Review of algebraic number theory

Inclusive paths in explicit number theory

July 04, 2023

Introduction

Introduction

- A fundamental theme in number theory is is the interplay between properties of prime numbers and the analytic properties of L-functions.

Introduction

- A fundamental theme in number theory is is the interplay between properties of prime numbers and the analytic properties of L-functions.
- These include
    - The Riemann zeta function $\zeta(s)$

Introduction

- A fundamental theme in number theory is is the interplay between properties of prime numbers and the analytic properties of L-functions.
- These include
  - The Riemann zeta function $\zeta(s)$
  - Dirichlet L-functions $L(s, \chi)$

Introduction

- A fundamental theme in number theory is is the interplay between properties of prime numbers and the analytic properties of L-functions.
- These include
  - The Riemann zeta function $\zeta(s)$
  - Dirichlet L-functions $L(s, \chi)$
  - Dedekind zeta functions (analogues of the Riemann zeta function for number fields)

Introduction

- A fundamental theme in number theory is is the interplay between properties of prime numbers and the analytic properties of L-functions.
- These include
  - The Riemann zeta function $\zeta(s)$
  - Dirichlet L-functions $L(s, \chi)$
  - Dedekind zeta functions (analogues of the Riemann zeta function for number fields)
  - Hecke L-functions (analogues of the Dirichlet L-functions) via characters of the ideal class group of a number field

Introduction

- A fundamental theme in number theory is is the interplay between properties of prime numbers and the analytic properties of L-functions.
- These include
  - The Riemann zeta function $\zeta(s)$
  - Dirichlet L-functions $L(s, \chi)$
  - Dedekind zeta functions (analogues of the Riemann zeta function for number fields)
  - Hecke L-functions (analogues of the Dirichlet L-functions) via characters of the ideal class group of a number field
  - Artin L-functions: Dirichlet series associated to linear representations of a Galois group G.

Introduction

- A fundamental theme in number theory is is the interplay between properties of prime numbers and the analytic properties of L-functions.
- These include
  - The Riemann zeta function $\zeta(s)$
  - Dirichlet L-functions $L(s, \chi)$
  - Dedekind zeta functions (analogues of the Riemann zeta function for number fields)
  - Hecke L-functions (analogues of the Dirichlet L-functions) via characters of the ideal class group of a number field
  - Artin L-functions: Dirichlet series associated to linear representations of a Galois group G.
- We review some notions from algebraic number theory needed to state the Chebotarev density theorem.

Algebraic integers

Algebraic integers

Our first goal is to generalize the study of the integral domain $\mathbb{Z}$ and its quotient field $\mathbb{Q}$.

Algebraic integers

Our first goal is to generalize the study of the integral domain $\mathbb{Z}$ and its quotient field $\mathbb{Q}$.

Definition

If $\alpha \in \mathbb{C}$ is a root of a monic, integral polynomial of degree d, that is, a root of a polynomial of the form

$$f(x) = \sum_{j=0}^{d-1} a_j x^j + x^d \in \mathbb{Z}[x],$$

which is irreducible over $\mathbb{Q}$, then α is called an **algebraic integer** *of degree d.*

- $a + bi$ $(a, b \in \mathbb{Z},\ b \neq 0)$ is an algebraic integer of degree 2, being a root of $x^2 - 2ax + a^2 + b^2$. Since $b \neq 0$, it is not a root of an integral, monic polynomial of degree 1.

- $a + bi$ $(a, b \in \mathbb{Z},\ b \neq 0)$ is an algebraic integer of degree 2, being a root of $x^2 - 2ax + a^2 + b^2$. Since $b \neq 0$, it is not a root of an integral, monic polynomial of degree 1.
- For a natural number m, let ζ_m denote a **primitive m-th root of unity**,

- $a + bi$ ($a, b \in \mathbb{Z}$, $b \neq 0$) is an algebraic integer of degree 2, being a root of $x^2 - 2ax + a^2 + b^2$. Since $b \neq 0$, it is not a root of an integral, monic polynomial of degree 1.
- For a natural number m, let ζ_m denote a **primitive m-th root of unity**, that is, a root of $x^m - 1$, but not a root of $x^d - 1$ for any natural number $d < m$.

- $a + bi$ $(a, b \in \mathbb{Z},\ b \neq 0)$ is an algebraic integer of degree 2, being a root of $x^2 - 2ax + a^2 + b^2$. Since $b \neq 0$, it is not a root of an integral, monic polynomial of degree 1.
- For a natural number m, let ζ_m denote a **primitive m-th root of unity**, that is, a root of $x^m - 1$, but not a root of $x^d - 1$ for any natural number $d < m$. For example, $\pm i$ are primitive 4-th roots of unity.

- $a + bi$ ($a, b \in \mathbb{Z},\ b \neq 0$) is an algebraic integer of degree 2, being a root of $x^2 - 2ax + a^2 + b^2$. Since $b \neq 0$, it is not a root of an integral, monic polynomial of degree 1.
- For a natural number m, let ζ_m denote a **primitive** m**-th root of unity**, that is, a root of $x^m - 1$, but not a root of $x^d - 1$ for any natural number $d < m$. For example, $\pm i$ are primitive 4-th roots of unity.

$$\frac{-1 \pm \sqrt{3}i}{2}$$

are primitive cube roots of unity.

- $a + bi$ ($a, b \in \mathbb{Z}$, $b \neq 0$) is an algebraic integer of degree 2, being a root of $x^2 - 2ax + a^2 + b^2$. Since $b \neq 0$, it is not a root of an integral, monic polynomial of degree 1.
- For a natural number m, let ζ_m denote a **primitive** m**-th root of unity**, that is, a root of $x^m - 1$, but not a root of $x^d - 1$ for any natural number $d < m$. For example, $\pm i$ are primitive 4-th roots of unity.

$$\frac{-1 \pm \sqrt{3}i}{2}$$

  are primitive cube roots of unity.
- Note (for later): numbers of the form

$$z_0 + z_1\zeta_n + z_2\zeta_n^2 + \cdots + z_{n-1}\zeta_n^{n-1},\ z_j \in \mathbb{Z}$$

  are called **cyclotomic integers** of order n.

Algebraic numbers and number fields

Algebraic numbers and number fields

Definition

An algebraic number α of degree $d \in \mathbb{N}$ is a root of a polynomial in $\mathbb{Q}[x]$ of degree d and not the root of any polynomial in $\mathbb{Q}[x]$ of degree less than d.

Algebraic numbers and number fields

Definition

An algebraic number α of degree $d \in \mathbb{N}$ is a root of a polynomial in $\mathbb{Q}[x]$ of degree d and not the root of any polynomial in $\mathbb{Q}[x]$ of degree less than d. In other words, an algebraic number is the root of an irreducible polynomial of degree d over $\mathbb{Q}$.

Algebraic numbers and number fields

Definition

An algebraic number α of degree $d \in \mathbb{N}$ is a root of a polynomial in $\mathbb{Q}[x]$ of degree d and not the root of any polynomial in $\mathbb{Q}[x]$ of degree less than d. In other words, an algebraic number is the root of an irreducible polynomial of degree d over $\mathbb{Q}$.

For example, $\sqrt{2}/3$ is an algebraic number, being a root of $9x^2 - 2$, but it is not an algebraic integer.

Algebraic numbers and number fields

Definition

An algebraic number α of degree $d \in \mathbb{N}$ is a root of a polynomial in $\mathbb{Q}[x]$ of degree d and not the root of any polynomial in $\mathbb{Q}[x]$ of degree less than d. In other words, an algebraic number is the root of an irreducible polynomial of degree d over $\mathbb{Q}$.

For example, $\sqrt{2}/3$ is an algebraic number, being a root of $9x^2 - 2$, but it is not an algebraic integer.

Let D be a squarefree integer with $|D| > 1$. If $4|(D-1)$, then $(-1 \pm \sqrt{D})/2$ is an algebraic integer.

Algebraic numbers and number fields

Definition

An algebraic number α of degree $d \in \mathbb{N}$ is a root of a polynomial in $\mathbb{Q}[x]$ of degree d and not the root of any polynomial in $\mathbb{Q}[x]$ of degree less than d. In other words, an algebraic number is the root of an irreducible polynomial of degree d over $\mathbb{Q}$.

For example, $\sqrt{2}/3$ is an algebraic number, being a root of $9x^2 - 2$, but it is not an algebraic integer.

Let D be a squarefree integer with $|D| > 1$. If $4|(D-1)$, then $(-1 \pm \sqrt{D})/2$ is an algebraic integer. It is a root of $x^2 + x + (1-D)/4 = 0$.

Algebraic numbers and number fields

Definition

An algebraic number α of degree $d \in \mathbb{N}$ is a root of a polynomial in $\mathbb{Q}[x]$ of degree d and not the root of any polynomial in $\mathbb{Q}[x]$ of degree less than d. In other words, an algebraic number is the root of an irreducible polynomial of degree d over $\mathbb{Q}$.

For example, $\sqrt{2}/3$ is an algebraic number, being a root of $9x^2 - 2$, but it is not an algebraic integer.

Let D be a squarefree integer with $|D| > 1$. If $4|(D-1)$, then $(-1 \pm \sqrt{D})/2$ is an algebraic integer. It is a root of $x^2 + x + (1-D)/4 = 0$.

Let $\overline{\mathbb{Q}}$ denote the set of all algebraic numbers, and let $\overline{\mathbb{Z}}$ denote the set of all algebraic integers.

- An **algebraic number field**, or a **number field** is a field of the form

$$\mathbb{F} = \mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_n) \subset \mathbb{C},\ \alpha_j \in \overline{\mathbb{Q}} \text{ for } 1 \leq j \leq n.$$

- An **algebraic number field**, or a **number field** is a field of the form

$$\mathbb{F} = \mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_n) \subset \mathbb{C},\ \alpha_j \in \overline{\mathbb{Q}} \text{ for } 1 \leq j \leq n.$$

- If $\mathbb{F}$ is a simple extension, that is, if $\mathbb{F} = \mathbb{Q}(\alpha)$ for some $\alpha \in \overline{\mathbb{Q}}$ of degree d, then $\mathbb{F}$ can be viewed as a vector space over $\mathbb{Q}$ with basis $\{1, \alpha, \alpha^2, \ldots, \alpha^{d-1}\}$.

- An **algebraic number field**, or a **number field** is a field of the form

$$\mathbb{F} = \mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_n) \subset \mathbb{C},\ \alpha_j \in \overline{\mathbb{Q}} \text{ for } 1 \leq j \leq n.$$

- If $\mathbb{F}$ is a simple extension, that is, if $\mathbb{F} = \mathbb{Q}(\alpha)$ for some $\alpha \in \overline{\mathbb{Q}}$ of degree d, then $\mathbb{F}$ can be viewed as a vector space over $\mathbb{Q}$ with basis $\{1, \alpha, \alpha^2, \ldots, \alpha^{d-1}\}$.
- By the Primitive Element Theorem for number fields, any number field $\mathbb{F}$ is a simple extension of $\mathbb{Q}$.

- An **algebraic number field**, or a **number field** is a field of the form

$$\mathbb{F} = \mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_n) \subset \mathbb{C},\ \alpha_j \in \overline{\mathbb{Q}} \text{ for } 1 \le j \le n.$$

- If $\mathbb{F}$ is a simple extension, that is, if $\mathbb{F} = \mathbb{Q}(\alpha)$ for some $\alpha \in \overline{\mathbb{Q}}$ of degree d, then $\mathbb{F}$ can be viewed as a vector space over $\mathbb{Q}$ with basis $\{1, \alpha, \alpha^2, \ldots, \alpha^{d-1}\}$.
- By the Primitive Element Theorem for number fields, any number field $\mathbb{F}$ is a simple extension of $\mathbb{Q}$. That is, any number field $\mathbb{F}$ is of the form $\mathbb{Q}(\alpha)$ for some $\alpha \in \overline{\mathbb{Q}}$.

- An **algebraic number field**, or a **number field** is a field of the form

$$\mathbb{F} = \mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_n) \subset \mathbb{C},\ \alpha_j \in \overline{\mathbb{Q}} \text{ for } 1 \leq j \leq n.$$

- If $\mathbb{F}$ is a simple extension, that is, if $\mathbb{F} = \mathbb{Q}(\alpha)$ for some $\alpha \in \overline{\mathbb{Q}}$ of degree d, then $\mathbb{F}$ can be viewed as a vector space over $\mathbb{Q}$ with basis $\{1, \alpha, \alpha^2, \ldots, \alpha^{d-1}\}$.
- By the Primitive Element Theorem for number fields, any number field $\mathbb{F}$ is a simple extension of $\mathbb{Q}$. That is, any number field $\mathbb{F}$ is of the form $\mathbb{Q}(\alpha)$ for some $\alpha \in \overline{\mathbb{Q}}$.
- An algebraic number α of degree d over a number field $\mathbb{F}$ is the root of an irreducible polynomial in $\mathbb{F}[x]$ of degree d.

- An **algebraic number field**, or a **number field** is a field of the form

$$\mathbb{F} = \mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_n) \subset \mathbb{C},\ \alpha_j \in \overline{\mathbb{Q}} \text{ for } 1 \le j \le n.$$

- If $\mathbb{F}$ is a simple extension, that is, if $\mathbb{F} = \mathbb{Q}(\alpha)$ for some $\alpha \in \overline{\mathbb{Q}}$ of degree d, then $\mathbb{F}$ can be viewed as a vector space over $\mathbb{Q}$ with basis $\{1, \alpha, \alpha^2, \ldots, \alpha^{d-1}\}$.
- By the Primitive Element Theorem for number fields, any number field $\mathbb{F}$ is a simple extension of $\mathbb{Q}$. That is, any number field $\mathbb{F}$ is of the form $\mathbb{Q}(\alpha)$ for some $\alpha \in \overline{\mathbb{Q}}$.
- An algebraic number α of degree d over a number field $\mathbb{F}$ is the root of an irreducible polynomial in $\mathbb{F}[x]$ of degree d.
- In fact, an algebraic number of degree d over a number field $\mathbb{F}$ is the root of a unique, monic irreducible polynomial in $\mathbb{F}[x]$ of degree d, which we call the minimal polynomial of α over $\mathbb{F}$ and denote as $m_{\alpha,\mathbb{F}}(x)$.

- An **algebraic number field**, or a **number field** is a field of the form
$$\mathbb{F} = \mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_n) \subset \mathbb{C},\ \alpha_j \in \overline{\mathbb{Q}} \text{ for } 1 \le j \le n.$$
- If $\mathbb{F}$ is a simple extension, that is, if $\mathbb{F} = \mathbb{Q}(\alpha)$ for some $\alpha \in \overline{\mathbb{Q}}$ of degree d, then $\mathbb{F}$ can be viewed as a vector space over $\mathbb{Q}$ with basis $\{1, \alpha, \alpha^2, \ldots, \alpha^{d-1}\}$.
- By the Primitive Element Theorem for number fields, any number field $\mathbb{F}$ is a simple extension of $\mathbb{Q}$. That is, any number field $\mathbb{F}$ is of the form $\mathbb{Q}(\alpha)$ for some $\alpha \in \overline{\mathbb{Q}}$.
- An algebraic number α of degree d over a number field $\mathbb{F}$ is the root of an irreducible polynomial in $\mathbb{F}[x]$ of degree d.
- In fact, an algebraic number of degree d over a number field $\mathbb{F}$ is the root of a unique, monic irreducible polynomial in $\mathbb{F}[x]$ of degree d, which we call the minimal polynomial of α over $\mathbb{F}$ and denote as $m_{\alpha,\mathbb{F}}(x)$.

