Number Fields and Galois Theory

Garima Rastogi and Xavier Choe

MIT PRIMES Circle

May 22nd, 2021

Garima R.

- Occupation: co-existing human being
- Place of work: High school at VLACS
- Grade: 9th

Xavier Choe

- The Newman School in Boston
- 14 years old
- Grade 10

Introduction

Overview

Overview

- Number theory from *Elementary Number Theory* by Jones and Jones

Overview

- Number theory from *Elementary Number Theory* by Jones and Jones
  - Divisibility
  - Prime Numbers
  - Congruences
  - Congruences of Prime-Power Moduli
  - Euler's Function
  - The Group of Units
  - Quadratic Residues

Overview

- Number theory from *Elementary Number Theory* by Jones and Jones
  - Divisibility
  - Prime Numbers
  - Congruences
  - Congruences of Prime-Power Moduli
  - Euler's Function
  - The Group of Units
  - Quadratic Residues
- Number fields

Overview

- Number theory from *Elementary Number Theory* by Jones and Jones
  - Divisibility
  - Prime Numbers
  - Congruences
  - Congruences of Prime-Power Moduli
  - Euler's Function
  - The Group of Units
  - Quadratic Residues
- Number fields
- Galois theory, especially in relation to number fields

Overview

- Number theory from *Elementary Number Theory* by Jones and Jones
  - Divisibility
  - Prime Numbers
  - Congruences
  - Congruences of Prime-Power Moduli
  - Euler's Function
  - The Group of Units
  - Quadratic Residues
- Number fields
- Galois theory, especially in relation to number fields
- Today's topic: number fields and Galois theory

Number Fields

Fields

Definition

A **field** F is a commutative ring containing the multiplicative identity where every non-zero element is a unit (has an inverse).

Fields

Definition

A **field** F is a commutative ring containing the multiplicative identity where every non-zero element is a unit (has an inverse).

Example

$\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are all examples of fields.

Fields

Definition

A **field** F is a commutative ring containing the multiplicative identity where every non-zero element is a unit (has an inverse).

Example

$\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are all examples of fields.

Non-Example

$\mathbb{Z}$ (the ring of integers) is not a field since only 1 and -1 have a multiplicative inverse.

Finite Fields

Definition

A **finite field** is a field with a finite number of elements.

Finite Fields

Definition

A **finite field** is a field with a finite number of elements.

Example

$\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ is a finite field (p is prime).

Finite Fields

The element 1 in any finite field generates a subfield of size a prime number p.

Finite Fields

The element 1 in any finite field generates a subfield of size a prime number p.

Proposition

Therefore every finite field is a finite extension of some $\mathbb{F}_p$.

Finite Fields

The element 1 in any finite field generates a subfield of size a prime number p.

Proposition

Therefore every finite field is a finite extension of some $\mathbb{F}_p$.

We denote these as $\mathbb{F}_q$ where $q = p^k$.

Cyclotomic Fields

Cyclotomic Fields

Definition

The n^{th} **roots of unity** are the n (distinct) complex solutions to $x^n = 1$.

Cyclotomic Fields

Definition

The n^{th} **roots of unity** are the n (distinct) complex solutions to $x^n = 1$.

The n n^{th} roots of unity form a regular n-gon with its vertices on the unit circle.

Cyclotomic Fields

Definition

The n^{th} **roots of unity** are the n (distinct) complex solutions to $x^n = 1$.

The n n^{th} roots of unity form a regular n-gon with its vertices on the unit circle.
These are the powers of $\zeta_n := e^{\frac{2\pi i}{n}}$.

Cyclotomic Fields

Definition

The n^{th} **roots of unity** are the n (distinct) complex solutions to $x^n = 1$.

The n n^{th} roots of unity form a regular n-gon with its vertices on the unit circle.
These are the powers of $\zeta_n := e^{\frac{2\pi i}{n}}$.

