Kronecker-Weber Theorem

Jinfei Huang

:3

July 17, 2023

Motivation

Definition

A field obtained by adjoining a complex root of unity $\zeta_n = e^{2\pi i/n}$ to the rational numbers $\mathbb{Q}$ is called a *cyclotomic field*.

Definition

Let $\mathbb{L}/\mathbb{K}$ be a field extension. The *Galois group* $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$ is the set of $\mathbb{K}$-automorphisms of $\mathbb{L}$.

Motivation

Definition

A field obtained by adjoining a complex root of unity $\zeta_n = e^{2\pi i/n}$ to the rational numbers $\mathbb{Q}$ is called a *cyclotomic field*.

Definition

Let $\mathbb{L}/\mathbb{K}$ be a field extension. The *Galois group* $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$ is the set of $\mathbb{K}$-automorphisms of $\mathbb{L}$.

$$(\mathbb{Z}/n\mathbb{Z})^\times \cong \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}), \qquad a \bmod n \mapsto (\zeta_n \mapsto \zeta_n^a)$$

Thus, $\mathbb{Q}(\zeta_n)$ is a *finite abelian extension* of $\mathbb{Q}$ of order $\phi(n)$: its Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ is abelian. In fact, every subfield of a cyclotomic field is also abelian; are these the only finite abelian extensions of $\mathbb{Q}$?

Classical main result

Theorem (Kronecker-Weber)

Every finite abelian extension of $\mathbb{Q}$ is contained in a cyclotomic field $\mathbb{Q}(\zeta_n)$.

Example

The extension $\mathbb{Q}(\sqrt{5})$ is abelian because $\mathrm{Gal}(\mathbb{Q}(\sqrt{5})/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$.
$\mathbb{Q}(\sqrt{5}) \subseteq \mathbb{Q}(\zeta_5)$, since $\sqrt{5} = e^{2\pi i/5} - e^{4\pi i/5} - e^{6\pi i/5} + e^{8\pi i/5} \in \mathbb{Q}(e^{2\pi i/5})$.

History

- Kronecker
  - announced the theorem
  - Lagrange resolvents
  - struggled with extensions of degree a power of 2
- Weber
  - published the first accepted "proof" (1886)
  - mistake went unnoticed for 90 years until it was corrected by Olaf Neumann
- Hilbert
  - gave the first complete proof in 1896
  - uses higher ramification groups
  - ideas gave rise to class field theory

Basic concepts

Definition

An *algebraic number field* K is a finite extension of the field of rational numbers $\mathbb{Q}$. Its ring of integers $\mathcal{O}_K$ is defined as the subring of $x \in K$ that are *integral* over $\mathbb{Z}$, i.e. x satisfies a monic polynomial equation with integer coefficients.

Definition

Let A be an integral domain with field of fractions $\mathbb{K}$. A *fractional ideal* $\mathfrak{a}$ of A is an A-submodule of $\mathbb{K}$ such that there is some $0 \neq d \in A$ with $d\mathfrak{a} \subseteq A$.

Definition

A *Dedekind domain* is an integral domain such that every nonzero fractional ideal is invertible.

Unique factorization of ideals

Proposition

Every nonzero proper ideal $\mathfrak{a}$ in a Dedekind domain A can be factored into a finite product $\mathfrak{a} = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\cdots\mathfrak{p}_n^{e_n}$ $(e_i > 0)$ of distinct prime ideals $\mathfrak{p}_i \neq \mathfrak{p}_j$. Furthermore, this factorization is unique up to permutation.

Importantly, the ring of integers $\mathcal{O}_K$ of an algebraic number field K is a Dedekind domain. Also, it turns out that $\mathcal{O}_K$ is a finite free $\mathbb{Z}$-module.

Ramification

Definition

Let p be a prime number and K an algebraic number field. The ideal

$$(p) = p\mathcal{O}_K = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$$

admits a factorization into distinct prime ideals $\mathfrak{P}_i$ of $\mathcal{O}_K$. We say that p is **ramified** in K if one of the exponents e_i is > 1; otherwise, p is *unramified*.