More about algebraic integers

- $\overline{\mathbb{Z}}$ is a subring of $\overline{\mathbb{Q}}$.

More about algebraic integers

- $\overline{\mathbb{Z}}$ is a subring of $\overline{\mathbb{Q}}$.
- For a number field $\mathbb{F}$, $\mathbb{F} \cap \overline{\mathbb{Z}}$ is a ring in $\mathbb{F}$, and is called the ring of algebraic integers of $\mathbb{F}$.

More about algebraic integers

- $\overline{\mathbb{Z}}$ is a subring of $\overline{\mathbb{Q}}$.
- For a number field $\mathbb{F}$, $\mathbb{F} \cap \overline{\mathbb{Z}}$ is a ring in $\mathbb{F}$, and is called the ring of algebraic integers of $\mathbb{F}$. It is denoted as $\mathcal{O}_{\mathbb{F}}$.

More about algebraic integers

- $\overline{\mathbb{Z}}$ is a subring of $\overline{\mathbb{Q}}$.
- For a number field $\mathbb{F}$, $\mathbb{F} \cap \overline{\mathbb{Z}}$ is a ring in $\mathbb{F}$, and is called the ring of algebraic integers of $\mathbb{F}$. It is denoted as $\mathcal{O}_{\mathbb{F}}$.
- $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$.

More about algebraic integers

- $\overline{\mathbb{Z}}$ is a subring of $\overline{\mathbb{Q}}$.
- For a number field $\mathbb{F}$, $\mathbb{F} \cap \overline{\mathbb{Z}}$ is a ring in $\mathbb{F}$, and is called the ring of algebraic integers of $\mathbb{F}$. It is denoted as $\mathcal{O}_{\mathbb{F}}$.
- $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$.
- For any number field $\mathbb{F}$, $\mathbb{Q} \cap \mathcal{O}_{\mathbb{F}} = \mathbb{Z}$.

More about algebraic integers

- $\overline{\mathbb{Z}}$ is a subring of $\overline{\mathbb{Q}}$.
- For a number field $\mathbb{F}$, $\mathbb{F} \cap \overline{\mathbb{Z}}$ is a ring in $\mathbb{F}$, and is called the ring of algebraic integers of $\mathbb{F}$. It is denoted as $\mathcal{O}_{\mathbb{F}}$.
- $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$.
- For any number field $\mathbb{F}$, $\mathbb{Q} \cap \mathcal{O}_{\mathbb{F}} = \mathbb{Z}$.
- The quotient field of $\mathcal{O}_{\mathbb{F}}$ is $\mathbb{F}$.

More about algebraic integers

- $\overline{\mathbb{Z}}$ is a subring of $\overline{\mathbb{Q}}$.
- For a number field $\mathbb{F}$, $\mathbb{F} \cap \overline{\mathbb{Z}}$ is a ring in $\mathbb{F}$, and is called the ring of algebraic integers of $\mathbb{F}$. It is denoted as $\mathcal{O}_{\mathbb{F}}$.
- $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$.
- For any number field $\mathbb{F}$, $\mathbb{Q} \cap \mathcal{O}_{\mathbb{F}} = \mathbb{Z}$.
- The quotient field of $\mathcal{O}_{\mathbb{F}}$ is $\mathbb{F}$.
- $\mathcal{O}_{\mathbb{F}}$ is a Dedekind domain. That is,

More about algebraic integers

- $\overline{\mathbb{Z}}$ is a subring of $\overline{\mathbb{Q}}$.
- For a number field $\mathbb{F}$, $\mathbb{F} \cap \overline{\mathbb{Z}}$ is a ring in $\mathbb{F}$, and is called the ring of algebraic integers of $\mathbb{F}$. It is denoted as $\mathcal{O}_{\mathbb{F}}$.
- $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$.
- For any number field $\mathbb{F}$, $\mathbb{Q} \cap \mathcal{O}_{\mathbb{F}} = \mathbb{Z}$.
- The quotient field of $\mathcal{O}_{\mathbb{F}}$ is $\mathbb{F}$.
- $\mathcal{O}_{\mathbb{F}}$ is a Dedekind domain. That is,$\mathcal{O}_{\mathbb{F}}$ is an integral domain such that

More about algebraic integers

- $\overline{\mathbb{Z}}$ is a subring of $\overline{\mathbb{Q}}$.
- For a number field $\mathbb{F}$, $\mathbb{F} \cap \overline{\mathbb{Z}}$ is a ring in $\mathbb{F}$, and is called the ring of algebraic integers of $\mathbb{F}$. It is denoted as $\mathcal{O}_{\mathbb{F}}$.
- $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$.
- For any number field $\mathbb{F}$, $\mathbb{Q} \cap \mathcal{O}_{\mathbb{F}} = \mathbb{Z}$.
- The quotient field of $\mathcal{O}_{\mathbb{F}}$ is $\mathbb{F}$.
- $\mathcal{O}_{\mathbb{F}}$ is a Dedekind domain. That is,$\mathcal{O}_{\mathbb{F}}$ is an integral domain such that
  - every ideal of $\mathcal{O}_{\mathbb{F}}$ is finitely generated,

More about algebraic integers

- $\overline{\mathbb{Z}}$ is a subring of $\overline{\mathbb{Q}}$.
- For a number field $\mathbb{F}$, $\mathbb{F} \cap \overline{\mathbb{Z}}$ is a ring in $\mathbb{F}$, and is called the ring of algebraic integers of $\mathbb{F}$. It is denoted as $\mathcal{O}_{\mathbb{F}}$.
- $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$.
- For any number field $\mathbb{F}$, $\mathbb{Q} \cap \mathcal{O}_{\mathbb{F}} = \mathbb{Z}$.
- The quotient field of $\mathcal{O}_{\mathbb{F}}$ is $\mathbb{F}$.
- $\mathcal{O}_{\mathbb{F}}$ is a Dedekind domain. That is,$\mathcal{O}_{\mathbb{F}}$ is an integral domain such that
  - every ideal of $\mathcal{O}_{\mathbb{F}}$ is finitely generated,
  - every nonzero prime ideal of $\mathcal{O}_{\mathbb{F}}$ is maximal,

More about algebraic integers

- $\overline{\mathbb{Z}}$ is a subring of $\overline{\mathbb{Q}}$.
- For a number field $\mathbb{F}$, $\mathbb{F} \cap \overline{\mathbb{Z}}$ is a ring in $\mathbb{F}$, and is called the ring of algebraic integers of $\mathbb{F}$. It is denoted as $\mathcal{O}_{\mathbb{F}}$.
- $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$.
- For any number field $\mathbb{F}$, $\mathbb{Q} \cap \mathcal{O}_{\mathbb{F}} = \mathbb{Z}$.
- The quotient field of $\mathcal{O}_{\mathbb{F}}$ is $\mathbb{F}$.
- $\mathcal{O}_{\mathbb{F}}$ is a Dedekind domain. That is,$\mathcal{O}_{\mathbb{F}}$ is an integral domain such that
  - every ideal of $\mathcal{O}_{\mathbb{F}}$ is finitely generated,
  - every nonzero prime ideal of $\mathcal{O}_{\mathbb{F}}$ is maximal,
  - and $\mathcal{O}_{\mathbb{F}}$ is integrally closed in $\mathbb{F}$.

More about algebraic integers

- $\overline{\mathbb{Z}}$ is a subring of $\overline{\mathbb{Q}}$.
- For a number field $\mathbb{F}$, $\mathbb{F} \cap \overline{\mathbb{Z}}$ is a ring in $\mathbb{F}$, and is called the ring of algebraic integers of $\mathbb{F}$. It is denoted as $\mathcal{O}_{\mathbb{F}}$.
- $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$.
- For any number field $\mathbb{F}$, $\mathbb{Q} \cap \mathcal{O}_{\mathbb{F}} = \mathbb{Z}$.
- The quotient field of $\mathcal{O}_{\mathbb{F}}$ is $\mathbb{F}$.
- $\mathcal{O}_{\mathbb{F}}$ is a Dedekind domain. That is,$\mathcal{O}_{\mathbb{F}}$ is an integral domain such that
  - every ideal of $\mathcal{O}_{\mathbb{F}}$ is finitely generated,
  - every nonzero prime ideal of $\mathcal{O}_{\mathbb{F}}$ is maximal,
  - and $\mathcal{O}_{\mathbb{F}}$ is integrally closed in $\mathbb{F}$. That is, if $\alpha \in \mathbb{F}$ is a root of a polynomial in $\mathcal{O}_{\mathbb{F}}[x]$ of degree > 1, then $\alpha \in \mathcal{O}_{\mathbb{F}}$.

Embeddings and conjugate fields

Embeddings and conjugate fields

- Let $K = \mathbb{Q}(\theta)$ for some algebraic $\theta \in \overline{\mathbb{Q}}$. That is, there exists a minimal polynomial $f(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{Q}[x]$ such that $f(\theta) = 0$.

Embeddings and conjugate fields

- Let $K = \mathbb{Q}(\theta)$ for some algebraic $\theta \in \overline{\mathbb{Q}}$. That is, there exists a minimal polynomial $f(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{Q}[x]$ such that $f(\theta) = 0$.
- Let $\sigma : K \to \mathbb{C}$ be an **embedding**, that is, a function satisfying, for all $a, b \in K$,

Embeddings and conjugate fields

- Let $K = \mathbb{Q}(\theta)$ for some algebraic $\theta \in \overline{\mathbb{Q}}$. That is, there exists a minimal polynomial $f(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{Q}[x]$ such that $f(\theta) = 0$.
- Let $\sigma : K \to \mathbb{C}$ be an **embedding**, that is, a function satisfying, for all $a, b \in K$,
  - $\sigma(a + b) = \sigma(a) + \sigma(b)$,
  - $\sigma(ab) = \sigma(a)\sigma(b)$,
  - and $\sigma(r) = r$ for all $r \in \mathbb{Q}$.

Embeddings and conjugate fields

- Let $K = \mathbb{Q}(\theta)$ for some algebraic $\theta \in \overline{\mathbb{Q}}$. That is, there exists a minimal polynomial $f(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{Q}[x]$ such that $f(\theta) = 0$.
- Let $\sigma : K \to \mathbb{C}$ be an **embedding**, that is, a function satisfying, for all $a, b \in K$,
  - $\sigma(a + b) = \sigma(a) + \sigma(b)$,
  - $\sigma(ab) = \sigma(a)\sigma(b)$,
  - and $\sigma(r) = r$ for all $r \in \mathbb{Q}$.
- Also, $0 = \sigma(f(\theta)) = f(\sigma(\theta))$. That is, $\sigma(\theta)$ is a root of f for any embedding $\sigma : K \to \mathbb{C}$.

Embeddings and conjugate fields

- Let $K = \mathbb{Q}(\theta)$ for some algebraic $\theta \in \overline{\mathbb{Q}}$. That is, there exists a minimal polynomial $f(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{Q}[x]$ such that $f(\theta) = 0$.
- Let $\sigma : K \to \mathbb{C}$ be an **embedding**, that is, a function satisfying, for all $a, b \in K$,
  - $\sigma(a + b) = \sigma(a) + \sigma(b)$,
  - $\sigma(ab) = \sigma(a)\sigma(b)$,
  - and $\sigma(r) = r$ for all $r \in \mathbb{Q}$.
- Also, $0 = \sigma(f(\theta)) = f(\sigma(\theta))$. That is, $\sigma(\theta)$ is a root of f for any embedding $\sigma : K \to \mathbb{C}$.
- Thus, there are only n choices for $\sigma(\theta)$, namely the distinct roots $\theta^{(1)}, \theta^{(2)}, \ldots, \theta^{(n)}$ of $f(x)$. We denote each embedding as $\sigma^{(i)}$.

Embeddings and conjugate fields

- Let $K = \mathbb{Q}(\theta)$ for some algebraic $\theta \in \overline{\mathbb{Q}}$. That is, there exists a minimal polynomial $f(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{Q}[x]$ such that $f(\theta) = 0$.
- Let $\sigma : K \to \mathbb{C}$ be an **embedding**, that is, a function satisfying, for all $a, b \in K$,
  - $\sigma(a + b) = \sigma(a) + \sigma(b)$,
  - $\sigma(ab) = \sigma(a)\sigma(b)$,
  - and $\sigma(r) = r$ for all $r \in \mathbb{Q}$.
- Also, $0 = \sigma(f(\theta)) = f(\sigma(\theta))$. That is, $\sigma(\theta)$ is a root of f for any embedding $\sigma : K \to \mathbb{C}$.
- Thus, there are only n choices for $\sigma(\theta)$, namely the distinct roots $\theta^{(1)}, \theta^{(2)}, \ldots, \theta^{(n)}$ of $f(x)$. We denote each embedding as $\sigma^{(i)}$. The fields $K^{(i)} := \mathbb{Q}(\theta^{(i)})$ are called the conjugate fields of K.

Embeddings and conjugate fields

- Let $K = \mathbb{Q}(\theta)$ for some algebraic $\theta \in \overline{\mathbb{Q}}$. That is, there exists a minimal polynomial $f(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{Q}[x]$ such that $f(\theta) = 0$.
- Let $\sigma : K \to \mathbb{C}$ be an **embedding**, that is, a function satisfying, for all $a, b \in K$,
  - $\sigma(a + b) = \sigma(a) + \sigma(b)$,
  - $\sigma(ab) = \sigma(a)\sigma(b)$,
  - and $\sigma(r) = r$ for all $r \in \mathbb{Q}$.
- Also, $0 = \sigma(f(\theta)) = f(\sigma(\theta))$. That is, $\sigma(\theta)$ is a root of f for any embedding $\sigma : K \to \mathbb{C}$.
- Thus, there are only n choices for $\sigma(\theta)$, namely the distinct roots $\theta^{(1)}, \theta^{(2)}, \ldots, \theta^{(n)}$ of $f(x)$. We denote each embedding as $\sigma^{(i)}$. The fields $K^{(i)} := \mathbb{Q}(\theta^{(i)})$ are called the conjugate fields of K.

