Class Field Theory and the Kronecker-Weber Theorem

Tanvir Ahmed

July 13, 2025

History

1. 1853: Kronecker announced proof of the Kronecker-Weber Theorem:

History

1. 1853: Kronecker announced proof of the Kronecker-Weber Theorem:

Theorem (Kronecker-Weber)

Every finite abelian extension of $\mathbb{Q}$ *is contained within* $\mathbb{Q}(\zeta_m)$ *for some* $m > 0$.

History

1. 1853: Kronecker announced proof of the Kronecker-Weber Theorem:

Theorem (Kronecker-Weber)

Every finite abelian extension of $\mathbb{Q}$ *is contained within* $\mathbb{Q}(\zeta_m)$ *for some* $m > 0$.

2. 1886: Weber published "corrected" proof of KW.

History

1. 1853: Kronecker announced proof of the Kronecker-Weber Theorem:

Theorem (Kronecker-Weber)

Every finite abelian extension of $\mathbb{Q}$ *is contained within* $\mathbb{Q}(\zeta_m)$ *for some* $m > 0$.

2. 1886: Weber published "corrected" proof of KW.
3. 1896: Hilbert published first correct proof of KW and made conjectures about class fields like the Hilbert class field.

History

1. 1853: Kronecker announced proof of the Kronecker-Weber Theorem:

Theorem (Kronecker-Weber)

Every finite abelian extension of $\mathbb{Q}$ *is contained within* $\mathbb{Q}(\zeta_m)$ *for some* $m > 0$.

2. 1886: Weber published "corrected" proof of KW.
3. 1896: Hilbert published first correct proof of KW and made conjectures about class fields like the Hilbert class field.
4. 1920: Takagi announced his Existence Theorem.

History

1. 1853: Kronecker announced proof of the Kronecker-Weber Theorem:

Theorem (Kronecker-Weber)

Every finite abelian extension of $\mathbb{Q}$ is contained within $\mathbb{Q}(\zeta_m)$ for some $m > 0$.

2. 1886: Weber published "corrected" proof of KW.
3. 1896: Hilbert published first correct proof of KW and made conjectures about class fields like the Hilbert class field.
4. 1920: Takagi announced his Existence Theorem.
5. 1927: Artin made the isomorphism in the Existence Theorem explicit by proving Artin Reciprocity.

Number Fields

A number field K is a finite extension of $\mathbb{Q}$. If we have that L is a field extension of K, we write L/K.

Number Fields

A number field K is a finite extension of $\mathbb{Q}$. If we have that L is a field extension of K, we write L/K.

Example

1. $\mathbb{Q}(\sqrt{2})/\mathbb{Q} = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$.

Number Fields

A number field K is a finite extension of $\mathbb{Q}$. If we have that L is a field extension of K, we write L/K.

Example

1. $\mathbb{Q}(\sqrt{2})/\mathbb{Q} = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$.
2. $\mathbb{Q}(\sqrt{3}, \sqrt{5})/\mathbb{Q} = \{a + b\sqrt{3} + c\sqrt{5} + d\sqrt{15} \mid a, b, c, d \in \mathbb{Q}\}$.

Number Fields

A number field K is a finite extension of $\mathbb{Q}$. If we have that L is a field extension of K, we write L/K.

Example

1. $\mathbb{Q}(\sqrt{2})/\mathbb{Q} = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$.
2. $\mathbb{Q}(\sqrt{3}, \sqrt{5})/\mathbb{Q} = \{a + b\sqrt{3} + c\sqrt{5} + d\sqrt{15} \mid a, b, c, d \in \mathbb{Q}\}$.
3. $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q} = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in \mathbb{Q}\}$.

Number Fields

A number field K is a finite extension of $\mathbb{Q}$. If we have that L is a field extension of K, we write L/K.

Example

1. $\mathbb{Q}(\sqrt{2})/\mathbb{Q} = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$.
2. $\mathbb{Q}(\sqrt{3}, \sqrt{5})/\mathbb{Q} = \{a + b\sqrt{3} + c\sqrt{5} + d\sqrt{15} \mid a, b, c, d \in \mathbb{Q}\}$.
3. $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q} = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in \mathbb{Q}\}$.
4. $\mathbb{Q}(\zeta_p)/\mathbb{Q} = \{a_0 + a_1\zeta_p + \cdots + a_{p-2}\zeta_p^{p-2} \mid a_i \in \mathbb{Q}\}$.

Number Fields

A number field K is a finite extension of $\mathbb{Q}$. If we have that L is a field extension of K, we write L/K.