Definition

The n^{th} cyclotomic field $\mathbb{Q}(\zeta_n)$, is the field consisting of $a_0 + a_1\zeta_n + a_2\zeta_n^2 + \cdots + a_{n-1}\zeta_n^{n-1}$ for $a_0, a_1, \ldots, a_{n-1} \in \mathbb{Q}$.

Cyclotomic Fields

Definition

The n^{th} **roots of unity** are the n (distinct) complex solutions to $x^n = 1$.

The n n^{th} roots of unity form a regular n-gon with its vertices on the unit circle.
These are the powers of $\zeta_n := e^{\frac{2\pi i}{n}}$.

Definition

The n^{th} cyclotomic field $\mathbb{Q}(\zeta_n)$, is the field consisting of $a_0 + a_1\zeta_n + a_2\zeta_n^2 + \cdots + a_{n-1}\zeta_n^{n-1}$ for $a_0, a_1, \ldots, a_{n-1} \in \mathbb{Q}$.

Remark: it actually has dimension $\phi(n)$ as a $\mathbb{Q}$-vector space, not n.

Number Fields

Number Fields

Definition

Algebraic number fields K, also known as **number fields**, are finite degree extension fields of $\mathbb{Q}$.

Number Fields

Definition

Algebraic number fields K, also known as **number fields**, are finite degree extension fields of $\mathbb{Q}$. In other words, the following conditions are satisfied:

- K is a field.
- $\mathbb{Q} \subseteq K$.
- K is a finite dimensional vector space over $\mathbb{Q}$.

Examples of Number Fields

Example

$\mathbb{Q}$, $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{d})$, and $\mathbb{Q}(\zeta_n)$ are all number fields.

Examples of Number Fields

Example

$\mathbb{Q}$, $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{d})$, and $\mathbb{Q}(\zeta_n)$ are all number fields.

Non-Example

The finite fields $\mathbb{F}_q$ are not number fields because they do not contain $\mathbb{Q}$.

Examples of Number Fields

Example

$\mathbb{Q}$, $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{d})$, and $\mathbb{Q}(\zeta_n)$ are all number fields.

Non-Example

The finite fields $\mathbb{F}_q$ are not number fields because they do not contain $\mathbb{Q}$.

Non-Example

The fields $\mathbb{R}$, $\mathbb{C}$, and $\mathbb{Q}(\pi)$ (or any other transcendental number) are not number fields because they are infinite-dimensional vector spaces over $\mathbb{Q}$ (alternatively, infinite-degree extensions).

Examples of Number Fields

Example

$\mathbb{Q}$, $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{d})$, and $\mathbb{Q}(\zeta_n)$ are all number fields.

Non-Example

The finite fields $\mathbb{F}_q$ are not number fields because they do not contain $\mathbb{Q}$.

Non-Example

The fields $\mathbb{R}$, $\mathbb{C}$, and $\mathbb{Q}(\pi)$ (or any other transcendental number) are not number fields because they are infinite-dimensional vector spaces over $\mathbb{Q}$ (alternatively, infinite-degree extensions).

Non-Example

The ring $\mathbb{Q}[x]/(x^2)$ is not a number field because it is not a field.

Minimal Polynomials

Minimal Polynomials

Definition

The **minimal polynomial** for a constant α over a given field F is a monic polynomial $f(x)$ of minimum degree that is irreducible over F such that $f(\alpha) = 0$.

Minimal Polynomials

Definition

The **minimal polynomial** for a constant α over a given field F is a monic polynomial $f(x)$ of minimum degree that is irreducible over F such that $f(\alpha) = 0$.

Essentially, the minimal polynomial is the smallest polynomial which still has α as a root.

Minimal Polynomials

Definition

The **minimal polynomial** for a constant α over a given field F is a monic polynomial $f(x)$ of minimum degree that is irreducible over F such that $f(\alpha) = 0$.

