of $A$ is principal;

3. $\dim_k \mathfrak{M}/\mathfrak{M}^2 \leq 1$.

Proof. 1) $\Rightarrow$ 2) $\Rightarrow$ 3) are easy.

3) $\Rightarrow$ 1). If $\dim_k \mathfrak{M}/\mathfrak{M}^2 = 0$, then by Nakayama’s lemma 6.5.1 $\mathfrak{M} = 0$ so $A$ is a field. When $\dim_k \mathfrak{M}/\mathfrak{M}^2 = 1$, then we have $\mathfrak{M}$ is principal say $\mathfrak{M} = (x)$. Now at $a$ be any ideal of $A$, we have $a \subseteq \mathfrak{M}, a \not\subseteq \mathfrak{M}^2$, so we have $y \in a$ such that $y = ax$ where $a \notin a$. So $a$ is a unit in $A$, hence $x^r \in a$ and hence $a = (x^r)$ and $A$ is principal.
Chapter 11

Discrete valuation ring and Dedekind domains

We are going to consider Noetherian integral domains with dimension 1. Namely, in which rings, the nonzero prime ideals are maximal.

**Proposition 11.0.4.** Let \( A \) be a Noetherian domain of dimension 1, then every non-zero ideal \( a \) in \( A \) can be uniquely expressed as a product of primary ideals whose radicals are all distinct.

**Proof.** Since \( A \) is Noetherian, then \( a \) has a minimal primary decomposition \( a = \cap_{i=1}^{n} q_i \), where \( q_i \) is \( p_i \)-primary. When \( a \neq 0 \), the \( p_i \)'s are maximal and hence pairwise coprime. So \( \prod_{i=1}^{n} q_i = \cap_{i=1}^{n} q_i \) and hence \( a = \prod_{i=1}^{n} q_i \). Conversely, if \( a = \prod q_i \), then the same arguments shows that \( a = \cap_{i=1}^{n} q_i \); this is a minimal primary decomposition of \( a \) in which each \( q_i \) is an isolated primary components, and is therefore unique. \( \square \)

11.1 Discrete valuation rings

Let \( K \) be a field. A **discrete valuation** on \( K \) is a mapping \( v \) of \( K^\times \) onto \( \mathbb{Z} \) such that

1. \( v(xy) = v(x) + v(y) \), i.e. \( v \) is a homomorphism.

2. \( v(x + y) \geq \min(v(x), v(y)) \).

The set consisting of 0 and all \( x \in K^\times \) such that \( v(x) \geq 0 \) is a ring, called the valuation ring of \( v \). We denote \( v(0) = +\infty \).
Example 11.1.1. $K = \mathbb{Q}$. Let $p$ be a fixed prime, for any $x \in \mathbb{Q}$ write $x = p^n y$ where $n \in \mathbb{Z}$ and both denominator and numerator of $n$ coprime to $p$ and define $v_p(x) = n$. Then $v_p$ is a discrete valuation and the valuation ring of $v_p$ is the local ring $\mathbb{Z}(p)$.

Example 11.1.2. $K = k(x)$, where $k$ is a field and $x$ an indeterminant. Take a fixed polynomial $f \in k[x]$ and define $v_f$ similarly as above. Then $v_f$ is a discrete valuation and the valuation ring is the local ring of $k[x]$ with respect to the prime ideal $f$.

An integral domain $A$ is a discrete valuation ring if there is a discrete valuation $v$ of its field of fractions $K$ such that $A$ is the valuation ring of $v$. $A$ is a local ring, and its maximal ideal $M$ is the set of all $x \in K$ such that $v(x) > 0$.

Proposition 11.1.1. Let $A$ be a Noetherian local domain of dimension 1, $\mathfrak{M}$ its maximal ideal, $k = A/\mathfrak{M}$ its residue field. Then the following are equivalent:

1. $A$ is a discrete valuation ring;
2. $A$ is integrally closed;
3. $\mathfrak{M}$ is a principal ideal;
4. $\dim_k(\mathfrak{M}/\mathfrak{M}^2) = 1$;
5. Every non-zero ideal is a power of $\mathfrak{M}$; i.e. there exists $x \in A$ such that every non-zero ideal is of the form $(x^k), k \geq 0$.