Example

1. $\mathbb{Q}(\sqrt{2})/\mathbb{Q} = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$.
2. $\mathbb{Q}(\sqrt{3}, \sqrt{5})/\mathbb{Q} = \{a + b\sqrt{3} + c\sqrt{5} + d\sqrt{15} \mid a, b, c, d \in \mathbb{Q}\}$.
3. $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q} = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in \mathbb{Q}\}$.
4. $\mathbb{Q}(\zeta_p)/\mathbb{Q} = \{a_0 + a_1\zeta_p + \cdots + a_{p-2}\zeta_p^{p-2} \mid a_i \in \mathbb{Q}\}$.

Each of these has a ring of integers, and they are $\mathbb{Z}[\sqrt{2}]$, $\mathbb{Z}[\sqrt{3}, \frac{1}{2}(1 + \sqrt{5})]$, $\mathbb{Z}[\sqrt[3]{2}]$, and $\mathbb{Z}[\zeta_p]$ respectively. The ring of integers of a number field K is denoted $\mathcal{O}_K$, and is always a free $\mathbb{Z}$-module of finite rank $[K : \mathbb{Q}]$ i.e. it looks like $\mathbb{Z}[\alpha_1, \ldots, \alpha_n]$ (but n isn't necessarily 1).

Number Fields continued

A key theorem in Algebraic Number Theory is that ideals in $\mathcal{O}_K$ have unique factorization.

Number Fields continued

A key theorem in Algebraic Number Theory is that ideals in $\mathcal{O}_K$ have unique factorization. That is, there is some set of prime ideals $\mathfrak{p}_1, \mathfrak{p}_2, \ldots$ such that all ideals are a unique product of powers of these ideals.

Number Fields continued

A key theorem in Algebraic Number Theory is that ideals in $\mathcal{O}_K$ have unique factorization. That is, there is some set of prime ideals $\mathfrak{p}_1, \mathfrak{p}_2, \ldots$ such that all ideals are a unique product of powers of these ideals.

Example

Let $K = \mathbb{Q}(i)$, $\mathcal{O}_K = \mathbb{Z}[i]$.

Number Fields continued

A key theorem in Algebraic Number Theory is that ideals in $\mathcal{O}_K$ have unique factorization. That is, there is some set of prime ideals $\mathfrak{p}_1, \mathfrak{p}_2, \ldots$ such that all ideals are a unique product of powers of these ideals.

Example

Let $K = \mathbb{Q}(i)$, $\mathcal{O}_K = \mathbb{Z}[i]$. It turns out $\mathbb{Z}[i]$ is a PID, so ideals are essentially the same as elements of the ring.

Number Fields continued

A key theorem in Algebraic Number Theory is that ideals in $\mathcal{O}_K$ have unique factorization. That is, there is some set of prime ideals $\mathfrak{p}_1, \mathfrak{p}_2, \ldots$ such that all ideals are a unique product of powers of these ideals.

Example

Let $K = \mathbb{Q}(i)$, $\mathcal{O}_K = \mathbb{Z}[i]$. It turns out $\mathbb{Z}[i]$ is a PID, so ideals are essentially the same as elements of the ring.

- (3) remains **inert** since it can't be factored further in $\mathbb{Z}[i]$.

Number Fields continued

A key theorem in Algebraic Number Theory is that ideals in $\mathcal{O}_K$ have unique factorization. That is, there is some set of prime ideals $\mathfrak{p}_1, \mathfrak{p}_2, \ldots$ such that all ideals are a unique product of powers of these ideals.

Example

Let $K = \mathbb{Q}(i)$, $\mathcal{O}_K = \mathbb{Z}[i]$. It turns out $\mathbb{Z}[i]$ is a PID, so ideals are essentially the same as elements of the ring.

- (3) remains **inert** since it can't be factored further in $\mathbb{Z}[i]$.
- (5) **splits** as $(5) = (1 + 2i)(1 - 2i)$.

Galois Extensions

Galois extensions of number fields are very nice. For simplicity, let's consider a general extension $K/\mathbb{Q}$. If p is a rational prime, we can factor the ideal $(p) = \{p\alpha \mid \alpha \in \mathcal{O}_K\}$ in $\mathcal{O}_K$, and we get something like this:

Galois Extensions

Galois extensions of number fields are very nice. For simplicity, let's consider a general extension $K/\mathbb{Q}$. If p is a rational prime, we can factor the ideal $(p) = \{p\alpha \mid \alpha \in \mathcal{O}_K\}$ in $\mathcal{O}_K$, and we get something like this:

$$(p) = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g}$$

for distinct prime ideals $\mathfrak{p}_i \subset \mathcal{O}_K$. We say that $\mathfrak{p}_i$'s lie **above** the ideal (p).