Essentially, the minimal polynomial is the smallest polynomial which still has α as a root.

Example

$x^2 + 1$ is the minimal polynomial for i over the field $\mathbb{R}$.

Characterizing Number Fields

Characterizing Number Fields

Theorem (Primitive Element Theorem)

Every finite extension of $\mathbb{Q}$ is $\mathbb{Q}(\alpha)$ where α is a root of its minimal polynomial $f(x)$ over $\mathbb{Q}$.

In other words, every number field is realized by adjoining some **single** element to $\mathbb{Q}$!

Characterizing Number Fields

Theorem (Primitive Element Theorem)

Every finite extension of $\mathbb{Q}$ is $\mathbb{Q}(\alpha)$ where α is a root of its minimal polynomial $f(x)$ over $\mathbb{Q}$.

In other words, every number field is realized by adjoining some **single** element to $\mathbb{Q}$!

Example

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7}, \sqrt{11})$$

$\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7}, \sqrt{11})$ would **still** be just $\mathbb{Q}$ adjoin some single element.

Characterizing Number Fields

Theorem (Primitive Element Theorem)

Every finite extension of $\mathbb{Q}$ is $\mathbb{Q}(\alpha)$ where α is a root of its minimal polynomial $f(x)$ over $\mathbb{Q}$.

In other words, every number field is realized by adjoining some **single** element to $\mathbb{Q}$!

Example

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7}, \sqrt{11})$$

$\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7}, \sqrt{11})$ would **still** be just $\mathbb{Q}$ adjoin some single element.
In fact, $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7}, \sqrt{11}) = \mathbb{Q}(\alpha)$ where $\alpha = \sqrt{2} + \sqrt{3} + \sqrt{5} + \sqrt{7} + \sqrt{11}$.

Ring of Integers

Ring of Integers

Definition

The **ring of integers** of a number field K, denoted $\mathcal{O}_K$, is the subset of K whose minimal polynomial over $\mathbb{Q}$ is monic and integer.

The field $\mathbb{Q}$ is the fractions using $\mathbb{Z}$, and $\mathbb{Z}$ is the "integer" part of $\mathbb{Q}$. In the same way, for a number field K, $\mathcal{O}_K$ is the "integer" part of K, and K is the fractions of using $\mathcal{O}_K$.

Ring of Integers

Definition

The **ring of integers** of a number field K, denoted $\mathcal{O}_K$, is the subset of K whose minimal polynomial over $\mathbb{Q}$ is monic and integer.

The field $\mathbb{Q}$ is the fractions using $\mathbb{Z}$, and $\mathbb{Z}$ is the "integer" part of $\mathbb{Q}$. In the same way, for a number field K, $\mathcal{O}_K$ is the "integer" part of K, and K is the fractions of using $\mathcal{O}_K$.

Proposition

$K \subset L$, where L is an extension of the field K, implies $\mathcal{O}_K \subset \mathcal{O}_L$.

Examples of Rings of Integers

Examples of Rings of Integers

Example

The ring of integers of $\mathbb{Q}$ is $\mathbb{Z}$.

Examples of Rings of Integers

Example

The ring of integers of $\mathbb{Q}$ is $\mathbb{Z}$.

Example

The ring of integers of $\mathbb{Q}(i)$ is $\mathbb{Z}[i]$.

Examples of Rings of Integers

Example

The ring of integers of $\mathbb{Q}$ is $\mathbb{Z}$.

Example

The ring of integers of $\mathbb{Q}(i)$ is $\mathbb{Z}[i]$.

Example

The ring of integers of $\mathbb{Q}(\sqrt{2})$ is $\mathbb{Z}[\sqrt{2}]$.

Examples of Rings of Integers

Example

The ring of integers of $\mathbb{Q}$ is $\mathbb{Z}$.

Example

The ring of integers of $\mathbb{Q}(i)$ is $\mathbb{Z}[i]$.