- Note that $\{1, \theta, \theta^2, \ldots, \theta^{n-1}\}$ is a $\mathbb{Q}$-basis of K. If $\sigma : K \to \mathbb{C}$ is an embedding, then

$$\sigma\left(\sum_{i=0}^{n-1} b_i \theta^i\right) = \sum_{i=0}^{n-1} b_i \sigma(\theta)^i .$$

- Note that $\{1, \theta, \theta^2, \ldots, \theta^{n-1}\}$ is a $\mathbb{Q}$-basis of K. If $\sigma : K \to \mathbb{C}$ is an embedding, then

$$\sigma\left(\sum_{i=0}^{n-1} b_i \theta^i\right) = \sum_{i=0}^{n-1} b_i \sigma(\theta)^i .$$

- If $\theta^{(i)}$ is real, we say that $K^{(i)}$ is a real embedding of K. Otherwise, $K^{(i)}$ is called a complex embedding of K.

- Note that $\{1, \theta, \theta^2, \ldots, \theta^{n-1}\}$ is a $\mathbb{Q}$-basis of K. If $\sigma : K \to \mathbb{C}$ is an embedding, then

$$\sigma\left(\sum_{i=0}^{n-1} b_i \theta^i\right) = \sum_{i=0}^{n-1} b_i \sigma(\theta)^i .$$

- If $\theta^{(i)}$ is real, we say that $K^{(i)}$ is a real embedding of K. Otherwise, $K^{(i)}$ is called a complex embedding of K.
- For example, consider $\mathbb{Q}(\sqrt{D})$. The embeddings are $\sigma(a + b\sqrt{D}) = a \pm b\sqrt{D}$.

- Note that $\{1, \theta, \theta^2, \ldots, \theta^{n-1}\}$ is a $\mathbb{Q}$-basis of K. If $\sigma : K \to \mathbb{C}$ is an embedding, then

$$\sigma\left(\sum_{i=0}^{n-1} b_i \theta^i\right) = \sum_{i=0}^{n-1} b_i \sigma\left(\theta\right)^i .$$

- If $\theta^{(i)}$ is real, we say that $K^{(i)}$ is a real embedding of K. Otherwise, $K^{(i)}$ is called a complex embedding of K.
- For example, consider $\mathbb{Q}(\sqrt{D})$. The embeddings are $\sigma(a + b\sqrt{D}) = a \pm b\sqrt{D}$. Also, the conjugate field of $\mathbb{Q}(\sqrt{D})$ is $\mathbb{Q}(\sqrt{D})$.

- Note that $\{1, \theta, \theta^2, \ldots, \theta^{n-1}\}$ is a $\mathbb{Q}$-basis of K. If $\sigma : K \to \mathbb{C}$ is an embedding, then

$$\sigma\left(\sum_{i=0}^{n-1} b_i \theta^i\right) = \sum_{i=0}^{n-1} b_i \sigma(\theta)^i .$$

- If $\theta^{(i)}$ is real, we say that $K^{(i)}$ is a real embedding of K. Otherwise, $K^{(i)}$ is called a complex embedding of K.
- For example, consider $\mathbb{Q}(\sqrt{D})$. The embeddings are $\sigma(a + b\sqrt{D}) = a \pm b\sqrt{D}$. Also, the conjugate field of $\mathbb{Q}(\sqrt{D})$ is $\mathbb{Q}(\sqrt{D})$.
- We call K a **Galois extension** of $\mathbb{Q}$ if all the conjugate fields of K are identical to K.

- Note that $\{1, \theta, \theta^2, \ldots, \theta^{n-1}\}$ is a $\mathbb{Q}$-basis of K. If $\sigma : K \to \mathbb{C}$ is an embedding, then

$$\sigma\left(\sum_{i=0}^{n-1} b_i \theta^i\right) = \sum_{i=0}^{n-1} b_i \sigma(\theta)^i.$$

- If $\theta^{(i)}$ is real, we say that $K^{(i)}$ is a real embedding of K. Otherwise, $K^{(i)}$ is called a complex embedding of K.
- For example, consider $\mathbb{Q}(\sqrt{D})$. The embeddings are $\sigma(a + b\sqrt{D}) = a \pm b\sqrt{D}$. Also, the conjugate field of $\mathbb{Q}(\sqrt{D})$ is $\mathbb{Q}(\sqrt{D})$.
- We call K a **Galois extension** of $\mathbb{Q}$ if all the conjugate fields of K are identical to K. Thus, any quadratic extension of $\mathbb{Q}$ is a Galois extension.

- Note that $\{1, \theta, \theta^2, \ldots, \theta^{n-1}\}$ is a $\mathbb{Q}$-basis of K. If $\sigma : K \to \mathbb{C}$ is an embedding, then

$$\sigma\left(\sum_{i=0}^{n-1} b_i \theta^i\right) = \sum_{i=0}^{n-1} b_i \sigma(\theta)^i .$$

- If $\theta^{(i)}$ is real, we say that $K^{(i)}$ is a real embedding of K. Otherwise, $K^{(i)}$ is called a complex embedding of K.
- For example, consider $\mathbb{Q}(\sqrt{D})$. The embeddings are $\sigma(a + b\sqrt{D}) = a \pm b\sqrt{D}$. Also, the conjugate field of $\mathbb{Q}(\sqrt{D})$ is $\mathbb{Q}(\sqrt{D})$.
- We call K a **Galois extension** of $\mathbb{Q}$ if all the conjugate fields of K are identical to K. Thus, any quadratic extension of $\mathbb{Q}$ is a Galois extension. Exercise: $\mathbb{Q}(^3\sqrt{2})$ is not a Galois extension of $\mathbb{Q}$.

- Note that $\{1, \theta, \theta^2, \ldots, \theta^{n-1}\}$ is a $\mathbb{Q}$-basis of K. If $\sigma : K \to \mathbb{C}$ is an embedding, then

$$\sigma\left(\sum_{i=0}^{n-1} b_i \theta^i\right) = \sum_{i=0}^{n-1} b_i \sigma(\theta)^i .$$

- If $\theta^{(i)}$ is real, we say that $K^{(i)}$ is a real embedding of K. Otherwise, $K^{(i)}$ is called a complex embedding of K.
- For example, consider $\mathbb{Q}(\sqrt{D})$. The embeddings are $\sigma(a + b\sqrt{D}) = a \pm b\sqrt{D}$. Also, the conjugate field of $\mathbb{Q}(\sqrt{D})$ is $\mathbb{Q}(\sqrt{D})$.
- We call K a **Galois extension** of $\mathbb{Q}$ if all the conjugate fields of K are identical to K. Thus, any quadratic extension of $\mathbb{Q}$ is a Galois extension. Exercise: $\mathbb{Q}(\sqrt[3]{2})$ is not a Galois extension of $\mathbb{Q}$.
- We can study the above notions for extensions K of an arbitrary number field $\mathbb{F}$, and define conjugate fields relative to $\mathbb{F}$ accordingly.

Norms and traces

Norms and traces

Let $[K : \mathbb{F}] = n$. We define $\text{Trace}_{K/\mathbb{F}}(\alpha)$ to be the sum of the conjugates of α. That is,

$$\text{Trace}_{K/\mathbb{F}}(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha).$$

Norms and traces

Let $[K:\mathbb{F}] = n$. We define $\text{Trace}_{K/\mathbb{F}}(\alpha)$ to be the sum of the conjugates of α. That is,

$$\text{Trace}_{K/\mathbb{F}}(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha).$$

We define $\text{Norm}_{K/\mathbb{F}}(\alpha)$ to be the product of the conjugates of α. That is,

$$\text{Trace}_{K/\mathbb{F}}(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha).$$

Norms and traces

Let $[K : \mathbb{F}] = n$. We define Trace $_{K/\mathbb{F}}(\alpha)$ to be the sum of the conjugates of α. That is,

$$\text{Trace}_{K/\mathbb{F}}(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha).$$

We define Norm $_{K/\mathbb{F}}(\alpha)$ to be the product of the conjugates of α. That is,

$$\text{Trace}_{K/\mathbb{F}}(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha).$$

For example, Trace $_{Q(\sqrt{D})/\mathbb{Q}}(a + b\sqrt{D}) = 2a$,

$$\text{Norm}_{Q(\sqrt{D})/\mathbb{Q}}(a + b\sqrt{D}) = a^2 - Db^2.$$

Norms and traces

Let $[K:\mathbb{F}] = n$. We define $\text{Trace}_{K/\mathbb{F}}(\alpha)$ to be the sum of the conjugates of α. That is,

$$\text{Trace}_{K/\mathbb{F}}(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha).$$

We define $\text{Norm}_{K/\mathbb{F}}(\alpha)$ to be the product of the conjugates of α. That is,

$$\text{Trace}_{K/\mathbb{F}}(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha).$$

For example, $\text{Trace}_{Q(\sqrt{D})/\mathbb{Q}}(a + b\sqrt{D}) = 2a$,

$$\text{Norm}_{Q(\sqrt{D})/\mathbb{Q}}(a + b\sqrt{D}) = a^2 - Db^2.$$

We often denote $\text{Trace}_{K/\mathbb{Q}}(\alpha)$ and $\text{Norm}_{K/\mathbb{Q}}(\alpha)$ as $\text{Trace}(\alpha)$ and $\text{Norm}(\alpha)$.

Norms and traces

Let $[K : \mathbb{F}] = n$. We define $\text{Trace}_{K/\mathbb{F}}(\alpha)$ to be the sum of the conjugates of α. That is,

$$\text{Trace}_{K/\mathbb{F}}(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha).$$

We define $\text{Norm}_{K/\mathbb{F}}(\alpha)$ to be the product of the conjugates of α. That is,

$$\text{Trace}_{K/\mathbb{F}}(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha).$$

For example, $\text{Trace}_{Q(\sqrt{D})/\mathbb{Q}}(a + b\sqrt{D}) = 2a$,

$$\text{Norm}_{Q(\sqrt{D})/\mathbb{Q}}(a + b\sqrt{D}) = a^2 - Db^2.$$

We often denote $\text{Trace}_{K/\mathbb{Q}}(\alpha)$ and $\text{Norm}_{K/\mathbb{Q}}(\alpha)$ as $\text{Trace}(\alpha)$ and $\text{Norm}(\alpha)$.

Structure of $\mathcal{O}_K$

Structure of $\mathcal{O}_K$

If $K = Q(\sqrt{D})$, what is $\mathcal{O}_K$?

Structure of $\mathcal{O}_K$

If $K = Q(\sqrt{D})$, what is $\mathcal{O}_K$?

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{D}] & \text{if } D \equiv 2, 3 \pmod 4 \\ \mathbb{Z}\left[\frac{1+\sqrt{D}}{2}\right] & \text{if } D \equiv 1 \pmod 4. \end{cases}$$

Structure of $\mathcal{O}_K$

If $K = Q(\sqrt{D})$, what is $\mathcal{O}_K$?

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{D}] & \text{if } D \equiv 2, 3 \pmod 4 \\ \mathbb{Z}\left[\frac{1+\sqrt{D}}{2}\right] & \text{if } D \equiv 1 \pmod 4). \end{cases}$$

More generally, if $[K : \mathbb{Q}] = n$, then there exist $\omega_1, \omega_2, \ldots, \omega_n \in \mathcal{O}_K$ such that

$$\mathcal{O}_K = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 + \ldots \mathbb{Z}\omega_n.$$

Structure of $\mathcal{O}_K$

If $K = Q(\sqrt{D})$, what is $\mathcal{O}_K$?

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{D}] & \text{if } D \equiv 2, 3 \pmod 4 \\ \mathbb{Z}\left[\frac{1+\sqrt{D}}{2}\right] & \text{if } D \equiv 1 \pmod 4). \end{cases}$$

More generally, if $[K : \mathbb{Q}] = n$, then there exist $\omega_1, \omega_2, \ldots, \omega_n \in \mathcal{O}_K$ such that

$$\mathcal{O}_K = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 + \ldots \mathbb{Z}\omega_n.$$

That is, $\{\omega_1, \omega_2, \ldots, \omega_n\}$ forms an integral basis of

Structure of $\mathcal{O}_K$

If $K = Q(\sqrt{D})$, what is $\mathcal{O}_K$?

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{D}] & \text{if } D \equiv 2, 3 \pmod 4 \\ \mathbb{Z}\left[\frac{1+\sqrt{D}}{2}\right] & \text{if } D \equiv 1 \pmod 4). \end{cases}$$

More generally, if $[K : \mathbb{Q}] = n$, then there exist $\omega_1, \omega_2, \ldots, \omega_n \in \mathcal{O}_K$ such that

$$\mathcal{O}_K = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 + \ldots \mathbb{Z}\omega_n.$$

That is, $\{\omega_1, \omega_2, \ldots, \omega_n\}$ forms an integral basis of $\mathcal{O}_K$.

Structure of $\mathcal{O}_K$

If $K = Q(\sqrt{D})$, what is $\mathcal{O}_K$?

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{D}] & \text{if } D \equiv 2, 3 \pmod 4 \\ \mathbb{Z}\left[\frac{1+\sqrt{D}}{2}\right] & \text{if } D \equiv 1 \pmod 4. \end{cases}$$

More generally, if $[K : \mathbb{Q}] = n$, then there exist $\omega_1, \omega_2, \ldots, \omega_n \in \mathcal{O}_K$ such that

$$\mathcal{O}_K = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 + \ldots \mathbb{Z}\omega_n.$$

That is, $\{\omega_1, \omega_2, \ldots, \omega_n\}$ forms an integral basis of $\mathcal{O}_K$.

Let ζ denote a primitive p-th root of unity and $K = \mathbb{Q}(\zeta)$. Then, $1, \zeta, \ldots, \zeta^{p-2}$ forms an integral basis of K.

Discriminant of a number field

Discriminant of a number field

Definition

Let $[K : \mathbb{Q}] = n$ *and suppose* $\{\omega_1, \omega_2, \ldots, \omega_n\}$ *is an integral basis of* $\mathcal{O}_K$*.*

Discriminant of a number field

Definition

Let $[K : \mathbb{Q}] = n$ and suppose $\{\omega_1, \omega_2, \ldots, \omega_n\}$ is an integral basis of $\mathcal{O}_K$. The **discriminant** *of K, d_K is defined as*

$$d_K := \det(\sigma_j(\omega_i))^2.$$

Discriminant of a number field

Definition

Let $[K : \mathbb{Q}] = n$ *and suppose* $\{\omega_1, \omega_2, \ldots, \omega_n\}$ *is an integral basis of* $\mathcal{O}_K$*. The* **discriminant** *of* K*,* d_K *is defined as*

$$d_K := \det(\sigma_j(\omega_i))^2.$$

The discriminant is well-defined. That is, the discriminant is independent of the choice of integral basis of K.