Galois Extensions

Galois extensions of number fields are very nice. For simplicity, let's consider a general extension $K/\mathbb{Q}$. If p is a rational prime, we can factor the ideal $(p) = \{p\alpha \mid \alpha \in \mathcal{O}_K\}$ in $\mathcal{O}_K$, and we get something like this:

$$(p) = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g}$$

for distinct prime ideals $\mathfrak{p}_i \subset \mathcal{O}_K$. We say that $\mathfrak{p}_i$'s lie **above** the ideal (p).

Now suppose $K/\mathbb{Q}$ is Galois. Then, $\mathrm{Gal}(K/\mathbb{Q})$ acts on the set $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_g\}$ because if $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$, $\sigma(\mathfrak{p}_i)$ is also a prime ideal above (p).

Galois Extensions

Galois extensions of number fields are very nice. For simplicity, let's consider a general extension $K/\mathbb{Q}$. If p is a rational prime, we can factor the ideal $(p) = \{p\alpha \mid \alpha \in \mathcal{O}_K\}$ in $\mathcal{O}_K$, and we get something like this:

$$(p) = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g}$$

for distinct prime ideals $\mathfrak{p}_i \subset \mathcal{O}_K$. We say that $\mathfrak{p}_i$'s lie **above** the ideal (p).

Now suppose $K/\mathbb{Q}$ is Galois. Then, $\mathrm{Gal}(K/\mathbb{Q})$ acts on the set $\{\mathfrak{p}_1, \dots, \mathfrak{p}_g\}$ because if $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$, $\sigma(\mathfrak{p}_i)$ is also a prime ideal above (p). It turns out that it also acts *transitively* on this set. In particular, for $1 \leq i, j \leq g$, there is $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ such that $\sigma(\mathfrak{p}_i) = \mathfrak{p}_j$.

Galois Extensions 2

This fact allows us to prove the following.

Galois Extensions 2

This fact allows us to prove the following.

Theorem

Let $K/\mathbb{Q}$ be Galois and p a rational prime.

Galois Extensions 2

This fact allows us to prove the following.

Theorem

Let $K/\mathbb{Q}$ be Galois and p a rational prime. Suppose

$$(p) = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g}$$

where the $\mathfrak{p}_i$'s are distinct primes.

Galois Extensions 2

This fact allows us to prove the following.

Theorem

Let $K/\mathbb{Q}$ be Galois and p a rational prime. Suppose

$$(p) = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g}$$

where the $\mathfrak{p}_i$'s are distinct primes. Then, $e_1 = \cdots = e_g$.

Galois Extensions 2

This fact allows us to prove the following.

Theorem

Let $K/\mathbb{Q}$ be Galois and p a rational prime. Suppose

$$(p) = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g}$$

where the $\mathfrak{p}_i$'s are distinct primes. Then, $e_1 = \cdots = e_g$.

Proof.

Choose $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ such that $\sigma(\mathfrak{p}_1) = \mathfrak{p}_i$.

Galois Extensions 2

This fact allows us to prove the following.

Theorem

Let $K/\mathbb{Q}$ be Galois and p a rational prime. Suppose

$$(p) = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g}$$

where the $\mathfrak{p}_i$'s are distinct primes.Then, $e_1 = \cdots = e_g$.

Proof.

Choose $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ such that $\sigma(\mathfrak{p}_1) = \mathfrak{p}_i$.We get

$$(p) = \sigma((p)) = \mathfrak{p}_i^{e_1} \cdots \sigma(\mathfrak{p}_g)^{e_g}.$$

Galois Extensions 2

This fact allows us to prove the following.

Theorem

Let $K/\mathbb{Q}$ be Galois and p a rational prime. Suppose

$$(p) = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g}$$

where the $\mathfrak{p}_i$'s are distinct primes. Then, $e_1 = \cdots = e_g$.

Proof.

Choose $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ such that $\sigma(\mathfrak{p}_1) = \mathfrak{p}_i$. We get

$$(p) = \sigma((p)) = \mathfrak{p}_i^{e_1} \cdots \sigma(\mathfrak{p}_g)^{e_g}.$$

σ permutes the $\mathfrak{p}_i$'s, so each of the primes in this factorization is distinct. Therefore, we can compare the exponent of $\mathfrak{p}_i$ in the two factorizations we have and conclude $e_1 = e_i$. ∎

Galois Extensions 3

We call $e = e_1 = \cdots = e_g$ the **ramification index** of p, and if $e > 1$, p is ramified.