Example

The ring of integers of $\mathbb{Q}(\sqrt{2})$ is $\mathbb{Z}[\sqrt{2}]$.

Example

The ring of integers of $\mathbb{Q}(\sqrt{d})$ for $d \equiv 1 \pmod 4$ (and d squarefree) is actually $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$.

Factorizing Ideals

Prime Ideals

Prime Ideals

Definition

A **prime ideal** of a commutative ring R is a proper ideal $\mathfrak{p}$ such that for two elements $a_1, a_2 \in R$ and $a_1 a_2 \in \mathfrak{p}$ implies $a_1 \in \mathfrak{p}$, $a_2 \in \mathfrak{p}$, or $a_1, a_2 \in \mathfrak{p}$.

Prime Ideals

Definition

A **prime ideal** of a commutative ring R is a proper ideal $\mathfrak{p}$ such that for two elements $a_1, a_2 \in R$ and $a_1 a_2 \in \mathfrak{p}$ implies $a_1 \in \mathfrak{p}$, $a_2 \in \mathfrak{p}$, or $a_1, a_2 \in \mathfrak{p}$.

Example

The prime ideals of $\mathbb{Z}$ are (0) and (p) for all prime integers p.

Prime Ideals

Definition

A **prime ideal** of a commutative ring R is a proper ideal $\mathfrak{p}$ such that for two elements $a_1, a_2 \in R$ and $a_1 a_2 \in \mathfrak{p}$ implies $a_1 \in \mathfrak{p}$, $a_2 \in \mathfrak{p}$, or $a_1, a_2 \in \mathfrak{p}$.

Example

The prime ideals of $\mathbb{Z}$ are (0) and (p) for all prime integers p.

Example

The only prime ideal of a field F is the zero ideal (0).

Prime Ideals

Definition

A **prime ideal** of a commutative ring R is a proper ideal $\mathfrak{p}$ such that for two elements $a_1, a_2 \in R$ and $a_1 a_2 \in \mathfrak{p}$ implies $a_1 \in \mathfrak{p}$, $a_2 \in \mathfrak{p}$, or $a_1, a_2 \in \mathfrak{p}$.

Example

The prime ideals of $\mathbb{Z}$ are (0) and (p) for all prime integers p.

Example

The only prime ideal of a field F is the zero ideal (0).

Non-Example

The ideal $(3, x^2 + 11)$ of $\mathbb{Z}[x]$ is not prime since $x^2 + 11 - 3 \cdot 4 = x^2 - 1 = (x - 1)(x + 1)$, but neither $x - 1$ nor $x + 1$ is in the ideal.

Factorizing Ideals in $\mathcal{O}_K$

Factorizing Ideals in $\mathcal{O}_K$

Theorem

All rings of integers $\mathcal{O}_K$ are Dedekind domains. All prime ideals are maximal ideals. Crucially, all ideals have unique factorization into prime ideals.

Factorizing Ideals in $\mathcal{O}_K$

Theorem

All rings of integers $\mathcal{O}_K$ are Dedekind domains. All prime ideals are maximal ideals. Crucially, all ideals have unique factorization into prime ideals.

Factorizing Ideals in $\mathcal{O}_K$

Theorem

All rings of integers $\mathcal{O}_K$ are Dedekind domains. All prime ideals are maximal ideals. Crucially, all ideals have unique factorization into prime ideals.

- $\mathbb{Q} \subset K \implies \mathcal{O}_{\mathbb{Q}} = \mathbb{Z} \subset \mathcal{O}_K$.

Factorizing Ideals in $\mathcal{O}_K$

Theorem

All rings of integers $\mathcal{O}_K$ are Dedekind domains. All prime ideals are maximal ideals. Crucially, all ideals have unique factorization into prime ideals.