Proof. 1) $\Rightarrow$ 2) If $A$ is a discrete valuation ring, let $F$ be its field of fractions. Then for any $x \in F$, either $x \in A$ or $x^{-1} \in A$. If $y \in K$ be integral over $A$, it satisfies

$$y^n + a_{n-1}y^{n-1} + \cdots + a_0 = 0, \ a_i \in A.$$

If $y \in A$, then we are done. If not, then $y = -(a_{n-1} + a_{n-2}y^{-1} + \cdots + a_0 y^{1-n} \in A$.

2) $\Rightarrow$ 3) For any ideal $0 \neq \mathfrak{a} = (a) \subseteq \mathfrak{M}$, there exist an integer $n$ such that $\mathfrak{M}^n \subseteq \mathfrak{a}$ and $\mathfrak{M}^{n-1} \not\subseteq \mathfrak{a}$. Choose $b \in \mathfrak{M}^{n-1}$ and let $x = a/b \in K \in F$. Then we have $x^{-1} \not\subseteq A$ since $b \not\in (a)$, hence $x^{-1}$ is not integral over $A$. So $x^{-1} \mathfrak{M} \not\subseteq \mathfrak{M}$ otherwise $\mathfrak{M}$ would be a faithful $A[x^{-1}]$-module, finitely generated as an
A-module. But $x^{-1} \mathfrak{M} \subseteq A$ by construction. Hence $x^{-1} \mathfrak{M} = A$ and therefore $\mathfrak{M} = Ax = (x)$.

3) $\Rightarrow$ 4) Since $\mathfrak{M}$ is principal, then $\dim_k \mathfrak{M}/\mathfrak{M}^2 \leq 1$. If $\mathfrak{M}/\mathfrak{M}^2 = 0$, then $A$ has dimension 0.

4) $\Rightarrow$ 5) Pick $x$ such that $x \in \mathfrak{M}$ and $x \notin \mathfrak{M}^2$. Since $M$ is principal, $\mathfrak{M} = (x)$. For any ideal $a$ of $A$, $a \supseteq (x^k)$ for some $k$. Then $a/\mathfrak{M}^k = a/\mathfrak{M}^k$ is an ideal in the Artinian local ring $A/\mathfrak{M}^k$. Hence Proposition 10.2.3 implies that $a = \mathfrak{M}^n = (x^n)$ for some $n$.

5) $\Rightarrow$ 1) For any $a \in A$, $a \in (x^k)$ and $x \notin (x^{k+1})$. Define $v(a) = k$. We can extend $v$ to the field of fractions $F$ of $A$ by $v(a/b) = v(a) - v(b)$. We can check that $v$ is a discrete valuation on $F$.

11.2 Dedekind domains

**Theorem 11.2.1.** Let $A$ be a Noetherian domain of dimension one. Then the following are equivalent:

1. $A$ is integrally closed;

2. Every primary ideals in $A$ is a prime power;

3. Every local ring $A_p, (p \neq 0)$ is a discrete valuation ring.

**Definition 11.2.1.** A ring satisfying the conditions of above is called a Dedekind domain.

**Corollary 11.2.1.** In a Dedekind domain, every non-zero ideal has a unique factorization as a product of prime ideals.

We will give two types of Dedekind domains.
Chapter 12

Algebraic integers

12.1 Algebraic integers form a ring and a \( \mathbb{Z} \)-module

Definition 12.1.1. A subset \( W \subset \mathbb{C} \) is called a \( \mathbb{Z} \)-module if

1. \( \gamma_1, \gamma_2 \in W \) implies that \( \gamma_1 \pm \gamma_2 \in W \);

2. There exist elements \( \gamma_1, \ldots, \gamma_n \in W \) such that every \( \gamma \in W \) is of the form \( \sum_{i=1}^{n} b_i \gamma_i \) with \( b_i \in \mathbb{Z} \).

Proposition 12.1.1. Let \( W \) be a \( \mathbb{Z} \)-module and suppose that \( \omega \in \mathbb{C} \) is such that \( \omega \gamma \in W \) for all \( \gamma \in W \). Then \( \omega \) is an algebraic integer.

Proof. \( \omega \gamma_i \in W \) hence \( \omega \gamma_i = \sum_{j=1}^{n} a_{ij} \gamma_j, a_{ij} \in \mathbb{Z} \). Hence \( \det(a_{ij} - \delta_{ij} \omega) = 0 \). \( \omega \) is a root of the characteristic polynomial of \( (a_{ij}) \) which is monic and have \( \mathbb{Z} \)-coefficients.