Galois Extensions 3

We call $e = e_1 = \cdots = e_g$ the **ramification index** of p, and if $e > 1$, p is ramified. For example, 2 is ramified in $\mathbb{Q}(i)$ because $(2) = (1+i)^2$.

Galois Extensions 3

We call $e = e_1 = \cdots = e_g$ the **ramification index** of p, and if $e > 1$, p is ramified. For example, 2 is ramified in $\mathbb{Q}(i)$ because $(2) = (1+i)^2$.

Theorem

Let e and g be defined as before. Then, $eg \mid [K : \mathbb{Q}]$.

Galois Extensions 3

We call $e = e_1 = \cdots = e_g$ the **ramification index** of p, and if $e > 1$, p is ramified. For example, 2 is ramified in $\mathbb{Q}(i)$ because $(2) = (1+i)^2$.

Theorem

Let e and g be defined as before. Then, $eg \mid [K : \mathbb{Q}]$.

We say a prime completely splits if $g = [K : \mathbb{Q}]$.

Galois Extensions 3

We call $e = e_1 = \cdots = e_g$ the **ramification index** of p, and if $e > 1$, p is ramified. For example, 2 is ramified in $\mathbb{Q}(i)$ because $(2) = (1+i)^2$.

Theorem

Let e and g be defined as before. Then, $eg \mid [K : \mathbb{Q}]$.

We say a prime completely splits if $g = [K : \mathbb{Q}]$.

Theorem

For an extension $K/\mathbb{Q}$, p ramifies $\iff p \mid \Delta_K$.

Galois Extensions 3

We call $e = e_1 = \cdots = e_g$ the **ramification index** of p, and if $e > 1$, p is ramified. For example, 2 is ramified in $\mathbb{Q}(i)$ because $(2) = (1+i)^2$.

Theorem

Let e and g be defined as before. Then, $eg \mid [K : \mathbb{Q}]$.

We say a prime completely splits if $g = [K : \mathbb{Q}]$.

Theorem

For an extension $K/\mathbb{Q}$, p ramifies $\iff p \mid \Delta_K$.

For $\mathcal{O}_K = \mathbb{Z}[\alpha]$, Δ_K is the discriminant of the minimal polynomial of α.

Cyclotomic Extensions

The cyclotomic extensions of $\mathbb{Q}$ are of the form $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ for $m > 1$.

Cyclotomic Extensions

The cyclotomic extensions of $\mathbb{Q}$ are of the form $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ for $m > 1$. We have $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) = (\mathbb{Z}/m\mathbb{Z})^{\times}$. Elements of the Galois Group look like

Cyclotomic Extensions

The cyclotomic extensions of $\mathbb{Q}$ are of the form $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ for $m > 1$. We have $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) = (\mathbb{Z}/m\mathbb{Z})^\times$. Elements of the Galois Group look like

$$\sigma_r : \zeta_m \to \zeta_m^r,$$

Cyclotomic Extensions

The cyclotomic extensions of $\mathbb{Q}$ are of the form $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ for $m > 1$. We have $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) = (\mathbb{Z}/m\mathbb{Z})^\times$. Elements of the Galois Group look like

$$\sigma_r : \zeta_m \to \zeta_m^r, \ \sigma_r \sigma_s = \sigma_{rs}$$

where the indices of the σ's are taken mod m.

Cyclotomic Extensions

The cyclotomic extensions of $\mathbb{Q}$ are of the form $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ for $m > 1$. We have $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) = (\mathbb{Z}/m\mathbb{Z})^\times$. Elements of the Galois Group look like

$$\sigma_r : \zeta_m \to \zeta_m^r, \ \sigma_r\sigma_s = \sigma_{rs}$$

where the indices of the σ's are taken mod m. For p an odd prime, we can calculate the discriminant of $\mathbb{Q}(\zeta_p)$, which is a fun calculation to do:

Cyclotomic Extensions

The cyclotomic extensions of $\mathbb{Q}$ are of the form $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ for $m > 1$. We have $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) = (\mathbb{Z}/m\mathbb{Z})^\times$. Elements of the Galois Group look like

$$\sigma_r : \zeta_m \to \zeta_m^r,\ \sigma_r\sigma_s = \sigma_{rs}$$

where the indices of the σ's are taken mod m. For p an odd prime, we can calculate the discriminant of $\mathbb{Q}(\zeta_p)$, which is a fun calculation to do:

$$\Delta_{\mathbb{Q}(\zeta_p)} = \prod_{1\leq i<j\leq p-1} (\zeta_p^i - \zeta_p^j)^2$$