- $\mathbb{Q} \subset K \implies \mathcal{O}_{\mathbb{Q}} = \mathbb{Z} \subset \mathcal{O}_K$.
- Prime ideal $p\mathbb{Z} \subset \mathbb{Z}$; lifting to $\mathcal{O}_K$, have $p\mathcal{O}_K$ (multiples of p in $\mathcal{O}_K$).

Factorizing Ideals in $\mathcal{O}_K$

Theorem

All rings of integers $\mathcal{O}_K$ are Dedekind domains. All prime ideals are maximal ideals. Crucially, all ideals have unique factorization into prime ideals.

- $\mathbb{Q} \subset K \implies \mathcal{O}_{\mathbb{Q}} = \mathbb{Z} \subset \mathcal{O}_K$.
- Prime ideal $p\mathbb{Z} \subset \mathbb{Z}$; lifting to $\mathcal{O}_K$, have $p\mathcal{O}_K$ (multiples of p in $\mathcal{O}_K$).
- This is an ideal, but unlike $p\mathbb{Z}$, it is usually not prime.

Factorizing Ideals in $\mathcal{O}_K$

Theorem

All rings of integers $\mathcal{O}_K$ are Dedekind domains. All prime ideals are maximal ideals. Crucially, all ideals have unique factorization into prime ideals.

- $\mathbb{Q} \subset K \implies \mathcal{O}_{\mathbb{Q}} = \mathbb{Z} \subset \mathcal{O}_K$.
- Prime ideal $p\mathbb{Z} \subset \mathbb{Z}$; lifting to $\mathcal{O}_K$, have $p\mathcal{O}_K$ (multiples of p in $\mathcal{O}_K$).
- This is an ideal, but unlike $p\mathbb{Z}$, it is usually not prime.
- We will study its prime factorization.

General Factorization Properties

Because $p\mathcal{O}_K$ is an ideal, it has prime factorization

$$p\mathcal{O}_K = \prod_{i=1}^{r} Q_i^{e_i},$$

where Q_i are prime ideals of $\mathcal{O}_K$.

General Factorization Properties

Because $p\mathcal{O}_K$ is an ideal, it has prime factorization

$$p\mathcal{O}_K = \prod_{i=1}^{r} Q_i^{e_i},$$

where Q_i are prime ideals of $\mathcal{O}_K$.
We already know that $\mathbb{Z}/p\mathbb{Z}$ is a field. On the other hand, $\mathcal{O}_K/Q_i$ is also a field.

General Factorization Properties

Because $p\mathcal{O}_K$ is an ideal, it has prime factorization

$$p\mathcal{O}_K = \prod_{i=1}^{r} Q_i^{e_i},$$

where Q_i are prime ideals of $\mathcal{O}_K$.
We already know that $\mathbb{Z}/p\mathbb{Z}$ is a field. On the other hand, $\mathcal{O}_K/Q_i$ is also a field.
Just as how $\mathbb{Z}$ is a subring of $\mathcal{O}_K$, $\mathbb{Z}/p\mathbb{Z}$ is a subfield of $\mathcal{O}_K/Q_i$.

General Factorization Properties

Because $p\mathcal{O}_K$ is an ideal, it has prime factorization

$$p\mathcal{O}_K = \prod_{i=1}^{r} Q_i^{e_i},$$

where Q_i are prime ideals of $\mathcal{O}_K$.
We already know that $\mathbb{Z}/p\mathbb{Z}$ is a field. On the other hand, $\mathcal{O}_K/Q_i$ is also a field.
Just as how $\mathbb{Z}$ is a subring of $\mathcal{O}_K$, $\mathbb{Z}/p\mathbb{Z}$ is a subfield of $\mathcal{O}_K/Q_i$.

Definition

We will denote f_i to be the degree of the extension. In other words, $f_i := [\mathcal{O}_K/Q_i : \mathbb{Z}/p\mathbb{Z}]$.