Discriminant of a number field

Definition

Let $[K:\mathbb{Q}] = n$ and suppose $\{\omega_1, \omega_2, \ldots, \omega_n\}$ is an integral basis of $\mathcal{O}_K$. The **discriminant** *of K, d_K is defined as*

$$d_K := \det(\sigma_j(\omega_i))^2.$$

The discriminant is well-defined. That is, the discriminant is independent of the choice of integral basis of K.
If $K = \mathbb{Q}(\sqrt{D})$ and $D \equiv 1 \pmod 4$, consider the integral basis $\{1, \frac{1+\sqrt{D}}{2}\}$. Then,

$$d_K = \left(\det \begin{bmatrix} 1 & (1+\sqrt{D})/2 \\ 1 & (1-\sqrt{D})/2 \end{bmatrix}\right)^2 = D.$$

Discriminant of a number field

Definition

Let $[K:\mathbb{Q}] = n$ and suppose $\{\omega_1, \omega_2, \ldots, \omega_n\}$ is an integral basis of $\mathcal{O}_K$. The **discriminant** *of K, d_K is defined as*

$$d_K := \det(\sigma_j(\omega_i))^2.$$

The discriminant is well-defined. That is, the discriminant is independent of the choice of integral basis of K.
If $K = \mathbb{Q}(\sqrt{D})$ and $D \equiv 1 \pmod 4$, consider the integral basis $\{1, \frac{1+\sqrt{D}}{2}\}$. Then,

$$d_K = \left(\det \begin{bmatrix} 1 & (1+\sqrt{D})/2 \\ 1 & (1-\sqrt{D})/2 \end{bmatrix}\right)^2 = D.$$

Also, $d_K = 4D$ if $D \not\equiv 1 \pmod 4$.

- We can generalize the notion of a discriminant for arbitrary elements of K.

- We can generalize the notion of a discriminant for arbitrary elements of K. Suppose $\{a_1, a_2, \dots, a_n\} \subset K$.

- We can generalize the notion of a discriminant for arbitrary elements of K. Suppose $\{a_1, a_2, \ldots, a_n\} \subset K$. We define

$$d_{K/\mathbb{Q}}(a_1, a_2, \ldots, a_n) := \det(\sigma_j(a_i))^2.$$

- We can generalize the notion of a discriminant for arbitrary elements of K. Suppose $\{a_1, a_2, \ldots, a_n\} \subset K$. We define

$$d_{K/\mathbb{Q}}(a_1, a_2, \ldots, a_n) := \det(\sigma_j(a_i))^2.$$

- It can be shown that

$$d_{K/\mathbb{Q}}(a) := d_{K/\mathbb{Q}}(1, a, a^2, \ldots, a^{n-1}) = \prod_{1\leq j<k\leq n} (\sigma_j(a) - \sigma_k(a))^2.$$

- We can generalize the notion of a discriminant for arbitrary elements of K. Suppose $\{a_1, a_2, \ldots, a_n\} \subset K$. We define

$$d_{K/\mathbb{Q}}(a_1, a_2, \ldots, a_n) := \det(\sigma_j(a_i))^2.$$

- It can be shown that

$$d_{K/\mathbb{Q}}(a) := d_{K/\mathbb{Q}}(1, a, a^2, \ldots, a^{n-1}) = \prod_{1\leq j<k\leq n} (\sigma_j(a) - \sigma_k(a))^2.$$

- In particular, let $K = \mathbb{Q}(\zeta_m)$.

- We can generalize the notion of a discriminant for arbitrary elements of K. Suppose $\{a_1, a_2, \ldots, a_n\} \subset K$. We define

$$d_{K/\mathbb{Q}}(a_1, a_2, \ldots, a_n) := \det(\sigma_j(a_i))^2.$$

- It can be shown that

$$d_{K/\mathbb{Q}}(a) := d_{K/\mathbb{Q}}(1, a, a^2, \ldots, a^{n-1}) = \prod_{1 \leq j < k \leq n} (\sigma_j(a) - \sigma_k(a))^2.$$

- In particular, let $K = \mathbb{Q}(\zeta_m)$. Then, $\{1, \zeta_m, \ldots, \zeta_m^{\phi(m)-1}\}$ is an integral basis of $\mathcal{O}_K$.

- We can generalize the notion of a discriminant for arbitrary elements of K. Suppose $\{a_1, a_2, \ldots, a_n\} \subset K$. We define

$$d_{K/\mathbb{Q}}(a_1, a_2, \ldots, a_n) := \det(\sigma_j(a_i))^2.$$

- It can be shown that

$$d_{K/\mathbb{Q}}(a) := d_{K/\mathbb{Q}}(1, a, a^2, \ldots, a^{n-1}) = \prod_{1 \le j < k \le n} (\sigma_j(a) - \sigma_k(a))^2.$$

- In particular, let $K = \mathbb{Q}(\zeta_m)$. Then, $\{1, \zeta_m, \ldots, \zeta_m^{\phi(m)-1}\}$ is an integral basis of $\mathcal{O}_K$. By applying the above formula,

$$d_K = \frac{(-1)^{\phi(m)/2} m^{\phi(m)}}{\prod_{p|m} p^{\phi(m)/(p-1)}}.$$

- We can generalize the notion of a discriminant for arbitrary elements of K. Suppose $\{a_1, a_2, \ldots, a_n\} \subset K$. We define

$$d_{K/\mathbb{Q}}(a_1, a_2, \ldots, a_n) := \det(\sigma_j(a_i))^2.$$

- It can be shown that

$$d_{K/\mathbb{Q}}(a) := d_{K/\mathbb{Q}}(1, a, a^2, \ldots, a^{n-1}) = \prod_{1 \leq j < k \leq n} (\sigma_j(a) - \sigma_k(a))^2.$$

- In particular, let $K = \mathbb{Q}(\zeta_m)$. Then, $\{1, \zeta_m, \ldots, \zeta_m^{\phi(m)-1}\}$ is an integral basis of $\mathcal{O}_K$. By applying the above formula,

$$d_K = \frac{(-1)^{\phi(m)/2} m^{\phi(m)}}{\prod_{p|m} p^{\phi(m)/(p-1)}}.$$

- Let K be an algebraic number field. If $d_{K/\mathbb{Q}}(\theta)$ is squarefree, then $\mathcal{O}_K = \mathbb{Z}[\theta]$.

- We can generalize the notion of a discriminant for arbitrary elements of K. Suppose $\{a_1, a_2, \ldots, a_n\} \subset K$. We define

$$d_{K/\mathbb{Q}}(a_1, a_2, \ldots, a_n) := \det(\sigma_j(a_i))^2.$$

- It can be shown that

$$d_{K/\mathbb{Q}}(a) := d_{K/\mathbb{Q}}(1, a, a^2, \ldots, a^{n-1}) = \prod_{1 \leq j < k \leq n} (\sigma_j(a) - \sigma_k(a))^2.$$

- In particular, let $K = \mathbb{Q}(\zeta_m)$. Then, $\{1, \zeta_m, \ldots, \zeta_m^{\phi(m)-1}\}$ is an integral basis of $\mathcal{O}_K$. By applying the above formula,

$$d_K = \frac{(-1)^{\phi(m)/2} m^{\phi(m)}}{\prod_{p|m} p^{\phi(m)/(p-1)}}.$$

- Let K be an algebraic number field. If $d_{K/\mathbb{Q}}(\theta)$ is squarefree, then $\mathcal{O}_K = \mathbb{Z}[\theta]$.

Ideals in $\mathcal{O}_K$

Ideals in $\mathcal{O}_K$

- So far, we have seen how $\mathcal{O}_K$ can be seen as a generalization of $\mathbb{Z}$.

Ideals in $\mathcal{O}_K$

- So far, we have seen how $\mathcal{O}_K$ can be seen as a generalization of $\mathbb{Z}$.
- To draw a meaningful generalization of the unique factorization of integers into prime powers in $\mathbb{Z}$, we have to treat ideals in $\mathcal{O}_K$ and discuss the factorization of ideals into prime ideals of $\mathcal{O}_K$.

Ideals in $\mathcal{O}_K$

- So far, we have seen how $\mathcal{O}_K$ can be seen as a generalization of $\mathbb{Z}$.
- To draw a meaningful generalization of the unique factorization of integers into prime powers in $\mathbb{Z}$, we have to treat ideals in $\mathcal{O}_K$ and discuss the factorization of ideals into prime ideals of $\mathcal{O}_K$.
- We recall the following fundamental facts:
  - Any ideal in $\mathcal{O}_K$ has an integral basis.

Ideals in $\mathcal{O}_K$

- So far, we have seen how $\mathcal{O}_K$ can be seen as a generalization of $\mathbb{Z}$.
- To draw a meaningful generalization of the unique factorization of integers into prime powers in $\mathbb{Z}$, we have to treat ideals in $\mathcal{O}_K$ and discuss the factorization of ideals into prime ideals of $\mathcal{O}_K$.
- We recall the following fundamental facts:
  - Any ideal in $\mathcal{O}_K$ has an integral basis.
  - Any nonzero ideal $\mathfrak{a}$ in $\mathcal{O}_K$ has finite index $|\mathcal{O}_K/\mathfrak{a}|$ in $\mathcal{O}_K$.

Ideals in $\mathcal{O}_K$

- So far, we have seen how $\mathcal{O}_K$ can be seen as a generalization of $\mathbb{Z}$.
- To draw a meaningful generalization of the unique factorization of integers into prime powers in $\mathbb{Z}$, we have to treat ideals in $\mathcal{O}_K$ and discuss the factorization of ideals into prime ideals of $\mathcal{O}_K$.
- We recall the following fundamental facts:
  - Any ideal in $\mathcal{O}_K$ has an integral basis.
  - Any nonzero ideal $\mathfrak{a}$ in $\mathcal{O}_K$ has finite index $|\mathcal{O}_K/\mathfrak{a}|$ in $\mathcal{O}_K$. We define the norm of a nonzero ideal in $\mathcal{O}_K$ to be its index $|\mathcal{O}_K/\mathfrak{a}|$ and denote it as $N(\mathfrak{a})$.

Ideals in $\mathcal{O}_K$

- So far, we have seen how $\mathcal{O}_K$ can be seen as a generalization of $\mathbb{Z}$.
- To draw a meaningful generalization of the unique factorization of integers into prime powers in $\mathbb{Z}$, we have to treat ideals in $\mathcal{O}_K$ and discuss the factorization of ideals into prime ideals of $\mathcal{O}_K$.
- We recall the following fundamental facts:
  - Any ideal in $\mathcal{O}_K$ has an integral basis.
  - Any nonzero ideal $\mathfrak{a}$ in $\mathcal{O}_K$ has finite index $|\mathcal{O}_K/\mathfrak{a}|$ in $\mathcal{O}_K$. We define the norm of a nonzero ideal in $\mathcal{O}_K$ to be its index $|\mathcal{O}_K/\mathfrak{a}|$ and denote it as $N(\mathfrak{a})$.
- If $\alpha \in \mathcal{O}_K$, then $N(\langle\alpha\rangle) = |N(\alpha)|$.

Prime ideals in $\mathcal{O}_K$

Prime ideals in $\mathcal{O}_K$

- Exercise: For any nonzero ideal $\mathfrak{a}$ in $\mathcal{O}_K$, $\mathfrak{a} \cap \mathbb{Z}$ must contain a nonzero integer.

Prime ideals in $\mathcal{O}_K$

- Exercise: For any nonzero ideal $\mathfrak{a}$ in $\mathcal{O}_K$, $\mathfrak{a} \cap \mathbb{Z}$ must contain a nonzero integer.
- By the definition of a prime ideal $\mathfrak{p}$, if $ab \in \mathfrak{p}$, then either $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$.

Prime ideals in $\mathcal{O}_K$

- Exercise: For any nonzero ideal $\mathfrak{a}$ in $\mathcal{O}_K$, $\mathfrak{a} \cap \mathbb{Z}$ must contain a nonzero integer.
- By the definition of a prime ideal $\mathfrak{p}$, if $ab \in \mathfrak{p}$, then either $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$.
- Thus, $\mathfrak{p}$ must contain some rational prime.

Prime ideals in $\mathcal{O}_K$

- Exercise: For any nonzero ideal $\mathfrak{a}$ in $\mathcal{O}_K$, $\mathfrak{a} \cap \mathbb{Z}$ must contain a nonzero integer.
- By the definition of a prime ideal $\mathfrak{p}$, if $ab \in \mathfrak{p}$, then either $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$.
- Thus, $\mathfrak{p}$ must contain some rational prime. But, if $\mathfrak{p}$ contains two rational primes p and q, then it would contain their greatest common divisor 1.

Prime ideals in $\mathcal{O}_K$

- Exercise: For any nonzero ideal $\mathfrak{a}$ in $\mathcal{O}_K$, $\mathfrak{a} \cap \mathbb{Z}$ must contain a nonzero integer.
- By the definition of a prime ideal $\mathfrak{p}$, if $ab \in \mathfrak{p}$, then either $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$.
- Thus, $\mathfrak{p}$ must contain some rational prime. But, if $\mathfrak{p}$ contains two rational primes p and q, then it would contain their greatest common divisor 1. This contradicts the nontriviality of $\mathfrak{p}$.

Prime ideals in $\mathcal{O}_K$

- Exercise: For any nonzero ideal $\mathfrak{a}$ in $\mathcal{O}_K$, $\mathfrak{a} \cap \mathbb{Z}$ must contain a nonzero integer.
- By the definition of a prime ideal $\mathfrak{p}$, if $ab \in \mathfrak{p}$, then either $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$.
- Thus, $\mathfrak{p}$ must contain some rational prime. But, if $\mathfrak{p}$ contains two rational primes p and q, then it would contain their greatest common divisor 1. This contradicts the nontriviality of $\mathfrak{p}$. Thus, $\mathfrak{p}$ can contain exactly one rational prime p.

Prime ideals in $\mathcal{O}_K$

- Exercise: For any nonzero ideal $\mathfrak{a}$ in $\mathcal{O}_K$, $\mathfrak{a} \cap \mathbb{Z}$ must contain a nonzero integer.
- By the definition of a prime ideal $\mathfrak{p}$, if $ab \in \mathfrak{p}$, then either $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$.
- Thus, $\mathfrak{p}$ must contain some rational prime. But, if $\mathfrak{p}$ contains two rational primes p and q, then it would contain their greatest common divisor 1. This contradicts the nontriviality of $\mathfrak{p}$. Thus, $\mathfrak{p}$ can contain exactly one rational prime p. We say that p lies below $\mathfrak{p}$.

Prime ideals in $\mathcal{O}_K$

- Exercise: For any nonzero ideal $\mathfrak{a}$ in $\mathcal{O}_K$, $\mathfrak{a} \cap \mathbb{Z}$ must contain a nonzero integer.
- By the definition of a prime ideal $\mathfrak{p}$, if $ab \in \mathfrak{p}$, then either $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$.
- Thus, $\mathfrak{p}$ must contain some rational prime. But, if $\mathfrak{p}$ contains two rational primes p and q, then it would contain their greatest common divisor 1. This contradicts the nontriviality of $\mathfrak{p}$. Thus, $\mathfrak{p}$ can contain exactly one rational prime p. We say that p lies below $\mathfrak{p}$.
- In this case, $\langle p \rangle = \mathfrak{p}\mathfrak{q}$ for an integral ideal $\mathfrak{q}$ of $\mathcal{O}_K$.