Cyclotomic Extensions

The cyclotomic extensions of $\mathbb{Q}$ are of the form $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ for $m > 1$. We have $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) = (\mathbb{Z}/m\mathbb{Z})^\times$. Elements of the Galois Group look like

$$\sigma_r : \zeta_m \to \zeta_m^r, \ \sigma_r \sigma_s = \sigma_{rs}$$

where the indices of the σ's are taken mod m. For p an odd prime, we can calculate the discriminant of $\mathbb{Q}(\zeta_p)$, which is a fun calculation to do:

$$\Delta_{\mathbb{Q}(\zeta_p)} = \prod_{1 \le i < j \le p-1} (\zeta_p^i - \zeta_p^j)^2 = (-1)^{\frac{p-1}{2}} p^{p-2}.$$

Cyclotomic Extensions

The cyclotomic extensions of $\mathbb{Q}$ are of the form $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ for $m > 1$. We have $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) = (\mathbb{Z}/m\mathbb{Z})^\times$. Elements of the Galois Group look like

$$\sigma_r : \zeta_m \to \zeta_m^r,\ \sigma_r\sigma_s = \sigma_{rs}$$

where the indices of the σ's are taken mod m. For p an odd prime, we can calculate the discriminant of $\mathbb{Q}(\zeta_p)$, which is a fun calculation to do:

$$\Delta_{\mathbb{Q}(\zeta_p)} = \prod_{1 \le i < j \le p-1} (\zeta_p^i - \zeta_p^j)^2 = (-1)^{\frac{p-1}{2}} p^{p-2}.$$

Thus, only p ramifies in $\mathbb{Q}(\zeta_p)$. In general, only primes dividing m ramify in $\mathbb{Q}(\zeta_m)$.

Cyclotomic Extensions

The cyclotomic extensions of $\mathbb{Q}$ are of the form $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ for $m > 1$. We have $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) = (\mathbb{Z}/m\mathbb{Z})^\times$. Elements of the Galois Group look like

$$\sigma_r : \zeta_m \to \zeta_m^r,\ \sigma_r\sigma_s = \sigma_{rs}$$

where the indices of the σ's are taken mod m. For p an odd prime, we can calculate the discriminant of $\mathbb{Q}(\zeta_p)$, which is a fun calculation to do:

$$\Delta_{\mathbb{Q}(\zeta_p)} = \prod_{1 \le i < j \le p-1} (\zeta_p^i - \zeta_p^j)^2 = (-1)^{\frac{p-1}{2}} p^{p-2}.$$

Thus, only p ramifies in $\mathbb{Q}(\zeta_p)$. In general, only primes dividing m ramify in $\mathbb{Q}(\zeta_m)$.

Example

In $\mathbb{Z}[\zeta_7]$, $(7) = (7, \zeta_7 - 1)^6$ which comes from the factorization $x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 \equiv (x-1)^6 \pmod 7$.

Cyclotomic Extensions 2

The only primes that completely split in $\mathbb{Q}(\zeta_m)$ are (p) for $p \equiv 1 \pmod{m}$. For example, in $\mathbb{Q}(\zeta_5)$, we have

Cyclotomic Extensions 2

The only primes that completely split in $\mathbb{Q}(\zeta_m)$ are (p) for $p \equiv 1 \pmod{m}$. For example, in $\mathbb{Q}(\zeta_5)$, we have

$$(11) = (11, \zeta_5 - 3)(11, \zeta_5 - 4)(11, \zeta_5 - 5)(11, \zeta_5 - 9)$$

Cyclotomic Extensions 2

The only primes that completely split in $\mathbb{Q}(\zeta_m)$ are (p) for $p \equiv 1 \pmod{m}$. For example, in $\mathbb{Q}(\zeta_5)$, we have

$$(11) = (11, \zeta_5 - 3)(11, \zeta_5 - 4)(11, \zeta_5 - 5)(11, \zeta_5 - 9)$$

while

$$(19) = (19, \zeta_5^2 + 5\zeta_5 + 1)(19, \zeta_5^2 + 15\zeta_5 + 1)$$

Cyclotomic Extensions 2

The only primes that completely split in $\mathbb{Q}(\zeta_m)$ are (p) for $p \equiv 1 \pmod{m}$. For example, in $\mathbb{Q}(\zeta_5)$, we have