A complex number is said to be an algebraic number is it is algebraic over \( \mathbb{Q} \) and an algebraic integer if it is the root of a monic polynomial in \( \mathbb{Z}[x] \).

Exercise 12.1.1. 1. If \( u \) is an algebraic number, there exists an integer \( n \) such that \( nu \) is an algebraic integer.

2. If \( r \in \mathbb{Q} \) is an algebraic integer, then \( r \in \mathbb{Z} \).

3. If \( u \) is an algebraic integer and \( n \in \mathbb{Z} \), then \( u + n \) and \( nu \) are algebraic integers.
4. The sum and product of two algebraic integers are algebraic integers.

Proof. 1. If \( u \) is a root of \( a_nx^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0 = 0 \). We may assume \( a_i \in \mathbb{Z}, a_n \neq 0 \). Then \( a_nu \) is an algebraic integer.

2. \( r \in \mathbb{Q} \), the irreducible polynomial is \( x - r \in \mathbb{Z}[x] \), then \( x \in \mathbb{Z} \).

3. It is easy to check by the definition of algebraic integers.

4. Let \( u \) and \( v \) are two algebraic integers. Let \( F = \mathbb{Q}(u, v) \). Pick \( e_i, i = 1, \ldots, n \) a basis of \( F \) over \( \mathbb{Q} \), then write \( u^i v^j e_k = \sum_l a_{i,j,k,l} e_l, 0 \leq i, j \leq n, 1 \leq k, l \leq n \), where \( a_{i,j,k,l} \in \mathbb{Q} \). We write every nonzero rational number \( r = \frac{a}{b} \) where \( (a, b) = 1 \) and \( b \geq 0 \). We denote \( \text{dem}(r) = b \) and define \( r(0) = 1 \). The let \( c_l = \text{lcm}(\text{dem}(a_{i,j,k,l}), 0 \leq i, j \leq n, 1 \leq k, l \leq n) \).

Let \( W = \oplus c_l \mathbb{Z} e_l \). Then we have \((u + v)W \subset W \) and \( uvW \subset W \). By Proposition 12.1.1, we know both \( u + v \) and \( uv \) are algebraic integers.

Consequently, we have

**Theorem 12.1.1.** Let \( F \) be an algebraic extension over \( \mathbb{Q} \). Then the algebraic numbers of \( F \) form a ring.

We denote the ring of integers of an algebraic number field \( F \) by \( \mathcal{O}_F \).

**Theorem 12.1.2.** If \( F \) is an algebraic number field, then ring of algebraic integers of \( F \) form a finitely \( \mathbb{Z} \)-module with finite rank.

**Example 12.1.1.** The ring of algebraic integers of the field \( \mathbb{Q}(i) \) is a ranks two lattice. Explicitly, \( \mathcal{O}_{\mathbb{Q}(i)} = \mathbb{Z} \oplus \mathbb{Z}i \). I.e for any \( z \in \mathcal{O}_{\mathbb{Q}(i)} \), then \( z = a + bi, a, b \in \mathbb{Z} \).

**Example 12.1.2.** The ring of algebraic integers of the field \( \mathbb{Q}(\sqrt{-7}) \) is also a ranks two lattice. Explicitly, \( \mathcal{O}_{\mathbb{Q}(\sqrt{-7})} = \mathbb{Z} \oplus \mathbb{Z}\sqrt{-7}+1 \).

More generally we have the following. Let \( d > 0 \) be an integer. Let \( K = \mathbb{Q}(\sqrt{-d}) \). Then

\[
\mathcal{O}_K = \begin{cases} 
\mathbb{Z} \oplus \sqrt{-d} \cdot \mathbb{Z} & \text{if } d = 1(4) \\
\mathbb{Z} \oplus \frac{\sqrt{-d}+1}{2} \cdot \mathbb{Z} & \text{if } d = 3(4)
\end{cases}
\]
12.2 Ring of integers of a number field is a Dedekind domain

By theorem 12.1.1 we know that given an algebraic number field, which is a finite extension of $\mathbb{Q}$, the algebraic integers of $F$ form a ring and a $\mathbb{Z}$-module with finite rank.