Prime ideals in $\mathcal{O}_K$

- Exercise: For any nonzero ideal $\mathfrak{a}$ in $\mathcal{O}_K$, $\mathfrak{a} \cap \mathbb{Z}$ must contain a nonzero integer.
- By the definition of a prime ideal $\mathfrak{p}$, if $ab \in \mathfrak{p}$, then either $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$.
- Thus, $\mathfrak{p}$ must contain some rational prime. But, if $\mathfrak{p}$ contains two rational primes p and q, then it would contain their greatest common divisor 1. This contradicts the nontriviality of $\mathfrak{p}$. Thus, $\mathfrak{p}$ can contain exactly one rational prime p. We say that p lies below $\mathfrak{p}$.
- In this case, $\langle p \rangle = \mathfrak{p}\mathfrak{q}$ for an integral ideal $\mathfrak{q}$ of $\mathcal{O}_K$. Thus, $N(\mathfrak{p})$ must divide $N(\langle p \rangle) = |N(p)|$.

Prime ideals in $\mathcal{O}_K$

- Exercise: For any nonzero ideal $\mathfrak{a}$ in $\mathcal{O}_K$, $\mathfrak{a} \cap \mathbb{Z}$ must contain a nonzero integer.
- By the definition of a prime ideal $\mathfrak{p}$, if $ab \in \mathfrak{p}$, then either $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$.
- Thus, $\mathfrak{p}$ must contain some rational prime. But, if $\mathfrak{p}$ contains two rational primes p and q, then it would contain their greatest common divisor 1. This contradicts the nontriviality of $\mathfrak{p}$. Thus, $\mathfrak{p}$ can contain exactly one rational prime p. We say that p lies below $\mathfrak{p}$.
- In this case, $\langle p \rangle = \mathfrak{p}\mathfrak{q}$ for an integral ideal $\mathfrak{q}$ of $\mathcal{O}_K$. Thus, $N(\mathfrak{p})$ must divide $N(\langle p \rangle) = |N(p)|$. As $p^{(i)} = p$ for each i, $|N(p)| = p^{[K:\mathbb{Q}]}$.

Prime ideals in $\mathcal{O}_K$

- Exercise: For any nonzero ideal $\mathfrak{a}$ in $\mathcal{O}_K$, $\mathfrak{a} \cap \mathbb{Z}$ must contain a nonzero integer.
- By the definition of a prime ideal $\mathfrak{p}$, if $ab \in \mathfrak{p}$, then either $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$.
- Thus, $\mathfrak{p}$ must contain some rational prime. But, if $\mathfrak{p}$ contains two rational primes p and q, then it would contain their greatest common divisor 1. This contradicts the nontriviality of $\mathfrak{p}$. Thus, $\mathfrak{p}$ can contain exactly one rational prime p. We say that p lies below $\mathfrak{p}$.
- In this case, $\langle p \rangle = \mathfrak{p}\mathfrak{q}$ for an integral ideal $\mathfrak{q}$ of $\mathcal{O}_K$. Thus, $N(\mathfrak{p})$ must divide $N(\langle p \rangle) = |N(p)|$. As $p^{(i)} = p$ for each i, $|N(p)| = p^{[K:\mathbb{Q}]}$. Thus, $N(\mathfrak{p}) = p^f$ for some $1 \leq f \leq [K : \mathbb{Q}]$.

Prime ideals in $\mathcal{O}_K$

- Exercise: For any nonzero ideal $\mathfrak{a}$ in $\mathcal{O}_K$, $\mathfrak{a} \cap \mathbb{Z}$ must contain a nonzero integer.
- By the definition of a prime ideal $\mathfrak{p}$, if $ab \in \mathfrak{p}$, then either $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$.
- Thus, $\mathfrak{p}$ must contain some rational prime. But, if $\mathfrak{p}$ contains two rational primes p and q, then it would contain their greatest common divisor 1. This contradicts the nontriviality of $\mathfrak{p}$. Thus, $\mathfrak{p}$ can contain exactly one rational prime p. We say that p lies below $\mathfrak{p}$.
- In this case, $\langle p \rangle = \mathfrak{p}\mathfrak{q}$ for an integral ideal $\mathfrak{q}$ of $\mathcal{O}_K$. Thus, $N(\mathfrak{p})$ must divide $N(\langle p \rangle) = |N(p)|$. As $p^{(i)} = p$ for each i, $|N(p)| = p^{[K:\mathbb{Q}]}$. Thus, $N(\mathfrak{p}) = p^f$ for some $1 \leq f \leq [K:\mathbb{Q}]$.
- f is called the **inertial degree** of $\mathfrak{p}$ in $\mathcal{O}_K$.

Factoring primes in a number field

Theorem (Unique factorization of ideals in $\mathcal{O}_K$)

Every proper nonzero ideal $\mathfrak{a}$ in $\mathcal{O}_K$ is uniquely representable as a product of prime ideals.

Factoring primes in a number field

Theorem (Unique factorization of ideals in $\mathcal{O}_K$)

Every proper nonzero ideal $\mathfrak{a}$ in $\mathcal{O}_K$ is uniquely representable as a product of prime ideals. That is,

$$\mathfrak{a} = \mathfrak{p}_1^{a_1}\mathfrak{p}_2^{a_2}\dots\mathfrak{p}_l^{a_l},$$

where $\mathfrak{p}_l$'s are the distinct prime ideals of $\mathcal{O}_K$ containing $\mathfrak{a}$, and $a_l \in \mathbb{N}$. This factorization is unique up to the order of the factors.

Factoring primes in a number field

Theorem (Unique factorization of ideals in $\mathcal{O}_K$)

Every proper nonzero ideal $\mathfrak{a}$ in $\mathcal{O}_K$ is uniquely representable as a product of prime ideals. That is,

$$\mathfrak{a} = \mathfrak{p}_1^{a_1}\mathfrak{p}_2^{a_2}\ldots\mathfrak{p}_l^{a_l},$$

where $\mathfrak{p}_l$'s are the distinct prime ideals of $\mathcal{O}_K$ containing $\mathfrak{a}$, and $a_l \in \mathbb{N}$. This factorization is unique up to the order of the factors.

Let $[K:\mathbb{Q}] = n$. Suppose, for a rational prime p,

$$\langle p\rangle = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\ldots\mathfrak{p}_l^{e_l}.$$

Factoring primes in a number field

Theorem (Unique factorization of ideals in $\mathcal{O}_K$)

Every proper nonzero ideal $\mathfrak{a}$ in $\mathcal{O}_K$ is uniquely representable as a product of prime ideals. That is,

$$\mathfrak{a} = \mathfrak{p}_1^{a_1}\mathfrak{p}_2^{a_2}\dots\mathfrak{p}_l^{a_l},$$

where $\mathfrak{p}_l$'s are the distinct prime ideals of $\mathcal{O}_K$ containing $\mathfrak{a}$, and $a_l \in \mathbb{N}$. This factorization is unique up to the order of the factors.

Let $[K : \mathbb{Q}] = n$. Suppose, for a rational prime p,

$$\langle p \rangle = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\dots\mathfrak{p}_l^{e_l}.$$

Suppose f_i is the inertial degree of $\mathfrak{p}_i$.

Factoring primes in a number field

Theorem (Unique factorization of ideals in $\mathcal{O}_K$)

Every proper nonzero ideal $\mathfrak{a}$ in $\mathcal{O}_K$ is uniquely representable as a product of prime ideals. That is,

$$\mathfrak{a} = \mathfrak{p}_1^{a_1}\mathfrak{p}_2^{a_2}\dots\mathfrak{p}_l^{a_l},$$

where $\mathfrak{p}_l$'s are the distinct prime ideals of $\mathcal{O}_K$ containing $\mathfrak{a}$, and $a_l \in \mathbb{N}$. This factorization is unique up to the order of the factors.

Let $[K:\mathbb{Q}] = n$. Suppose, for a rational prime p,

$$\langle p \rangle = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\dots\mathfrak{p}_l^{e_l}.$$

Suppose f_i is the inertial degree of $\mathfrak{p}_i$. Then, $\sum_{i=1}^{l} e_i f_i = n$.

Factoring primes in a number field

Theorem (Unique factorization of ideals in $\mathcal{O}_K$)

Every proper nonzero ideal $\mathfrak{a}$ in $\mathcal{O}_K$ is uniquely representable as a product of prime ideals. That is,

$$\mathfrak{a} = \mathfrak{p}_1^{a_1}\mathfrak{p}_2^{a_2}\ldots\mathfrak{p}_l^{a_l},$$

where $\mathfrak{p}_l$'s are the distinct prime ideals of $\mathcal{O}_K$ containing $\mathfrak{a}$, and $a_l \in \mathbb{N}$. This factorization is unique up to the order of the factors.

Let $[K : \mathbb{Q}] = n$. Suppose, for a rational prime p,

$$\langle p\rangle = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\ldots\mathfrak{p}_l^{e_l}.$$

Suppose f_i is the inertial degree of $\mathfrak{p}_i$. Then, $\sum_{i=1}^{l} e_i f_i = n$. Note that e_i is called the **ramification index of** $\mathfrak{p}_i$ in K (that is, $\mathfrak{p}_i^{e_i}|\langle p\rangle$, and $\mathfrak{p}_i^{e_i+1} \nmid \langle p\rangle$).

Factoring primes in a number field

Theorem (Unique factorization of ideals in $\mathcal{O}_K$)

Every proper nonzero ideal $\mathfrak{a}$ in $\mathcal{O}_K$ is uniquely representable as a product of prime ideals. That is,

$$\mathfrak{a} = \mathfrak{p}_1^{a_1}\mathfrak{p}_2^{a_2}\dots\mathfrak{p}_l^{a_l},$$

where $\mathfrak{p}_l$'s are the distinct prime ideals of $\mathcal{O}_K$ containing $\mathfrak{a}$, and $a_l \in \mathbb{N}$. This factorization is unique up to the order of the factors.

Let $[K : \mathbb{Q}] = n$. Suppose, for a rational prime p,

$$\langle p \rangle = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\dots\mathfrak{p}_l^{e_l}.$$

Suppose f_i is the inertial degree of $\mathfrak{p}_i$. Then, $\sum_{i=1}^{l} e_i f_i = n$. Note that e_i is called the **ramification index of** $\mathfrak{p}_i$ in K (that is, $\mathfrak{p}_i^{e_i} | \langle p \rangle$, and $\mathfrak{p}_i^{e_i+1} \nmid \langle p \rangle$).
Also, l is called the **decomposition number of** p in K and it can be shown that $l \leq n$.

Ramification

Ramification

Definition

Let $[K:\mathbb{Q}] = n$*, and let* p *be a rational prime. Let* $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_l$ *be the prime ideals in* $\mathcal{O}_K$ *lying above* p*. That is,*

Ramification

Definition

Let $[K : \mathbb{Q}] = n$*, and let* p *be a rational prime. Let* $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_l$ *be the prime ideals in* $\mathcal{O}_K$ *lying above* p*. That is,*

$$\langle p \rangle = \mathfrak{p}_1^{e_1} \mathfrak{p}_2^{e_2} \ldots \mathfrak{p}_l^{e_l}.$$

Ramification

Definition

Let $[K:\mathbb{Q}] = n$, and let p be a rational prime. Let $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_l$ be the prime ideals in $\mathcal{O}_K$ lying above p. That is,

$$\langle p \rangle = \mathfrak{p}_1^{e_1} \mathfrak{p}_2^{e_2} \ldots \mathfrak{p}_l^{e_l}.$$

If $e_i > 1$ for some $1 \leq i \leq l$, then p is said to ramify in K. If $e_i = 1$ for all i, then p is said to be unramified in K.

Ramification

Definition

Let $[K : \mathbb{Q}] = n$*, and let* p *be a rational prime. Let* $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_l$ *be the prime ideals in* $\mathcal{O}_K$ *lying above* p*. That is,*

$$\langle p \rangle = \mathfrak{p}_1^{e_1} \mathfrak{p}_2^{e_2} \ldots \mathfrak{p}_l^{e_l}.$$

If $e_i > 1$ *for some* $1 \leq i \leq l$*, then* p *is said to ramify in* K*. If* $e_i = 1$ *for all* i*, then* p *is said to be unramified in* K*.*

Theorem (**Dedekind**)

A rational prime p *ramifies in* K *if and only if* $p | d(K)$*.*

Factoring primes in a quadratic field

Factoring primes in a quadratic field

Theorem

Let $K = \mathbb{Q}(\sqrt{D})$, and let $p \in \mathbb{Z}$ be a prime.

Factoring primes in a quadratic field

Theorem

Let $K = \mathbb{Q}(\sqrt{D})$*, and let* $p \in \mathbb{Z}$ *be a prime. Then,*

1. $\langle p \rangle = \mathfrak{p}_1\mathfrak{p}_2$ *if* $p > 2$, $(D/p) = 1$*. Here,* $N(\mathfrak{p}_1) = N(\mathfrak{p}_2) = p$*.*

Factoring primes in a quadratic field

Theorem

Let $K = \mathbb{Q}(\sqrt{D})$, and let $p \in \mathbb{Z}$ be a prime. Then,

1. $\langle p \rangle = \mathfrak{p}_1\mathfrak{p}_2$ *if* $p > 2$, $(D/p) = 1$. *Here,* $N(\mathfrak{p}_1) = N(\mathfrak{p}_2) = p$.
2. $\langle p \rangle = \mathfrak{p}$ *if* $p > 2$, *and* $(D/p) = -1$. *Here,* $N(\mathfrak{p}) = p^2$.

Factoring primes in a quadratic field

Theorem

Let $K = \mathbb{Q}(\sqrt{D})$, and let $p \in \mathbb{Z}$ be a prime. Then,

1. $\langle p \rangle = \mathfrak{p}_1\mathfrak{p}_2$ *if* $p > 2$, $(D/p) = 1$. *Here,* $N(\mathfrak{p}_1) = N(\mathfrak{p}_2) = p$.
2. $\langle p \rangle = \mathfrak{p}$ *if* $p > 2$, *and* $(D/p) = -1$. *Here,* $N(\mathfrak{p}) = p^2$.
3. $\langle p \rangle = \mathfrak{p}^2$ *if* $p > 2$, *and* $p | D$. *Here,* $N(\mathfrak{p}) = p$.

Factoring primes in a quadratic field

Theorem

Let $K = \mathbb{Q}(\sqrt{D})$, and let $p \in \mathbb{Z}$ be a prime. Then,

1. $\langle p \rangle = \mathfrak{p}_1\mathfrak{p}_2$ *if* $p > 2$, $(D/p) = 1$. *Here,* $N(\mathfrak{p}_1) = N(\mathfrak{p}_2) = p$.
2. $\langle p \rangle = \mathfrak{p}$ *if* $p > 2$, *and* $(D/p) = -1$. *Here,* $N(\mathfrak{p}) = p^2$.
3. $\langle p \rangle = \mathfrak{p}^2$ *if* $p > 2$, *and* $p|D$. *Here,* $N(\mathfrak{p}) = p$.
4. $\langle p \rangle = \mathfrak{p}_1\mathfrak{p}_2$ *if* $p = 2$ *and* $D \equiv 1 (\text{mod } 8)$. *Here,* $N(\mathfrak{p}_1) = N(\mathfrak{p}_2) = p$.