$$(11) = (11, \zeta_5 - 3)(11, \zeta_5 - 4)(11, \zeta_5 - 5)(11, \zeta_5 - 9)$$

while

$$(19) = (19, \zeta_5^2 + 5\zeta_5 + 1)(19, \zeta_5^2 + 15\zeta_5 + 1)$$

which come from the factorizations

Cyclotomic Extensions 2

The only primes that completely split in $\mathbb{Q}(\zeta_m)$ are (p) for $p \equiv 1 \pmod{m}$. For example, in $\mathbb{Q}(\zeta_5)$, we have

$$(11) = (11, \zeta_5 - 3)(11, \zeta_5 - 4)(11, \zeta_5 - 5)(11, \zeta_5 - 9)$$

while

$$(19) = (19, \zeta_5^2 + 5\zeta_5 + 1)(19, \zeta_5^2 + 15\zeta_5 + 1)$$

which come from the factorizations

$$x^4 + x^3 + x^2 + x + 1 \equiv (x-3)(x-4)(x-5)(x-9) \pmod{11}$$
$$x^4 + x^3 + x^2 + x + 1 \equiv (x^2 + 5x + 1)(x^2 + 15x + 1) \pmod{19}$$

Abelian Extesions

A Galois extension L/K is called abelian if $\mathrm{Gal}(L/K)$ is abelian.

Abelian Extesions

A Galois extension L/K is called abelian if $\mathrm{Gal}(L/K)$ is abelian. By Galois Theory, the subextensions of $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ have Galois groups corresponding to the subgroups of $(\mathbb{Z}/m\mathbb{Z})^\times$, which are all abelian.

Abelian Extesions

A Galois extension L/K is called abelian if $\mathrm{Gal}(L/K)$ is abelian. By Galois Theory, the subextensions of $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ have Galois groups corresponding to the subgroups of $(\mathbb{Z}/m\mathbb{Z})^\times$, which are all abelian.

For example, for p an odd prime, there is a quadratic extension of $\mathbb{Q}$ contained in $\mathbb{Q}(\zeta_p)$ (all quadratic extensions are abelian). This field is $\mathbb{Q}(\sqrt{p^*})$ where $p^* = \pm p$ and $p^* \equiv 1 \pmod 4$. Some of you know this better as Gauss sums.

Abelian Extesions

A Galois extension L/K is called abelian if $\mathrm{Gal}(L/K)$ is abelian. By Galois Theory, the subextensions of $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ have Galois groups corresponding to the subgroups of $(\mathbb{Z}/m\mathbb{Z})^\times$, which are all abelian.

For example, for p an odd prime, there is a quadratic extension of $\mathbb{Q}$ contained in $\mathbb{Q}(\zeta_p)$ (all quadratic extensions are abelian). This field is $\mathbb{Q}(\sqrt{p^*})$ where $p^* = \pm p$ and $p^* \equiv 1 \pmod 4$. Some of you know this better as Gauss sums.

Example

- $\mathbb{Q}(\sqrt{5}) \subset \mathbb{Q}(\zeta_5)$ and $\zeta_5 - \zeta_5^2 - \zeta_5^3 + \zeta_5^4 = \sqrt{5}$.

Abelian Extesions

A Galois extension L/K is called abelian if $\mathrm{Gal}(L/K)$ is abelian. By Galois Theory, the subextensions of $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ have Galois groups corresponding to the subgroups of $(\mathbb{Z}/m\mathbb{Z})^\times$, which are all abelian.

For example, for p an odd prime, there is a quadratic extension of $\mathbb{Q}$ contained in $\mathbb{Q}(\zeta_p)$ (all quadratic extensions are abelian). This field is $\mathbb{Q}(\sqrt{p^*})$ where $p^* = \pm p$ and $p^* \equiv 1 \pmod 4$. Some of you know this better as Gauss sums.

Example

- $\mathbb{Q}(\sqrt{5}) \subset \mathbb{Q}(\zeta_5)$ and $\zeta_5 - \zeta_5^2 - \zeta_5^3 + \zeta_5^4 = \sqrt{5}$.
- $\mathbb{Q}(\sqrt{-7}) \subset \mathbb{Q}(\zeta_7)$ and $\zeta_7 + \zeta_7^2 - \zeta_7^3 + \zeta_7^4 - \zeta_7^5 - \zeta_7^6 = \sqrt{-7}$.

Abelian Extesions

A Galois extension L/K is called abelian if $\text{Gal}(L/K)$ is abelian. By Galois Theory, the subextensions of $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ have Galois groups corresponding to the subgroups of $(\mathbb{Z}/m\mathbb{Z})^\times$, which are all abelian.