Relationship of dimension with factorization

Theorem

We have

$$[K : \mathbb{Q}] = \sum_{i=1}^{r} e_i f_i.$$

Relationship of dimension with factorization

Theorem

We have

$$[K : \mathbb{Q}] = \sum_{i=1}^{r} e_i f_i.$$

Even better, when $K/\mathbb{Q}$ is Galois (which we will define later):

Theorem

Let $K/\mathbb{Q}$ be Galois. Then all of the e_i and f_i are the same, so

$$[K : \mathbb{Q}] = ref.$$

Computing The Factorization

Computing The Factorization

By the Primitive element theorem, $K = \mathbb{Q}(\alpha)$. Let $f(x)$ be the minimal polynomial of α. It turns out that factorization of $p\mathcal{O}_K$ is as easy as factorizing $f(x)$ modulo p (for all but finitely many p).

Computing The Factorization

By the Primitive element theorem, $K = \mathbb{Q}(\alpha)$. Let $f(x)$ be the minimal polynomial of α. It turns out that factorization of $p\mathcal{O}_K$ is as easy as factorizing $f(x)$ modulo p (for all but finitely many p).

Example

- In $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$, $\alpha = \sqrt{2}$, and $f(x) = x^2 - 2$.

Computing The Factorization

By the Primitive element theorem, $K = \mathbb{Q}(\alpha)$. Let $f(x)$ be the minimal polynomial of α. It turns out that factorization of $p\mathcal{O}_K$ is as easy as factorizing $f(x)$ modulo p (for all but finitely many p).

Example

- In $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$, $\alpha = \sqrt{2}$, and $f(x) = x^2 - 2$.
- To factor $7\mathcal{O}_{\mathbb{Q}(\sqrt{2})}$, we just factor $x^2 - 2 \pmod 7$.

Computing The Factorization

By the Primitive element theorem, $K = \mathbb{Q}(\alpha)$. Let $f(x)$ be the minimal polynomial of α. It turns out that factorization of $p\mathcal{O}_K$ is as easy as factorizing $f(x)$ modulo p (for all but finitely many p).

Example

- In $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$, $\alpha = \sqrt{2}$, and $f(x) = x^2 - 2$.
- To factor $7\mathcal{O}_{\mathbb{Q}(\sqrt{2})}$, we just factor $x^2 - 2 \pmod 7$.
- $x^2 - 2 \equiv (x-3)(x-4) \pmod 7$.

Computing The Factorization

By the Primitive element theorem, $K = \mathbb{Q}(\alpha)$. Let $f(x)$ be the minimal polynomial of α. It turns out that factorization of $p\mathcal{O}_K$ is as easy as factorizing $f(x)$ modulo p (for all but finitely many p).

Example

- In $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$, $\alpha = \sqrt{2}$, and $f(x) = x^2 - 2$.
- To factor $7\mathcal{O}_{\mathbb{Q}(\sqrt{2})}$, we just factor $x^2 - 2 \pmod 7$.
- $x^2 - 2 \equiv (x-3)(x-4) \pmod 7$.
- Plug in $x = \alpha$ to get product of ideals: $7\mathcal{O}_{\mathbb{Q}(\sqrt{2})} = (7, \alpha - 3)(7, \alpha - 4)$.

Computing The Factorization

By the Primitive element theorem, $K = \mathbb{Q}(\alpha)$. Let $f(x)$ be the minimal polynomial of α. It turns out that factorization of $p\mathcal{O}_K$ is as easy as factorizing $f(x)$ modulo p (for all but finitely many p).

Example

- In $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$, $\alpha = \sqrt{2}$, and $f(x) = x^2 - 2$.
- To factor $7\mathcal{O}_{\mathbb{Q}(\sqrt{2})}$, we just factor $x^2 - 2 \pmod 7$.
- $x^2 - 2 \equiv (x-3)(x-4) \pmod 7$.
- Plug in $x = \alpha$ to get product of ideals: $7\mathcal{O}_{\mathbb{Q}(\sqrt{2})} = (7, \alpha - 3)(7, \alpha - 4)$.
- Degree of terms are all 1, so all $f_i = 1$.