**Theorem 12.2.1.** The ring of integers in an algebraic number field $K$ is a Dedekind domain.

**Proof.** Let $K$ be an algebraic number field. Let $A$ be the set of all algebraic integers. The field $K$ is a separable extension of $\mathbb{Q}$ (because the characteristic is zero). By Theorem 12.1.2, $A$ is a $\mathbb{Z}$-module with finite rank and hence a Noetherian ring over $\mathbb{Z}$. Also $A$ is integrally closed. Since every nonzero ideal is maximal, hence $A$ is a Dedekind domain.

\[\square\]

12.3 Primary decomposition for imaginary quadratic number fields

**Example 12.3.1.** Let $K = \mathbb{Z}(i)$. Its ring of integers is $\mathbb{Z}[i]$ which is a p.i.d. Let $p$ be a prime ideal of $\mathbb{Z}[i]$. Let $f : \mathbb{Z} \rightarrow \mathbb{Z}[i]$ be the embedding map. Then $p^c = p \cap \mathbb{Z} = (p)$ is a prime ideal in $\mathbb{Z}$. We have the following examples of prime factorization over $\mathbb{Z}[i]$.

\[
\begin{array}{ccc}
(1 + i)^2 & (1 + 2i)(1 - 2i) & (3) \\
\text{(2)} & \sqrt{} & \text{(5)} & \text{(3)} \\
\end{array}
\quad \text{over } \mathbb{Z}[i]
\]

In algebraic number theory, we say over $\mathbb{Z}[i]$ the ideal $(2)$ ramifies with ramification degree 2; the ideal $(5)$ splits completely; and the ideal $(3)$ is inert. In general, for any prime $p \in \mathbb{Q}$,

\[
\begin{array}{ccc}
p^2 & p \bar{p} & (p) \\
\text{(2)} & \sqrt{} & \text{(4)} & \text{(3)} & \text{over } \mathbb{Z}
\end{array}
\]
More generally, we have the following. For any prime $q > 0$, let $K = \mathbb{Q}(\sqrt{-q})$. For any $a \in \mathbb{Z}$, define the Legendre symbol

$$\left( \frac{a}{q} \right) = a^{\frac{q-1}{2}} \mod q = \begin{cases} 
0 & \text{if } x^2 - a = 0 \mod q \text{ has only one solution;} \\
1 & \text{if } x^2 - a = 0 \mod q \text{ has two different solutions;} \\
-1 & \text{if } x^2 - a = 0 \mod q \text{ has no solution;}
\end{cases}$$

The factorization of a prime ideal $(p)$ in $\mathbb{Z}$ over $\mathbb{Z}[i]$ is indicated by the following:

$$\begin{array}{c|c|c|c}
\text{p}^2 & \text{p} \overline{p} & (p) & \text{over } \mathcal{O}_K \\
\hline
(p) & (p) & (p) & \text{over } \mathbb{Z}
\end{array}$$

Moreover, we can generalize the above results to any imaginary quadratic number field $\mathbb{Q}(\sqrt{-d}), d > 0$. Accordingly, we can generalize the Legendre symbol to Jacobi symbol. For more details, please refer to [IR90].
Chapter 13

Algebraic curves

13.1 Affine varieties and affine curves

Definition 13.1.1. Given a commutative ring $A$ with unit, let $V = \text{Spec}(A) = \{\text{maximal ideals of } A\}$ be the spectrum of the ring $A$. In algebraic geometry, we can endow with the spectrum of a ring a special topology, called the Zarisk topology, where the closed sets correspond to the spectra of ideals of $A$. Under such a topology, $\text{Spec}(A)$, as a topological space, is called an affine variety.

Example 13.1.1. Let $k$ be a field. Let $x_i$ be indeterminants. Let

$$A^n_k = \text{Spec}(k[x_1, \cdots, x_n]) = \{\text{maximal ideals of } k[x]\} = \{(x_1 - a_1, \cdots, x_n - a_n) \mid a_i \in k\}.$$ 

It is called the $n$-dimensional affine space over the field $k$.

Definition 13.1.2. On the other hand, we call $A$ to be the ring of regular functions of the affine variety $V$. More formally, given an affine variety $V$, it can be embedded into the an affine space $\phi : V \to A^n_k$. Let

$$I(V) = \{f \in k[x_1, \cdots, x_n] \mid f(P) = 0 \text{ for all } P \in V\}.$$ 

It is easy to check $I(V)$ is an ideal in $k[x_1, \cdots, x_n]$. Then the ring

$$k[V] = k[x_1, \cdots, x_n]/I(V)$$ 

is called the ring of regular functions of $V$ over the field $k$. Its field of fractions, denoted by $k(V)$ called the field of regular functions of $V$ over the field $k$. 