For example, for p an odd prime, there is a quadratic extension of $\mathbb{Q}$ contained in $\mathbb{Q}(\zeta_p)$ (all quadratic extensions are abelian). This field is $\mathbb{Q}(\sqrt{p^*})$ where $p^* = \pm p$ and $p^* \equiv 1 \pmod 4$. Some of you know this better as Gauss sums.

Example

- $\mathbb{Q}(\sqrt{5}) \subset \mathbb{Q}(\zeta_5)$ and $\zeta_5 - \zeta_5^2 - \zeta_5^3 + \zeta_5^4 = \sqrt{5}$.
- $\mathbb{Q}(\sqrt{-7}) \subset \mathbb{Q}(\zeta_7)$ and $\zeta_7 + \zeta_7^2 - \zeta_7^3 + \zeta_7^4 - \zeta_7^5 - \zeta_7^6 = \sqrt{-7}$.

The Kronecker-Weber Theorem states that all finite abelian extensions of $\mathbb{Q}$ arise from taking subextensions of the cyclotomic extensions.

Statements of Class Field Theory: Moduli

For a number field K, a modulus $\mathfrak{m}$ is a formal product of prime ideals of $\mathcal{O}_K$ and real embeddings of K. We write $\mathfrak{m} = \mathfrak{m}_0 \mathfrak{m}_\infty$ where:

Statements of Class Field Theory: Moduli

For a number field K, a modulus $\mathfrak{m}$ is a formal product of prime ideals of $\mathcal{O}_K$ and real embeddings of K. We write $\mathfrak{m} = \mathfrak{m}_0 \mathfrak{m}_\infty$ where:

- The finite part $\mathfrak{m}_0$ is just an ideal of $\mathcal{O}_K$.

Statements of Class Field Theory: Moduli

For a number field K, a modulus $\mathfrak{m}$ is a formal product of prime ideals of $\mathcal{O}_K$ and real embeddings of K. We write $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$ where:

- The finite part $\mathfrak{m}_0$ is just an ideal of $\mathcal{O}_K$.
- The infinite part $\mathfrak{m}_\infty$ is a set of real embeddings (injective field homomorphisms $\tau : K \to \mathbb{R}$) of K.

Statements of Class Field Theory: Moduli

For a number field K, a modulus $\mathfrak{m}$ is a formal product of prime ideals of $\mathcal{O}_K$ and real embeddings of K. We write $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$ where:

- The finite part $\mathfrak{m}_0$ is just an ideal of $\mathcal{O}_K$.
- The infinite part $\mathfrak{m}_\infty$ is a set of real embeddings (injective field homomorphisms $\tau : K \to \mathbb{R}$) of K.

Example

- All moduli of $\mathbb{Q}$ are of the form m or $m\infty$ for a positive integer m.

Statements of Class Field Theory: Moduli

For a number field K, a modulus $\mathfrak{m}$ is a formal product of prime ideals of $\mathcal{O}_K$ and real embeddings of K. We write $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$ where:

- The finite part $\mathfrak{m}_0$ is just an ideal of $\mathcal{O}_K$.
- The infinite part $\mathfrak{m}_\infty$ is a set of real embeddings (injective field homomorphisms $\tau : K \to \mathbb{R}$) of K.

Example

- All moduli of $\mathbb{Q}$ are of the form m or $m\infty$ for a positive integer m.
- The moduli of $\mathbb{Q}(i)$ are just the ideals of $\mathbb{Z}[i]$ because $\mathbb{Q}(i)$ has no real embeddings.

Statements of Class Field Theory: Ray Class Groups

The Ray Class Groups are generalizations of the normal class group. Let K be a number field and $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$ a modulus in what continues.

Statements of Class Field Theory: Ray Class Groups

The Ray Class Groups are generalizations of the normal class group. Let K be a number field and $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$ a modulus in what continues.

Definition

- Let $I_K^{\mathfrak{m}}$ be the multiplicative group of fractional ideals of $\mathcal{O}_K$ which are relatively prime to $\mathfrak{m}$.

Statements of Class Field Theory: Ray Class Groups

The Ray Class Groups are generalizations of the normal class group. Let K be a number field and $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$ a modulus in what continues.

Definition

- Let $I_K^{\mathfrak{m}}$ be the multiplicative group of fractional ideals of $\mathcal{O}_K$ which are relatively prime to $\mathfrak{m}$.
- Let $P_K^{\mathfrak{m}}$ be the multiplicative group of principal fractional ideals of the form $\alpha\mathcal{O}_K$ ($\alpha \in K^\times$) such that $\alpha \equiv 1 \pmod{\mathfrak{m}_0}$ and for any $\tau \in \mathfrak{m}_\infty$, $\tau(\alpha) > 0$.