Factoring primes in a quadratic field

Theorem

Let $K = \mathbb{Q}(\sqrt{D})$, and let $p \in \mathbb{Z}$ be a prime. Then,

1. $\langle p \rangle = \mathfrak{p}_1\mathfrak{p}_2$ *if* $p > 2$, $(D/p) = 1$. *Here,* $N(\mathfrak{p}_1) = N(\mathfrak{p}_2) = p$.
2. $\langle p \rangle = \mathfrak{p}$ *if* $p > 2$, *and* $(D/p) = -1$. *Here,* $N(\mathfrak{p}) = p^2$.
3. $\langle p \rangle = \mathfrak{p}^2$ *if* $p > 2$, *and* $p | D$. *Here,* $N(\mathfrak{p}) = p$.
4. $\langle p \rangle = \mathfrak{p}_1\mathfrak{p}_2$ *if* $p = 2$ *and* $D \equiv 1 \pmod 8$. *Here,* $N(\mathfrak{p}_1) = N(\mathfrak{p}_2) = p$.
5. $\langle p \rangle = \mathfrak{p}$ *if* $p = 2$ *and* $D \equiv 5 \pmod 8$. *Here,* $N(\mathfrak{p}) = p^2$.

Factoring primes in a quadratic field

Theorem

Let $K = \mathbb{Q}(\sqrt{D})$, and let $p \in \mathbb{Z}$ be a prime. Then,

1. $\langle p \rangle = \mathfrak{p}_1\mathfrak{p}_2$ *if* $p > 2$, $(D/p) = 1$. *Here,* $N(\mathfrak{p}_1) = N(\mathfrak{p}_2) = p$.
2. $\langle p \rangle = \mathfrak{p}$ *if* $p > 2$, *and* $(D/p) = -1$. *Here,* $N(\mathfrak{p}) = p^2$.
3. $\langle p \rangle = \mathfrak{p}^2$ *if* $p > 2$, *and* $p|D$. *Here,* $N(\mathfrak{p}) = p$.
4. $\langle p \rangle = \mathfrak{p}_1\mathfrak{p}_2$ *if* $p = 2$ *and* $D \equiv 1 \pmod 8$. *Here,* $N(\mathfrak{p}_1) = N(\mathfrak{p}_2) = p$.
5. $\langle p \rangle = \mathfrak{p}$ *if* $p = 2$ *and* $D \equiv 5 \pmod 8$. *Here,* $N(\mathfrak{p}) = p^2$.
6. $\langle p \rangle = \mathfrak{p}^2$ *if* $p = 2$ *and* $D \equiv 2, 3 \pmod 4$. *Here,* $N(\mathfrak{p}) = p$.

Factoring primes in a quadratic field

Theorem

Let $K = \mathbb{Q}(\sqrt{D})$, and let $p \in \mathbb{Z}$ be a prime. Then,

1. $\langle p \rangle = \mathfrak{p}_1\mathfrak{p}_2$ *if* $p > 2$, $(D/p) = 1$. *Here,* $N(\mathfrak{p}_1) = N(\mathfrak{p}_2) = p$.
2. $\langle p \rangle = \mathfrak{p}$ *if* $p > 2$, *and* $(D/p) = -1$. *Here,* $N(\mathfrak{p}) = p^2$.
3. $\langle p \rangle = \mathfrak{p}^2$ *if* $p > 2$, *and* $p|D$. *Here,* $N(\mathfrak{p}) = p$.
4. $\langle p \rangle = \mathfrak{p}_1\mathfrak{p}_2$ *if* $p = 2$ *and* $D \equiv 1 (\mathrm{mod}\ 8)$. *Here,* $N(\mathfrak{p}_1) = N(\mathfrak{p}_2) = p$.
5. $\langle p \rangle = \mathfrak{p}$ *if* $p = 2$ *and* $D \equiv 5 (\mathrm{mod}\ 8)$. *Here,* $N(\mathfrak{p}) = p^2$.
6. $\langle p \rangle = \mathfrak{p}^2$ *if* $p = 2$ *and* $D \equiv 2, 3 (\mathrm{mod}\ 4)$. *Here,* $N(\mathfrak{p}) = p$.

In Cases 1 and 4, we say that p splits in K. In Cases 2 and 5, we say that p is inert in K. In Cases 3 and 6, we say that p ramifies in K.

Factoring primes in a monogenic number field

Factoring primes in a monogenic number field

- An algebraic number field K of degree n is said to be **monogenic** if there exists $\theta \in \mathcal{O}_K$ such that

$$\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\theta + \cdots + \mathbb{Z}\theta^{n-1}.$$

Factoring primes in a monogenic number field

- An algebraic number field K of degree n is said to be **monogenic** if there exists $\theta \in \mathcal{O}_K$ such that
$$\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\theta + \cdots + \mathbb{Z}\theta^{n-1}.$$

- Let $f(x) \in \mathbb{Z}[x]$ be an irreducible polynomial such that $f(\theta) = 0$.

Factoring primes in a monogenic number field

- An algebraic number field K of degree n is said to be **monogenic** if there exists $\theta \in \mathcal{O}_K$ such that
$$\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\theta + \cdots + \mathbb{Z}\theta^{n-1}.$$

- Let $f(x) \in \mathbb{Z}[x]$ be an irreducible polynomial such that $f(\theta) = 0$.
- Let p be a rational prime and let $g_1(x), g_2(x), \ldots, g_l(x)$ be distinct monic irreducible polynomials in $\mathbb{Z}_p[x]$ such that
$$f(x) \equiv g_1(x)^{e_1} g_2(x)^{e_2} \ldots g_l(x)^{e_l} \pmod{p}.$$

Factoring primes in a monogenic number field

- An algebraic number field K of degree n is said to be **monogenic** if there exists $\theta \in \mathcal{O}_K$ such that

$$\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\theta + \cdots + \mathbb{Z}\theta^{n-1}.$$

- Let $f(x) \in \mathbb{Z}[x]$ be an irreducible polynomial such that $f(\theta) = 0$.
- Let p be a rational prime and let $g_1(x), g_2(x), \ldots, g_l(x)$ be distinct monic irreducible polynomials in $\mathbb{Z}_p[x]$ such that

$$f(x) \equiv g_1(x)^{e_1} g_2(x)^{e_2} \ldots g_l(x)^{e_l} \pmod{p}.$$

- For each i, let $f_i(x) \in \mathbb{Z}[x]$ such that $f_i(x) \equiv g_i(x) \pmod{p}$, and define $\mathfrak{p}_i = \langle p, f_i(\theta) \rangle$.

Factoring primes in a monogenic number field

- An algebraic number field K of degree n is said to be **monogenic** if there exists $\theta \in \mathcal{O}_K$ such that

$$\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\theta + \cdots + \mathbb{Z}\theta^{n-1}.$$

- Let $f(x) \in \mathbb{Z}[x]$ be an irreducible polynomial such that $f(\theta) = 0$.
- Let p be a rational prime and let $g_1(x), g_2(x), \ldots, g_l(x)$ be distinct monic irreducible polynomials in $\mathbb{Z}_p[x]$ such that

$$f(x) \equiv g_1(x)^{e_1} g_2(x)^{e_2} \ldots g_l(x)^{e_l} \pmod{p}.$$

- For each i, let $f_i(x) \in \mathbb{Z}[x]$ such that $f_i(x) \equiv g_i(x) \pmod{p}$, and define $\mathfrak{p}_i = \langle p, f_i(\theta) \rangle$.
- Then, $\langle p \rangle = \mathfrak{p}_1^{e_1} \mathfrak{p}_2^{e_2} \ldots \mathfrak{p}_l^{e_l}$.

Factoring primes in $K/\mathbb{F}$

Factoring primes in $K/\mathbb{F}$

- If $K/\mathbb{F}$ is an extension of number fields (that is, $[K:\mathbb{F}]$ and $[\mathbb{F}:\mathbb{Q}]$ are finite), we call K a relative extension of $\mathbb{F}$. If $\mathbb{F} = \mathbb{Q}$, we say that K is an absolute extension.

Factoring primes in $K/\mathbb{F}$

- If $K/\mathbb{F}$ is an extension of number fields (that is, $[K : \mathbb{F}]$ and $[\mathbb{F} : \mathbb{Q}]$ are finite), we call K a relative extension of $\mathbb{F}$. If $\mathbb{F} = \mathbb{Q}$, we say that K is an absolute extension.
- We can generalize the notions that we learnt in previous slides and ask how a prime ideal $\mathfrak{p}$ in $\mathcal{O}_{\mathbb{F}}$ factors in $\mathcal{O}_K$.

Factoring primes in $K/\mathbb{F}$

- If $K/\mathbb{F}$ is an extension of number fields (that is, $[K : \mathbb{F}]$ and $[\mathbb{F} : \mathbb{Q}]$ are finite), we call K a relative extension of $\mathbb{F}$. If $\mathbb{F} = \mathbb{Q}$, we say that K is an absolute extension.
- We can generalize the notions that we learnt in previous slides and ask how a prime ideal $\mathfrak{p}$ in $\mathcal{O}_{\mathbb{F}}$ factors in $\mathcal{O}_K$.
- Let $\mathfrak{P}$ be a prime ideal in $\mathcal{O}_K$. There exists exactly one prime ideal $\mathfrak{p}$ of $\mathcal{O}_{\mathbb{F}}$ lying below $\mathfrak{P}$, that is,

Factoring primes in $K/\mathbb{F}$

- If $K/\mathbb{F}$ is an extension of number fields (that is, $[K : \mathbb{F}]$ and $[\mathbb{F} : \mathbb{Q}]$ are finite), we call K a relative extension of $\mathbb{F}$. If $\mathbb{F} = \mathbb{Q}$, we say that K is an absolute extension.
- We can generalize the notions that we learnt in previous slides and ask how a prime ideal $\mathfrak{p}$ in $\mathcal{O}_{\mathbb{F}}$ factors in $\mathcal{O}_K$.
- Let $\mathfrak{P}$ be a prime ideal in $\mathcal{O}_K$. There exists exactly one prime ideal $\mathfrak{p}$ of $\mathcal{O}_{\mathbb{F}}$ lying below $\mathfrak{P}$, that is, $\mathfrak{P}$ can contain exactly one prime ideal $\mathfrak{p}$ of $\mathbb{F}$.

Factoring primes in $K/\mathbb{F}$

- If $K/\mathbb{F}$ is an extension of number fields (that is, $[K : \mathbb{F}]$ and $[\mathbb{F} : \mathbb{Q}]$ are finite), we call K a relative extension of $\mathbb{F}$. If $\mathbb{F} = \mathbb{Q}$, we say that K is an absolute extension.
- We can generalize the notions that we learnt in previous slides and ask how a prime ideal $\mathfrak{p}$ in $\mathcal{O}_{\mathbb{F}}$ factors in $\mathcal{O}_K$.
- Let $\mathfrak{P}$ be a prime ideal in $\mathcal{O}_K$. There exists exactly one prime ideal $\mathfrak{p}$ of $\mathcal{O}_{\mathbb{F}}$ lying below $\mathfrak{P}$, that is, $\mathfrak{P}$ can contain exactly one prime ideal $\mathfrak{p}$ of $\mathbb{F}$.
- The inertial degree of $\mathfrak{P}_i$ in $\mathcal{O}_K$ is defined as

$$f_{K/\mathbb{F}}(\mathfrak{P}_i) := [\mathcal{O}_K/\mathfrak{P}_i : \mathcal{O}_{\mathbb{F}}/\mathfrak{p}].$$

Factoring primes in $K/\mathbb{F}$

- If $K/\mathbb{F}$ is an extension of number fields (that is, $[K : \mathbb{F}]$ and $[\mathbb{F} : \mathbb{Q}]$ are finite), we call K a relative extension of $\mathbb{F}$. If $\mathbb{F} = \mathbb{Q}$, we say that K is an absolute extension.
- We can generalize the notions that we learnt in previous slides and ask how a prime ideal $\mathfrak{p}$ in $\mathcal{O}_{\mathbb{F}}$ factors in $\mathcal{O}_K$.
- Let $\mathfrak{P}$ be a prime ideal in $\mathcal{O}_K$. There exists exactly one prime ideal $\mathfrak{p}$ of $\mathcal{O}_{\mathbb{F}}$ lying below $\mathfrak{P}$, that is, $\mathfrak{P}$ can contain exactly one prime ideal $\mathfrak{p}$ of $\mathbb{F}$.
- The inertial degree of $\mathfrak{P}_i$ in $\mathcal{O}_K$ is defined as

$$f_{K/\mathbb{F}}(\mathfrak{P}_i) := [\mathcal{O}_K/\mathfrak{P}_i : \mathcal{O}_{\mathbb{F}}/\mathfrak{p}].$$

- The fields $\mathcal{O}_K/\mathfrak{P}_i$ and $\mathcal{O}_{\mathbb{F}}/\mathfrak{p}$ are called the residue fields at $\mathfrak{P}_i$ and $\mathfrak{p}$ respectively.

Factoring primes in $K/\mathbb{F}$

- If $K/\mathbb{F}$ is an extension of number fields (that is, $[K:\mathbb{F}]$ and $[\mathbb{F}:\mathbb{Q}]$ are finite), we call K a relative extension of $\mathbb{F}$. If $\mathbb{F}=\mathbb{Q}$, we say that K is an absolute extension.
- We can generalize the notions that we learnt in previous slides and ask how a prime ideal $\mathfrak{p}$ in $\mathcal{O}_{\mathbb{F}}$ factors in $\mathcal{O}_K$.
- Let $\mathfrak{P}$ be a prime ideal in $\mathcal{O}_K$. There exists exactly one prime ideal $\mathfrak{p}$ of $\mathcal{O}_{\mathbb{F}}$ lying below $\mathfrak{P}$, that is, $\mathfrak{P}$ can contain exactly one prime ideal $\mathfrak{p}$ of $\mathbb{F}$.
- The inertial degree of $\mathfrak{P}_i$ in $\mathcal{O}_K$ is defined as

$$f_{K/\mathbb{F}}(\mathfrak{P}_i) := [\mathcal{O}_K/\mathfrak{P}_i : \mathcal{O}_{\mathbb{F}}/\mathfrak{p}].$$

- The fields $\mathcal{O}_K/\mathfrak{P}_i$ and $\mathcal{O}_{\mathbb{F}}/\mathfrak{p}$ are called the residue fields at $\mathfrak{P}_i$ and $\mathfrak{p}$ respectively.
- Thus, the inertial degree $f_{K/\mathbb{F}}(\mathfrak{P}_i)$ is the degree of the extension of these finite fields.

- Suppose

$$\mathfrak{p}\mathcal{O}_K = \prod_{i=1}^{l} \mathfrak{P}_j^{e_i},\ e_i \in \mathbb{N},$$

where $\mathfrak{P}_i$ are distinct prime ideals in $\mathcal{O}_K$.