91
Definition 13.1.3. Let $V_1, V_2$ be affine varieties. A rational map from $V_1$ to $V_2$ is map of the form

$$
\phi : V_1 \rightarrow V_2 \\
\phi = [f_1, \cdots, f_n]
$$

where $f_i \in \overline{k}(V_1)$ such that for any $P \in V_1$,

$$
\phi(P) = [f_1(P), \cdots, f_n(P)] \in V_2.
$$

If all $f_i \in k[x_1, \cdots, x_m]$, then $\phi$ is said to be defined over $K$. Such a rational map defined over $k$ induces a function

$$
\phi^*: k(V_2) \rightarrow k(V_1) \\
\phi^*(f) = f \circ \phi
$$

Definition 13.1.4. An affine $C$ satisfying $\dim_k k(C) = 1$ is called a curve over the field $k$.

Definition 13.1.5. Let $\phi : C_1 \rightarrow C_2$ be a map of curves defined over $k$. If $\phi$ is a constant, then we define the degree of $\phi$ to be 0; otherwise we say $\phi$ is finite, and define its degree by

$$
\deg \phi = [k(C_1) : \phi^*k(C_2)].
$$

We say that $\phi$ is separable (inseparable, purely inseparable) if the extension $k(C_1)/\phi^*k(C_2)$ has the corresponding property and we denote the separable and inseparable degrees of the extension by $\deg_s \phi$ and $\deg_i \phi$.

For more details, please refer to chapter 1 of [Har77] or chapter 1 and 2 of [Sil86].

13.2 An example - Elliptic curve

Example 13.2.1. Let $k$ be an algebraically closed field. We pick $k = \mathbb{C}$ here. $A = \mathbb{C}[x, y]/(y^2 = x^3 + x)$. It is a domain with dimension 1 as any nonzero prime ideal of $A$ is of the form $(x - x_0, y - y_0)$ where $P_0 = (x_0, y_0)$ is a point on the locus of the equation $C : y^2 = x^3 + x$, which is a complex curve (due to
13.2. AN EXAMPLE - ELLIPTIC CURVE

\( \dim A = 1 \). Let \( f(x, y) = y^2 - x^3 - x \) and \( \mathfrak{M}_P = \{ f \in A, f(P_0) = f(x_0, y_0) = 0 \} \). It is easy to see

\[
\Phi : A \rightarrow \mathbb{C}
\]

\[
f \mapsto f(P)
\]

is a surjective ring homomorphism. Since \( \mathbb{C} \) is a field, hence \( \mathfrak{M}_P \), which is the kernel of \( \Phi \), is maximal. Moreover, \( A/\mathfrak{M}_P = \mathbb{C} \). Now \( \dim_{\mathbb{C}} \mathfrak{M}_P/\mathfrak{M}_P^2 \leq 2 \) and \( \mathfrak{M}_P = (x - x_0, y - y_0), \mathfrak{M}_P^2 = ((x - x_0)^2, (y - y_0)^2, (x - x_0)(y - y_0)) \). Then

\[
x - x_0 = (y - y_0)^2 - (x - x_0)^3 \in \mathfrak{M}_P^2.
\]

Hence

\[
\dim_{\mathbb{C}} \mathfrak{M}_P/\mathfrak{M}_P^2 = 1 = \dim A \tag{13.1}
\]

On the other hand, condition (13.1) implies that when localized at a nonzero prime ideal we obtained a discrete valuation ring. So \( A \) itself is a Dedekind domain.

**Remark 13.2.1.** When condition (13.1) is satisfied at a point \( P \) of a curve \( C \), then the curve is said to be smooth at \( P \). Otherwise, the point \( P \) is said to be a singular point. If \( C \) is smooth at all \( P \), then \( C \) is said to be a smooth curve.