Galois Theory

Motivation

Motivation

Is i or $-i$ the square root of -1?

Motivation

Is i or $-i$ the square root of -1?
We arbitrarily choose i, but there is no real reason to pick one over another.

Motivation

Is i or $-i$ the square root of -1?
We arbitrarily choose i, but there is no real reason to pick one over another.
In this case, let's look at the automorphisms of $\mathbb{C}$ preserving $\mathbb{R}$.

Motivation

Is i or $-i$ the square root of -1?
We arbitrarily choose i, but there is no real reason to pick one over another.
In this case, let's look at the automorphisms of $\mathbb{C}$ preserving $\mathbb{R}$.
These consist of $\{1, \sigma\}$ where 1 is the identity on $\mathbb{C}$ and σ is complex conjugation.

Motivation

Is i or $-i$ the square root of -1?
We arbitrarily choose i, but there is no real reason to pick one over another.
In this case, let's look at the automorphisms of $\mathbb{C}$ preserving $\mathbb{R}$.
These consist of $\{1, \sigma\}$ where 1 is the identity on $\mathbb{C}$ and σ is complex conjugation.
Because complex conjugation is in here, we cannot tell i and $-i$ apart.

Motivation

Is i or $-i$ the square root of -1?
We arbitrarily choose i, but there is no real reason to pick one over another.
In this case, let's look at the automorphisms of $\mathbb{C}$ preserving $\mathbb{R}$.
These consist of $\{1, \sigma\}$ where 1 is the identity on $\mathbb{C}$ and σ is complex conjugation.
Because complex conjugation is in here, we cannot tell i and $-i$ apart.
Galois theory aims to quantify these issues.

Galois extensions

Galois extensions

Certain extensions (in our case, of number fields) behave better than others. We will study **Galois extensions**, but for the purposes of this talk we will ignore the technical details of how they are defined.

Galois extensions

Certain extensions (in our case, of number fields) behave better than others. We will study **Galois extensions**, but for the purposes of this talk we will ignore the technical details of how they are defined.

Example

$\mathbb{Q}(i)/\mathbb{Q}$, $\mathbb{Q}(\zeta_n)/\mathbb{Q}$, and $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ are all Galois extensions.

Galois group

Galois group

Definition

Let $F \subset E$ be a Galois extension. The **Galois group** of E/F, denoted as $G = \text{Gal}(E/F)$, is the set of all automorphisms of E that map every element of F to itself.

Galois group

Definition

Let $F \subset E$ be a Galois extension. The **Galois group** of E/F, denoted as $G = \text{Gal}(E/F)$, is the set of all automorphisms of E that map every element of F to itself.

Example

The automorphisms of $\mathbb{C}$ fixing $\mathbb{R}$ means that i must be sent to $\pm i$.

Galois group

Definition

Let $F \subset E$ be a Galois extension. The **Galois group** of E/F, denoted as $G = \mathrm{Gal}(E/F)$, is the set of all automorphisms of E that map every element of F to itself.

Example

The automorphisms of $\mathbb{C}$ fixing $\mathbb{R}$ means that i must be sent to $\pm i$.
If $i \mapsto i$, then it is the identity on $\mathbb{C}$. If $i \mapsto -i$, it is complex conjugation on $\mathbb{C}$.

Galois group

Definition

Let $F \subset E$ be a Galois extension. The **Galois group** of E/F, denoted as $G = \text{Gal}(E/F)$, is the set of all automorphisms of E that map every element of F to itself.