- Suppose
$$\mathfrak{p}\mathcal{O}_K = \prod_{i=1}^{l} \mathfrak{P}_j^{e_i},\ e_i \in \mathbb{N},$$
where $\mathfrak{P}_i$ are distinct prime ideals in $\mathcal{O}_K$.
- The number e_i is called the ramification index of $\mathfrak{P}_i$ in $\mathcal{O}_K$, and is denoted as $e_{K/\mathbb{F}}(\mathfrak{P}_i)$.

- Suppose
$$\mathfrak{p}\mathcal{O}_K = \prod_{i=1}^{l} \mathfrak{P}_j^{e_i},\ e_i \in \mathbb{N},$$
where $\mathfrak{P}_i$ are distinct prime ideals in $\mathcal{O}_K$.
- The number e_i is called the ramification index of $\mathfrak{P}_i$ in $\mathcal{O}_K$, and is denoted as $e_{K/\mathbb{F}}(\mathfrak{P}_i)$.
- $\mathfrak{p}$ is said to ramify in K if $e_{K/\mathbb{F}}(\mathfrak{P}_i) > 1$ for some i.

- Suppose

$$\mathfrak{p}\mathcal{O}_K = \prod_{i=1}^{l} \mathfrak{P}_j^{e_i}, \; e_i \in \mathbb{N},$$

  where $\mathfrak{P}_i$ are distinct prime ideals in $\mathcal{O}_K$.
- The number e_i is called the ramification index of $\mathfrak{P}_i$ in $\mathcal{O}_K$, and is denoted as $e_{K/\mathbb{F}}(\mathfrak{P}_i)$.
- $\mathfrak{p}$ is said to ramify in K if $e_{K/\mathbb{F}}(\mathfrak{P}_i) > 1$ for some i. Otherwise, $\mathfrak{p}$ is said to be unramified in K.

- Suppose

$$\mathfrak{p}\mathcal{O}_K = \prod_{i=1}^{l} \mathfrak{P}_j^{e_i},\ e_i \in \mathbb{N},$$

where $\mathfrak{P}_i$ are distinct prime ideals in $\mathcal{O}_K$.

- The number e_i is called the ramification index of $\mathfrak{P}_i$ in $\mathcal{O}_K$, and is denoted as $e_{K/\mathbb{F}}(\mathfrak{P}_i)$.
- $\mathfrak{p}$ is said to ramify in K if $e_{K/\mathbb{F}}(\mathfrak{P}_i) > 1$ for some i. Otherwise, $\mathfrak{p}$ is said to be unramified in K.
- $l = l_{K/\mathbb{F}}(\mathfrak{p})$ is said to be the decomposition number of $\mathfrak{p}$ in $\mathcal{O}_K$.

- Suppose
$$\mathfrak{p}\mathcal{O}_K = \prod_{i=1}^{l} \mathfrak{P}_j^{e_i},\ e_i \in \mathbb{N},$$
where $\mathfrak{P}_i$ are distinct prime ideals in $\mathcal{O}_K$.
- The number e_i is called the ramification index of $\mathfrak{P}_i$ in $\mathcal{O}_K$, and is denoted as $e_{K/\mathbb{F}}(\mathfrak{P}_i)$.
- $\mathfrak{p}$ is said to ramify in K if $e_{K/\mathbb{F}}(\mathfrak{P}_i) > 1$ for some i. Otherwise, $\mathfrak{p}$ is said to be unramified in K.
- $l = l_{K/\mathbb{F}}(\mathfrak{p})$ is said to be the decomposition number of $\mathfrak{p}$ in $\mathcal{O}_K$.

Inert, completely split and ramified

- Suppose $K/\mathbb{F}$ is a finite extension of number fields, and let $\mathfrak{p}$ be a prime ideal in $\mathcal{O}_{\mathbb{F}}$ such that $\mathfrak{p}\mathcal{O}_K = \prod_{i=1}^{l} \mathfrak{P}_i^{e_i}$, $e_i \in \mathbb{N}$, where $\mathfrak{P}_i$ are distinct prime ideals in $\mathcal{O}_K$.

Inert, completely split and ramified

- Suppose $K/\mathbb{F}$ is a finite extension of number fields, and let $\mathfrak{p}$ be a prime ideal in $\mathcal{O}_{\mathbb{F}}$ such that $\mathfrak{p}\mathcal{O}_K = \prod_{i=1}^{l} \mathfrak{P}_i^{e_i}$, $e_i \in \mathbb{N}$, where $\mathfrak{P}_i$ are distinct prime ideals in $\mathcal{O}_K$.
- Then $\sum_{i=1}^{l} e_{K/\mathbb{F}}(\mathfrak{P}_i) f_{K/\mathbb{F}}(\mathfrak{P}_i) = [K : \mathbb{F}]$.

Inert, completely split and ramified

- Suppose $K/\mathbb{F}$ is a finite extension of number fields, and let $\mathfrak{p}$ be a prime ideal in $\mathcal{O}_{\mathbb{F}}$ such that $\mathfrak{p}\mathcal{O}_K = \prod_{i=1}^{l} \mathfrak{P}_i^{e_i}$, $e_i \in \mathbb{N}$, where $\mathfrak{P}_i$ are distinct prime ideals in $\mathcal{O}_K$.
- Then $\sum_{i=1}^{l} e_{K/\mathbb{F}}(\mathfrak{P}_i) f_{K/\mathbb{F}}(\mathfrak{P}_i) = [K : \mathbb{F}]$.
- Then $\mathfrak{p}$ is said to be **completely ramified** or **totally ramified** in $\mathcal{O}_K$ whenever

$$e_i := e_{K/\mathbb{F}}(\mathfrak{P}_i) = [K : \mathbb{F}]$$

for some $1 \leq i \leq l$.

Inert, completely split and ramified

- Suppose $K/\mathbb{F}$ is a finite extension of number fields, and let $\mathfrak{p}$ be a prime ideal in $\mathcal{O}_{\mathbb{F}}$ such that $\mathfrak{p}\mathcal{O}_K = \prod_{i=1}^{l} \mathfrak{P}_i^{e_i}$, $e_i \in \mathbb{N}$, where $\mathfrak{P}_i$ are distinct prime ideals in $\mathcal{O}_K$.
- Then $\sum_{i=1}^{l} e_{K/\mathbb{F}}(\mathfrak{P}_i) f_{K/\mathbb{F}}(\mathfrak{P}_i) = [K : \mathbb{F}]$.
- Then $\mathfrak{p}$ is said to be **completely ramified** or **totally ramified** in $\mathcal{O}_K$ whenever

$$e_i := e_{K/\mathbb{F}}(\mathfrak{P}_i) = [K : \mathbb{F}]$$

for some $1 \leq i \leq l$. In this case, $l = 1$ and $f_{K/\mathbb{F}}(\mathfrak{P}_i) = 1$.

Inert, completely split and ramified

- Suppose $K/\mathbb{F}$ is a finite extension of number fields, and let $\mathfrak{p}$ be a prime ideal in $\mathcal{O}_{\mathbb{F}}$ such that $\mathfrak{p}\mathcal{O}_K = \prod_{i=1}^{l} \mathfrak{P}_i^{e_i}$, $e_i \in \mathbb{N}$, where $\mathfrak{P}_i$ are distinct prime ideals in $\mathcal{O}_K$.
- Then $\sum_{i=1}^{l} e_{K/\mathbb{F}}(\mathfrak{P}_i) f_{K/\mathbb{F}}(\mathfrak{P}_i) = [K : \mathbb{F}]$.
- Then $\mathfrak{p}$ is said to be **completely ramified** or **totally ramified** in $\mathcal{O}_K$ whenever

$$e_i := e_{K/\mathbb{F}}(\mathfrak{P}_i) = [K : \mathbb{F}]$$

  for some $1 \leq i \leq l$. In this case, $l = 1$ and $f_{K/\mathbb{F}}(\mathfrak{P}_i) = 1$.
- We say that $\mathfrak{p}$ is said to **split completely** in $\mathcal{O}_K$ if $l = l_{K/\mathbb{F}}(\mathfrak{p}) = [K : \mathbb{F}]$.

Inert, completely split and ramified

- Suppose $K/\mathbb{F}$ is a finite extension of number fields, and let $\mathfrak{p}$ be a prime ideal in $\mathcal{O}_{\mathbb{F}}$ such that $\mathfrak{p}\mathcal{O}_K = \prod_{i=1}^{l} \mathfrak{P}_i^{e_i}$, $e_i \in \mathbb{N}$, where $\mathfrak{P}_i$ are distinct prime ideals in $\mathcal{O}_K$.
- Then $\sum_{i=1}^{l} e_{K/\mathbb{F}}(\mathfrak{P}_i) f_{K/\mathbb{F}}(\mathfrak{P}_i) = [K : \mathbb{F}]$.
- Then $\mathfrak{p}$ is said to be **completely ramified** or **totally ramified** in $\mathcal{O}_K$ whenever

$$e_i := e_{K/\mathbb{F}}(\mathfrak{P}_i) = [K : \mathbb{F}]$$

  for some $1 \leq i \leq l$. In this case, $l = 1$ and $f_{K/\mathbb{F}}(\mathfrak{P}_i) = 1$.
- We say that $\mathfrak{p}$ is said to **split completely** in $\mathcal{O}_K$ if $l = l_{K/\mathbb{F}}(\mathfrak{p}) = [K : \mathbb{F}]$. In this case, $e_{K/\mathbb{F}}(\mathfrak{P}_i) = f_{K/\mathbb{F}}(\mathfrak{P}_i) = 1$ for each $1 \leq i \leq l$.

Inert, completely split and ramified

- Suppose $K/\mathbb{F}$ is a finite extension of number fields, and let $\mathfrak{p}$ be a prime ideal in $\mathcal{O}_{\mathbb{F}}$ such that $\mathfrak{p}\mathcal{O}_K = \prod_{i=1}^{l} \mathfrak{P}_i^{e_i}$, $e_i \in \mathbb{N}$, where $\mathfrak{P}_i$ are distinct prime ideals in $\mathcal{O}_K$.
- Then $\sum_{i=1}^{l} e_{K/\mathbb{F}}(\mathfrak{P}_i) f_{K/\mathbb{F}}(\mathfrak{P}_i) = [K : \mathbb{F}]$.
- Then $\mathfrak{p}$ is said to be **completely ramified** or **totally ramified** in $\mathcal{O}_K$ whenever

$$e_i := e_{K/\mathbb{F}}(\mathfrak{P}_i) = [K : \mathbb{F}]$$

  for some $1 \leq i \leq l$. In this case, $l = 1$ and $f_{K/\mathbb{F}}(\mathfrak{P}_i) = 1$.
- We say that $\mathfrak{p}$ is said to **split completely** in $\mathcal{O}_K$ if $l = l_{K/\mathbb{F}}(\mathfrak{p}) = [K : \mathbb{F}]$. In this case, $e_{K/\mathbb{F}}(\mathfrak{P}_i) = f_{K/\mathbb{F}}(\mathfrak{P}_i) = 1$ for each $1 \leq i \leq l$.
- If $f_{K/\mathbb{F}}(\mathfrak{P}_i) = [K : \mathbb{F}]$ for some i, then $l_{K/\mathbb{F}}(\mathfrak{p}) = 1 = e_{K/\mathbb{F}}(\mathfrak{P}_i)$.

Inert, completely split and ramified

- Suppose $K/\mathbb{F}$ is a finite extension of number fields, and let $\mathfrak{p}$ be a prime ideal in $\mathcal{O}_{\mathbb{F}}$ such that $\mathfrak{p}\mathcal{O}_K = \prod_{i=1}^{l} \mathfrak{P}_i^{e_i}$, $e_i \in \mathbb{N}$, where $\mathfrak{P}_i$ are distinct prime ideals in $\mathcal{O}_K$.
- Then $\sum_{i=1}^{l} e_{K/\mathbb{F}}(\mathfrak{P}_i) f_{K/\mathbb{F}}(\mathfrak{P}_i) = [K : \mathbb{F}]$.
- Then $\mathfrak{p}$ is said to be **completely ramified** or **totally ramified** in $\mathcal{O}_K$ whenever

$$e_i := e_{K/\mathbb{F}}(\mathfrak{P}_i) = [K : \mathbb{F}]$$

  for some $1 \leq i \leq l$. In this case, $l = 1$ and $f_{K/\mathbb{F}}(\mathfrak{P}_i) = 1$.
- We say that $\mathfrak{p}$ is said to **split completely** in $\mathcal{O}_K$ if $l = l_{K/\mathbb{F}}(\mathfrak{p}) = [K : \mathbb{F}]$. In this case, $e_{K/\mathbb{F}}(\mathfrak{P}_i) = f_{K/\mathbb{F}}(\mathfrak{P}_i) = 1$ for each $1 \leq i \leq l$.
- If $f_{K/\mathbb{F}}(\mathfrak{P}_i) = [K : \mathbb{F}]$ for some i, then $l_{K/\mathbb{F}}(\mathfrak{p}) = 1 = e_{K/\mathbb{F}}(\mathfrak{P}_i)$. That is, $\mathfrak{p} = \mathfrak{P}_i$.

Inert, completely split and ramified

- Suppose $K/\mathbb{F}$ is a finite extension of number fields, and let $\mathfrak{p}$ be a prime ideal in $\mathcal{O}_{\mathbb{F}}$ such that $\mathfrak{p}\mathcal{O}_K = \prod_{i=1}^{l} \mathfrak{P}_i^{e_i}$, $e_i \in \mathbb{N}$, where $\mathfrak{P}_i$ are distinct prime ideals in $\mathcal{O}_K$.
- Then $\sum_{i=1}^{l} e_{K/\mathbb{F}}(\mathfrak{P}_i) f_{K/\mathbb{F}}(\mathfrak{P}_i) = [K : \mathbb{F}]$.
- Then $\mathfrak{p}$ is said to be **completely ramified** or **totally ramified** in $\mathcal{O}_K$ whenever

$$e_i := e_{K/\mathbb{F}}(\mathfrak{P}_i) = [K : \mathbb{F}]$$

  for some $1 \leq i \leq l$. In this case, $l = 1$ and $f_{K/\mathbb{F}}(\mathfrak{P}_i) = 1$.
- We say that $\mathfrak{p}$ is said to **split completely** in $\mathcal{O}_K$ if $l = l_{K/\mathbb{F}}(\mathfrak{p}) = [K : \mathbb{F}]$. In this case, $e_{K/\mathbb{F}}(\mathfrak{P}_i) = f_{K/\mathbb{F}}(\mathfrak{P}_i) = 1$ for each $1 \leq i \leq l$.
- If $f_{K/\mathbb{F}}(\mathfrak{P}_i) = [K : \mathbb{F}]$ for some i, then $l_{K/\mathbb{F}}(\mathfrak{p}) = 1 = e_{K/\mathbb{F}}(\mathfrak{P}_i)$. That is, $\mathfrak{p} = \mathfrak{P}_i$. In this case, we say that $\mathfrak{p}$ is inert in $\mathcal{O}_K$.