Example

In the number field $\mathbb{Q}(i)$, which has ring of integers $\mathbb{Z}[i]$, one has $2 = (1+i)(1-i)$, so $(2) = \mathfrak{P}^2$ where $\mathfrak{P} = (1+i)$ is prime.

Trace and discriminant

Definition

Let B/A be a ring extension such that B is a free A-module of rank n. For each x in B, multiplication by x defines an A-linear endomorphism $T_x : B \to B$, the trace of which we call the *trace* $\mathrm{Tr}_{B/A}(x)$ of x. Thus, $\mathrm{Tr}_{B/A}$ specifies a map from B to A.

Definition

With B/A as above, and let $\alpha_1, \ldots, \alpha_n$ be a basis for B over A. The *discriminant* $\mathrm{disc}(\alpha_1, \ldots, \alpha_n)$ of the basis $\alpha_1, \ldots, \alpha_n$ is defined as the determinant of its trace pairing matrix:

$$\mathrm{disc}(\alpha_1, \ldots, \alpha_n) = \det(\mathrm{Tr}_{B/A}(\alpha_i \alpha_j)) \in A.$$

Trace and discriminant, cont.

If $\alpha_1, \dots, \alpha_n$ and $\alpha'_1, \dots, \alpha'_n$ be two bases for the free A-module B. Write $\alpha'_j = \sum a_{ji}\alpha_i$, and let $M = (a_{ij})$ be the change of basis matrix. Then

$$\mathrm{Tr}_{B|A}(\alpha'_k \alpha'_l) = \sum_{i,j} \mathrm{Tr}_{B|A}(a_{ki}\alpha_i a_{lj}\alpha_j) = \sum_{i,j} a_{ki}\,\mathrm{Tr}_{B|A}(\alpha_i\alpha_j)a_{ji},$$

so $(\mathrm{Tr}_{B|A}(\alpha'_k\alpha'_l)) = M \cdot (\mathrm{Tr}_{B|A}(\alpha_i\alpha_j)) \cdot M^T$ and

$$\mathrm{disc}(\alpha'_1, \dots, \alpha'_n) = (\det M)^2\,\mathrm{disc}(\alpha_1, \dots, \alpha_n).$$

Therefore, as the matrix M is invertible, the discriminant is well-defined up to multiplication by the square of a unit in A. When $A = \mathbb{Z}$, the discriminant is independent of the choice of basis.

Primes that ramify

Since the ring of integers of a number field is a finite free $\mathbb{Z}$-module, we are enabled to choose a $\mathbb{Z}$-basis $\alpha_1, \ldots, \alpha_n$ and define the *discriminant* of K as $\text{disc}(\mathcal{O}_K/\mathbb{Z}) = \text{disc}(\alpha_1, \ldots, \alpha_n)$. Sometimes the notation Δ_K is used.

Primes that ramify

Since the ring of integers of a number field is a finite free $\mathbb{Z}$-module, we are enabled to choose a $\mathbb{Z}$-basis $\alpha_1, \dots, \alpha_n$ and define the *discriminant* of K as $\mathrm{disc}(\mathcal{O}_K/\mathbb{Z}) = \mathrm{disc}(\alpha_1, \dots, \alpha_n)$. Sometimes the notation Δ_K is used.

Theorem

Let K be an algebraic number field, p a prime number. Then p ramifies in K if and only if p divides the integer Δ_K.

Theorem

For any number field $K \neq \mathbb{Q}$, we have $|\Delta_K| > 1$.

Consequently, only finitely many primes p ramify in a number field K. If K is a proper extension, there is at least one such p.