Example

The automorphisms of $\mathbb{C}$ fixing $\mathbb{R}$ means that i must be sent to $\pm i$.
If $i \mapsto i$, then it is the identity on $\mathbb{C}$. If $i \mapsto -i$, it is complex conjugation on $\mathbb{C}$.
$\text{Gal}(\mathbb{C}/\mathbb{R}) = \{1, \sigma\}$

Examples of Galois groups

Examples of Galois groups

Example

- Consider $\mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$.
- Minimal polynomial: $x^2 - 2$, roots $\pm\sqrt{2}$.
- Galois group: $\{1, f\} \cong \mathbb{Z}/2\mathbb{Z}$, with 1 is the identity automorphism and f mapping $\sqrt{2}$ to $-\sqrt{2}$.

Examples of Galois groups

Example

- Consider $\mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$.
- Minimal polynomial: $x^2 - 2$, roots $\pm\sqrt{2}$.
- Galois group: $\{1, f\} \cong \mathbb{Z}/2\mathbb{Z}$, with 1 is the identity automorphism and f mapping $\sqrt{2}$ to $-\sqrt{2}$.

Example

- Consider $\mathrm{Gal}(\mathbb{Q}(i, \sqrt{2})/\mathbb{Q})$.
- Galois group: $\{1, \alpha, \beta, \alpha\beta\} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
- 1 is identity; α fixes $\sqrt{2}$ and sends $i \mapsto -i$; β fixes i and sends $\sqrt{2} \mapsto -\sqrt{2}$.

Examples of Galois groups

Example

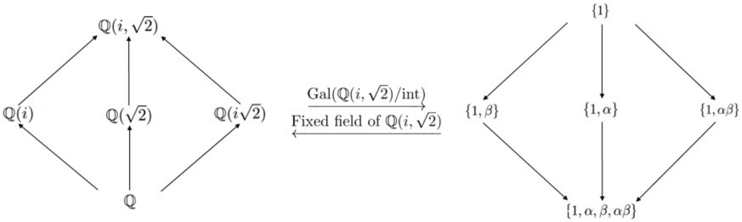
- Consider $\mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$.
- Minimal polynomial: $x^2 - 2$, roots $\pm\sqrt{2}$.
- Galois group: $\{1, f\} \cong \mathbb{Z}/2\mathbb{Z}$, with 1 is the identity automorphism and f mapping $\sqrt{2}$ to $-\sqrt{2}$.

Example

- Consider $\mathrm{Gal}(\mathbb{Q}(i, \sqrt{2})/\mathbb{Q})$.
- Galois group: $\{1, \alpha, \beta, \alpha\beta\} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
- 1 is identity; α fixes $\sqrt{2}$ and sends $i \mapsto -i$; β fixes i and sends $\sqrt{2} \mapsto -\sqrt{2}$.

We now look at a visual way to represent this.

Galois Correspondence



$$\mathrm{Gal}(\mathbb{Q}(i, \sqrt{2})/\mathbb{Q}) = \{1, \alpha, \beta, \alpha\beta\}$$

$$\alpha(\sqrt{2}) = \sqrt{2},\ \alpha(i) = -i,$$
$$\beta(\sqrt{2}) = -\sqrt{2},\ \beta(i) = i,$$
$$\alpha\beta(\sqrt{2}) = -\sqrt{2},\ \alpha\beta(i) = -i.$$

Fundamental Theorem of Galois Theory

Definition

Every finite Galois Extension and its subfields share a **1 to 1 correspondence** with the Galois Group and its subgroups.

Fundamental Theorem of Galois Theory

Definition

Every finite Galois Extension and its subfields share a **1 to 1 correspondence** with the Galois Group and its subgroups. These subfields and subgroups are in an *inclusion reversing bijection*.

Acknowledgments

We would like to thank the following:

- MIT Math Department for organizing this conference and program,
- MIT PRIMES Circle for providing us with this opportunity,
- Dr. Peter Haine, for organizing PRIMES Circle,
- Merrick Cai, our mentor, for teaching and helping us throughout the program,
- our parents for their support and encouragement,
- and our Internet connection for not giving out while we presented :)


QUESTIONS