Galois extensions, ramification and inertia

Galois extensions, ramification and inertia

Theorem

Let $K/\mathbb{F}$ be a Galois extension of number fields, that is, all the $\mathbb{F}$-conjugate fields of K are identical.
Let $\mathfrak{p}$ be a prime ideal in $\mathcal{O}_{\mathbb{F}}$ such that $\mathfrak{p}\mathcal{O}_K = \prod_{i=1}^{l} \mathfrak{P}_i^{e_i}$, $e_i \in \mathbb{N}$, where $\mathfrak{P}_i$ are distinct prime ideals in $\mathcal{O}_K$, with $e_i = e_{K/\mathbb{F}}(\mathfrak{P}_i)$, $f_i = f_{K/\mathbb{F}}(\mathfrak{P}_i)$ and $l = l_{K/\mathbb{F}}(\mathfrak{p})$.

Galois extensions, ramification and inertia

Theorem

Let $K/\mathbb{F}$ be a Galois extension of number fields, that is, all the $\mathbb{F}$-conjugate fields of K are identical.
Let $\mathfrak{p}$ be a prime ideal in $\mathcal{O}_{\mathbb{F}}$ such that $\mathfrak{p}\mathcal{O}_K = \prod_{i=1}^{l} \mathfrak{P}_i^{e_i}$, $e_i \in \mathbb{N}$, where $\mathfrak{P}_i$ are distinct prime ideals in $\mathcal{O}_K$, with $e_i = e_{K/\mathbb{F}}(\mathfrak{P}_i)$, $f_i = f_{K/\mathbb{F}}(\mathfrak{P}_i)$ and $l = l_{K/\mathbb{F}}(\mathfrak{p})$.
Then,

$$e_{K/\mathbb{F}}(\mathfrak{P}_i) = e_{K/\mathbb{F}}(\mathfrak{P}_j),\ f_{K/\mathbb{F}}(\mathfrak{P}_i) = f_{K/\mathbb{F}}(\mathfrak{P}_j) \text{ for all } 1 \leq i, j \leq l.$$

Galois extensions, ramification and inertia

Theorem

Let $K/\mathbb{F}$ be a Galois extension of number fields, that is, all the $\mathbb{F}$-conjugate fields of K are identical.
Let $\mathfrak{p}$ be a prime ideal in $\mathcal{O}_\mathbb{F}$ such that $\mathfrak{p}\mathcal{O}_K = \prod_{i=1}^{l} \mathfrak{P}_i^{e_i}$, $e_i \in \mathbb{N}$, where $\mathfrak{P}_i$ are distinct prime ideals in $\mathcal{O}_K$, with $e_i = e_{K/\mathbb{F}}(\mathfrak{P}_i)$, $f_i = f_{K/\mathbb{F}}(\mathfrak{P}_i)$ and $l = l_{K/\mathbb{F}}(\mathfrak{p})$.
Then,

$$e_{K/\mathbb{F}}(\mathfrak{P}_i) = e_{K/\mathbb{F}}(\mathfrak{P}_j),\ f_{K/\mathbb{F}}(\mathfrak{P}_i) = f_{K/\mathbb{F}}(\mathfrak{P}_j) \text{ for all } 1 \leq i, j \leq l.$$

Since the above values are equal, we may respectively denote them as $e_{K/\mathbb{F}}(\mathfrak{p})$ and $f_{K/\mathbb{F}}(\mathfrak{p})$.

Theorem

Let $K/\mathbb{F}$ be a Galois extension of number fields, that is, all the $\mathbb{F}$-conjugate fields of K are identical.
Let $\mathfrak{p}$ be a prime ideal in $\mathcal{O}_{\mathbb{F}}$ such that $\mathfrak{p}\mathcal{O}_K = \prod_{i=1}^{l} \mathfrak{P}_i^{e_i}$, $e_i \in \mathbb{N}$, where $\mathfrak{P}_i$ are distinct prime ideals in $\mathcal{O}_K$, with $e_i = e_{K/\mathbb{F}}(\mathfrak{P}_i)$, $f_i = f_{K/\mathbb{F}}(\mathfrak{P}_i)$ and $l = l_{K/\mathbb{F}}(\mathfrak{p})$.
Then,

$$e_{K/\mathbb{F}}(\mathfrak{P}_i) = e_{K/\mathbb{F}}(\mathfrak{P}_j),\ f_{K/\mathbb{F}}(\mathfrak{P}_i) = f_{K/\mathbb{F}}(\mathfrak{P}_j) \text{ for all } 1 \leq i,j \leq l.$$

Since the above values are equal, we may respectively denote them as $e_{K/\mathbb{F}}(\mathfrak{p})$ and $f_{K/\mathbb{F}}(\mathfrak{p})$. Thus,

$$e_{K/\mathbb{F}}(\mathfrak{p}) f_{K/\mathbb{F}}(\mathfrak{p}) l_{K/\mathbb{F}}(\mathfrak{p}) = [K : \mathbb{F}].$$

Decomposition group and inertia group

Decomposition group and inertia group

- The set of all $\mathbb{F}$-embeddings of K forms a group called the Galois group of K over $\mathbb{F}$ and denoted $\mathrm{Gal}(K/\mathbb{F})$.

Decomposition group and inertia group

- The set of all $\mathbb{F}$-embeddings of K forms a group called the Galois group of K over $\mathbb{F}$ and denoted $\mathrm{Gal}(K/\mathbb{F})$.
- Suppose K is a Galois extension of $\mathbb{F}$. Then, for any $\sigma \in \mathrm{Gal}(K/\mathbb{F})$, $\sigma : K \to K$ and $\sigma(\mathbb{F}) = \mathbb{F}$.

Decomposition group and inertia group

- The set of all $\mathbb{F}$-embeddings of K forms a group called the Galois group of K over $\mathbb{F}$ and denoted $\mathrm{Gal}(K/\mathbb{F})$.
- Suppose K is a Galois extension of $\mathbb{F}$. Then, for any $\sigma \in \mathrm{Gal}(K/\mathbb{F})$, $\sigma : K \to K$ and $\sigma(\mathbb{F}) = \mathbb{F}$. In fact, $\mathbb{F}$ is the fixed field of $\mathrm{Gal}(K/\mathbb{F})$.

Decomposition group and inertia group

- The set of all $\mathbb{F}$-embeddings of K forms a group called the Galois group of K over $\mathbb{F}$ and denoted $\mathrm{Gal}(K/\mathbb{F})$.
- Suppose K is a Galois extension of $\mathbb{F}$. Then, for any $\sigma \in \mathrm{Gal}(K/\mathbb{F})$, $\sigma : K \to K$ and $\sigma(\mathbb{F}) = \mathbb{F}$. In fact, $\mathbb{F}$ is the fixed field of $\mathrm{Gal}(K/\mathbb{F})$.
- Let $\mathfrak{p}$ be a fixed prime ideal in $\mathcal{O}_{\mathbb{F}}$. Then, $\mathrm{Gal}(K/\mathbb{F})$ transitively permutes the prime ideals of $\mathcal{O}_K$ lying above $\mathfrak{p}$.

Decomposition group and inertia group

- The set of all $\mathbb{F}$-embeddings of K forms a group called the Galois group of K over $\mathbb{F}$ and denoted $\mathrm{Gal}(K/\mathbb{F})$.
- Suppose K is a Galois extension of $\mathbb{F}$. Then, for any $\sigma \in \mathrm{Gal}(K/\mathbb{F})$, $\sigma : K \to K$ and $\sigma(\mathbb{F}) = \mathbb{F}$. In fact, $\mathbb{F}$ is the fixed field of $\mathrm{Gal}(K/\mathbb{F})$.
- Let $\mathfrak{p}$ be a fixed prime ideal in $\mathcal{O}_{\mathbb{F}}$. Then, $\mathrm{Gal}(K/\mathbb{F})$ transitively permutes the prime ideals of $\mathcal{O}_K$ lying above $\mathfrak{p}$.
- That is, let

$$\mathfrak{p}\mathcal{O}_K = \prod_{i=1}^{l} \mathfrak{P}_i^{e_i}.$$

Decomposition group and inertia group

- The set of all $\mathbb{F}$-embeddings of K forms a group called the Galois group of K over $\mathbb{F}$ and denoted $\mathrm{Gal}(K/\mathbb{F})$.
- Suppose K is a Galois extension of $\mathbb{F}$. Then, for any $\sigma \in \mathrm{Gal}(K/\mathbb{F})$, $\sigma : K \to K$ and $\sigma(\mathbb{F}) = \mathbb{F}$. In fact, $\mathbb{F}$ is the fixed field of $\mathrm{Gal}(K/\mathbb{F})$.
- Let $\mathfrak{p}$ be a fixed prime ideal in $\mathcal{O}_{\mathbb{F}}$. Then, $\mathrm{Gal}(K/\mathbb{F})$ transitively permutes the prime ideals of $\mathcal{O}_K$ lying above $\mathfrak{p}$.
- That is, let

$$\mathfrak{p}\mathcal{O}_K = \prod_{i=1}^{l} \mathfrak{P}_i^{e_i}.$$

  Then, for each $1 \leq i, j \leq l$, $\sigma(\mathfrak{P}_i) = \mathfrak{P}_j$ for some $\sigma \in \mathrm{Gal}(K/\mathbb{F})$.

- For a prime ideal $\mathfrak{P}$ of $\mathcal{O}_K$, the **decomposition group of $\mathfrak{P}$ in K** is defined as

$$D_{\mathfrak{P}}(K/\mathbb{F}) := \{\sigma \in \mathrm{Gal}(K/\mathbb{F}) :\ \sigma(\mathfrak{P}) = \mathfrak{P}\}.$$

- For a prime ideal $\mathfrak{P}$ of $\mathcal{O}_K$, the **decomposition group of $\mathfrak{P}$ in K** is defined as

$$D_{\mathfrak{P}}(K/\mathbb{F}) := \{\sigma \in \mathrm{Gal}(K/\mathbb{F}) : \sigma(\mathfrak{P}) = \mathfrak{P}\}.$$

- For any $\rho \in \mathrm{Gal}(K/\mathbb{F})$,

$$\rho^{-1} D_{\mathfrak{P}}(K/\mathbb{F}) \rho = D_{\rho(\mathfrak{P})}(K/\mathbb{F}).$$

- For a prime ideal $\mathfrak{P}$ of $\mathcal{O}_K$, the **decomposition group of $\mathfrak{P}$ in K** is defined as

$$D_{\mathfrak{P}}(K/\mathbb{F}) := \{\sigma \in \mathrm{Gal}(K/\mathbb{F}) : \sigma(\mathfrak{P}) = \mathfrak{P}\}.$$

- For any $\rho \in \mathrm{Gal}(K/\mathbb{F})$,

$$\rho^{-1} D_{\mathfrak{P}}(K/\mathbb{F}) \rho = D_{\rho(\mathfrak{P})}(K/\mathbb{F}).$$

- If $\mathfrak{P}$ lies over a prime $\mathfrak{p}$ in $\mathcal{O}_{\mathbb{F}}$, then $|D_{\mathfrak{P}}(K/\mathbb{F})| = e_{K/\mathbb{F}}(\mathfrak{p}) f_{K/\mathbb{F}}(\mathfrak{p})$.

- For a prime ideal $\mathfrak{P}$ of $\mathcal{O}_K$, the **inertia group of $\mathfrak{P}$ in K** is defined as

$$\mathcal{T}_{\mathfrak{P}}(K/\mathbb{F}) := \{\sigma \in \mathrm{Gal}(K/\mathbb{F}) : \sigma(\alpha) - \alpha \in \mathfrak{P} \text{ for all } \alpha \in \mathcal{O}_K\}.$$

- For a prime ideal $\mathfrak{P}$ of $\mathcal{O}_K$, the **inertia group of $\mathfrak{P}$ in K** is defined as

  $$\mathcal{T}_{\mathfrak{P}}(K/\mathbb{F}) := \{\sigma \in \mathrm{Gal}(K/\mathbb{F}) :\ \sigma(\alpha) - \alpha \in \mathfrak{P} \text{ for all } \alpha \in \mathcal{O}_K\}.$$

- For any $\rho \in \mathrm{Gal}(K/\mathbb{F})$,

  $$\rho^{-1}\mathcal{T}_{\mathfrak{P}}(K/\mathbb{F})\rho = \mathcal{T}_{\rho(\mathfrak{P})}(K/\mathbb{F}).$$

- For a prime ideal $\mathfrak{P}$ of $\mathcal{O}_K$, the **inertia group of $\mathfrak{P}$ in K** is defined as

  $$\mathcal{T}_{\mathfrak{P}}(K/\mathbb{F}) := \{\sigma \in \mathrm{Gal}(K/\mathbb{F}) : \sigma(\alpha) - \alpha \in \mathfrak{P} \text{ for all } \alpha \in \mathcal{O}_K\}.$$

- For any $\rho \in \mathrm{Gal}(K/\mathbb{F})$,

  $$\rho^{-1}\mathcal{T}_{\mathfrak{P}}(K/\mathbb{F})\rho = \mathcal{T}_{\rho(\mathfrak{P})}(K/\mathbb{F}).$$

- If $\mathfrak{P}$ lies over a prime $\mathfrak{p}$ in $\mathcal{O}_{\mathbb{F}}$, then

  $$|\,\mathrm{Gal}(K/\mathbb{F}) : \mathcal{T}_{\mathfrak{P}}(K/\mathbb{F})| = I_{K/\mathbb{F}}(\mathfrak{p}) f_{K/\mathbb{F}}(\mathfrak{p}).$$

- For a prime ideal $\mathfrak{P}$ of $\mathcal{O}_K$, the **inertia group of $\mathfrak{P}$ in K** is defined as

$$\mathcal{T}_{\mathfrak{P}}(K/\mathbb{F}) := \{\sigma \in \mathrm{Gal}(K/\mathbb{F}) : \sigma(\alpha) - \alpha \in \mathfrak{P} \text{ for all } \alpha \in \mathcal{O}_K\}.$$

- For any $\rho \in \mathrm{Gal}(K/\mathbb{F})$,

$$\rho^{-1}\mathcal{T}_{\mathfrak{P}}(K/\mathbb{F})\rho = \mathcal{T}_{\rho(\mathfrak{P})}(K/\mathbb{F}).$$

- If $\mathfrak{P}$ lies over a prime $\mathfrak{p}$ in $\mathcal{O}_{\mathbb{F}}$, then

$$|\,\mathrm{Gal}(K/\mathbb{F}) : \mathcal{T}_{\mathfrak{P}}(K/\mathbb{F})| = I_{K/\mathbb{F}}(\mathfrak{p})f_{K/\mathbb{F}}(\mathfrak{p}).$$

References

1. "Problems in algebraic number theory" by Jody Esmonde and M. Ram Murty (Springer GTM)
2. "Algebraic number theory" by Richard A. Mollin (Discrete Mathematics and its Applications).
3. "Introductory algebraic number theory" by Şaban Alaca and Kenneth S. Williams (Cambridge University Press)