Calculating the discriminant

Let us calculate the discriminant of $K = \mathbb{Q}(\zeta_p)$ for an odd prime p. The ring of integers $\mathbb{Z}[\zeta_p]$ of K admits a $\mathbb{Z}$-basis $1, \zeta_p, \ldots, \zeta_p^{p-1}$.

$$\Delta_K = \mathrm{disc}(1, \zeta_p, \ldots, \zeta_p^{p-1}) = \prod_{1 \leq i < j \leq n} (\zeta_p^i - \zeta_p^j).$$

We have the identities $p = \prod_{j=1}^{p-1}(1 - \zeta_p^j)$ and $(-1)^{p-1} = \prod_{j=0}^{p-1} \zeta_p^j$. Differentiating $X^p - 1 = \prod_{j=0}^{p-1}(X - \zeta_p^j)$ and substituting $X = \zeta_p^i$, then multiplying over all such i gives $p^p(-1)^{(p-1)^2} = \prod_{i,j=0,\, i \neq j}^{p-1}(\zeta_p^i - \zeta_p^j)$. After some algebra, we see that $\Delta_K = (-1)^{(p-1)/2} p^{p-2}$.

Reduction to prime-power order

Theorem (Kronecker-Weber)

Every finite abelian extension of $\mathbb{Q}$ is contained within a cyclotomic field.

Lemma

If the theorem holds for cyclic extensions of prime-power order, then it holds for all finite abelian extensions.

Proof (sketch).

Suppose $K/\mathbb{Q}$ is finite abelian. Then $\mathrm{Gal}(K/\mathbb{Q})$ decomposes into a direct product of cyclic groups $G_1, \ldots, G_r$ of prime-power degree. If K_i is the fixed field of $\prod_{j \neq i} G_j$, then $K_i \subseteq \mathbb{Q}(\zeta_{n_i})$ for some n_i. Setting $n = n_1 \cdots n_r$ yields

$$K = K_1 \cdots K_r \subseteq \mathbb{Q}(\zeta_n),$$

Further reductions

Lemma

It suffices to show the theorem is true for cyclic extensions $K/\mathbb{Q}$ of prime-power degree p^m such that p is the only prime that ramifies in K.

- Case 1: p is an odd prime
- Case 2: $p = 2$
  - Base case deals with quadratic extension
  - Every cyclic extension $\mathbb{K}/\mathbb{Q}$ of degree 2^m is contained in a cyclotomic field

Case 1: p is an odd prime

Lemma

Let p be a prime and let $K/\mathbb{Q}$ be a finite p-power abelian extension unramified outside p. Then $\mathrm{Gal}(K/\mathbb{Q})$ is cyclic.

Setup: $K/\mathbb{Q}$ cyclic of degree p^m such that p is the only prime that ramifies in K.

Proof of case 1 (sketch).

Recall that $\mathrm{Gal}(\mathbb{Q}(\zeta_{p^{m+1}})/\mathbb{Q}) = (\mathbb{Z}/p^{m+1}\mathbb{Z})^\times$, a cyclic group of order $\phi(p^{m+1}) = (p-1)p^m$. This group has a cyclic subgroup of index p^m. Let K' be its fixed field. Then $\mathrm{Gal}(K'/\mathbb{Q}) \cong \mathbb{Z}/p^m\mathbb{Z} = \mathrm{Gal}(K/\mathbb{Q})$. Since K and K' are unramified outside p, so is KK'. The degree of $\mathbb{K}'/\mathbb{Q}$ is a power of p, so by the previous lemma, $\mathbb{K}\mathbb{K}'/\mathbb{Q}$ is cyclic. Finally, a degree argument shows that $K = K' = KK'$, so $K \subseteq \mathbb{Q}(\zeta_{p^{m+1}})$.

Further remarks

Theorem (Local Kronecker-Weber)

Every finite abelian extension K of $\mathbb{Q}_p$ is contained in $\mathbb{Q}_p(\zeta_m)$ for some m.

The local and global versions are equivalent.

Question

Can we extend the Kronecker-Weber on abelian extensions of the rationals to any base number field?

This is known as Hilbert's 12th Problem; it is open as of 2023.

Thank you