Consider the homomorphism \( f : \mathbb{C}[x] \hookrightarrow A \). The contraction of any prime \( \mathfrak{p} \) ideal in \( A \) is still a prime ideal in \( \mathbb{C}[x] \). For example

\[
(x - 0, y - 0) \cap \mathbb{C}[x] = (x - 0).
\]

\[
(x - 1, y - \sqrt{2}) \cap \mathbb{C}[x] = (x - 1) = (x - 1, y + \sqrt{2}).
\]

Similar to the factorization for quadratic imaginary number field, we have the factorization for any ideal \( (x - a), a \in \mathbb{C} \) over \( A \) as follows:

\[
\begin{array}{cc}
(x - a, 0)^2 & (x - a, y - \sqrt{b}) (x - a, y + \sqrt{b}) \\
| & \sqrt{b} \\
(x - a) & (x - a) \\
\end{array}
\]

over \( A \)

\[
\begin{array}{cc}
\text{if } b = a^2 + a = 0; & \text{if } b = a^2 + a \neq 0;
\end{array}
\]

over \( \mathbb{C} \)

Now let \( k \) be a field with characteristic \( \text{char}(k) = 2 \). Let \( A = k[x, y]/(y^2 = x^3 + x) \). In terms of field extension, we can say that the field of fractions \( k(C) \)
of $A$ is a quadratic extension of the field of fractions $k(x)$ of $k[x]$. In other words, $k(C) = k(x)(u)$, where $u$ is a solution of the equation $y^2 - x^3 - x = 0$.

The map

$$f' : k(x) \hookrightarrow k(C)$$

induced a map

$$C = \text{Spec}(A) \rightarrow A^1_k = \text{Spec}(k[x])$$

(a rational map between the affine variety $C$ and the affine variety $A^1_k$.)

Then $\deg f'^* = 2$. When $\text{char}(k) = 2$, $\deg f'^* = 2$. When $\text{char}(k) \neq 2$, $\deg f'^* = 2$.

### 13.3 An example of singular algebraic curve

**Example 13.3.1.** Similarly, when we localize $A = \mathbb{C}[x, y]/(y^2 - x^3 + x^2)$ at the prime ideal $(x, y)$, we obtained that $\dim \mathbb{C} \mathfrak{M}_P / \mathfrak{M}_P^2 = 2$. Hence $y^2 = x^3 + x^2$ has a singular point at $(0, 0)$ while it is smooth everywhere else. In this case $A$ is not a Dedekind domain.
Bibliography


[Har77] Robin Hartshorne, Algebraic geometry, Springer-Verlag, New York, 1977, Graduate Texts in Mathematics, No. 52. MR MR0463157 (57 #3116)


Index

Z-module, 87
affine space, 91
affine variety, 91
algebra, 74
algebra, finitely generated, 74
algebraic closure of a field, 29
algebraic curve, 91
algebraic element, 18
algebraic number, 87
algebraic number field, 21, 89
algebraically closed field, 28
Artinian ring, 67
Artinian ring, left, 67
Artinian ring, local, 80
Artinian ring, right, 67
chain condition, acceding, 67
chain condition, descending, 67
characteristic, 15
composite of fields, 18
composition series, 70
contraction, ideal, 55
Dedekind domain, 85
degree of map between curves, 92
degree, inseparable, 41
degree, of an extension, 16
degree, separable, 41
dimension of a ring, 80
discrete valuation, 83
discrete valuation ring, 84
extension, 16
extension finite, 16
extension, abelian, 47
extension, cyclic, 47
extension, ideal, 55
extension, simple, 20
field, 15
field of invariants, 30
field of rational functions, 16
field of regular functions of an affine variety, 91
field, residue, 56
field, splitting, 24
finite field, 49
fraction, ring or module, 57
Galois extension, 33
Galois group, 29
Hilbert Basis Theorem, 73
ideal, irreducible, 76
ideal, primary, 63
inseparable, purely, 37
integral closure, 60
integral element, 59
integrally closed domain, 61
isomorphism of fields, 23
isomorphism, fields, 23
INDEX

Jacobson radical, 57
Legendre symbol, 90
length of the chain of modules, 70
linearly independent, automorphisms, 46
localization, 58
minimal polynomial, 18
module, Artinian, 67
module, Noetherian, 67
multiplicatively closed set, 57
multiplicity of a root, 26
nilradical, 56
Noetherian ring, 67
Noetherian ring, left, 67
Noetherian ring, right, 67
norm, 45
normal extension, 31
perfect field, 27
primary decomposition, 64, 76
primary decomposition, minimal, 65
prime finite field, 15
principal ideal domain, 16
purely inseparable closure, 40
purely inseparable extension, 37
radical, 63
rational map between affine varieties, 92
ring of regular functions of an affine variety, 91
ring, commutative, 55
ring, local, 56
root, multiple, 26
separable closure, 40
separable polynomial, 27
separable, field, 27
simple extension, 17
simple root, 26
singular point, 93
smooth curve, 93
spectrum of a ring, 91
transcendental element, 18