Statements of Class Field Theory: Ray Class Groups

The Ray Class Groups are generalizations of the normal class group. Let K be a number field and $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$ a modulus in what continues.

Definition

- Let $I_K^{\mathfrak{m}}$ be the multiplicative group of fractional ideals of $\mathcal{O}_K$ which are relatively prime to $\mathfrak{m}$.
- Let $P_K^{\mathfrak{m}}$ be the multiplicative group of principal fractional ideals of the form $\alpha\mathcal{O}_K$ $(\alpha \in K^\times)$ such that $\alpha \equiv 1 \pmod{\mathfrak{m}_0}$ and for any $\tau \in \mathfrak{m}_\infty$, $\tau(\alpha) > 0$.

Then, we define $\mathrm{Cl}_K^{\mathfrak{m}} = I_K^{\mathfrak{m}}/P_K^{\mathfrak{m}}$. For $\mathfrak{m} = (1)$, we get $\mathrm{Cl}_K^{\mathfrak{m}} = \mathrm{Cl}(K)$, the usual class group.

Statements of Class Field Theory: Ray Class Groups

The Ray Class Groups are generalizations of the normal class group. Let K be a number field and $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$ a modulus in what continues.

Definition

- Let $I_K^{\mathfrak{m}}$ be the multiplicative group of fractional ideals of $\mathcal{O}_K$ which are relatively prime to $\mathfrak{m}$.
- Let $P_K^{\mathfrak{m}}$ be the multiplicative group of principal fractional ideals of the form $\alpha\mathcal{O}_K$ $(\alpha \in K^\times)$ such that $\alpha \equiv 1 \pmod{\mathfrak{m}_0}$ and for any $\tau \in \mathfrak{m}_\infty$, $\tau(\alpha) > 0$.

Then, we define $\mathrm{Cl}_K^{\mathfrak{m}} = I_K^{\mathfrak{m}}/P_K^{\mathfrak{m}}$. For $\mathfrak{m} = (1)$, we get $\mathrm{Cl}_K^{\mathfrak{m}} = \mathrm{Cl}(K)$, the usual class group.

Example

$\mathrm{Cl}_{\mathbb{Q}}^{m} = (\mathbb{Z}/m\mathbb{Z})^\times/\{\pm 1\}$ and $\mathrm{Cl}_{\mathbb{Q}}^{m\infty} = (\mathbb{Z}/m\mathbb{Z})^\times$ for $m > 1$.

Statements of Class Field Theory: Existence Theorem

During WW1, Teiji Takagi proved the following (this is only a corollary of the Existence Theorem):

Statements of Class Field Theory: Existence Theorem

During WW1, Teiji Takagi proved the following (this is only a corollary of the Existence Theorem):

Theorem (Existence Theorem)

Let K be a number field. For every modulus $\mathfrak{m}$, there is a unique ray class field $K_{\mathfrak{m}}$ such that $\mathrm{Gal}(K_{\mathfrak{m}}/K) \cong \mathrm{Cl}_K^{\mathfrak{m}}$

During WW1, Teiji Takagi proved the following (this is only a corollary of the Existence Theorem):

Theorem (Existence Theorem)

Let K be a number field. For every modulus $\mathfrak{m}$, there is a unique ray class field $K_{\mathfrak{m}}$ such that $\mathrm{Gal}(K_{\mathfrak{m}}/K) \cong \mathrm{Cl}_K^{\mathfrak{m}}$ and the prime ideals that completely split are those contained in $P_K^{\mathfrak{m}}$.

Statements of Class Field Theory: Existence Theorem

During WW1, Teiji Takagi proved the following (this is only a corollary of the Existence Theorem):

Theorem (Existence Theorem)

Let K be a number field. For every modulus $\mathfrak{m}$, there is a unique ray class field $K_{\mathfrak{m}}$ such that $\mathrm{Gal}(K_{\mathfrak{m}}/K) \cong \mathrm{Cl}_K^{\mathfrak{m}}$ and the prime ideals that completely split are those contained in $P_K^{\mathfrak{m}}$. Furthermore, every finite abelian extension of K is a subfield of one of these $K_{\mathfrak{m}}$'s.

Kronecker-Weber Theorem

Let $K = \mathbb{Q}$. We want to know what the ray class fields are. It turns out $K_{m\infty} = \mathbb{Q}(\zeta_m)$. This is because

Kronecker-Weber Theorem

Let $K = \mathbb{Q}$. We want to know what the ray class fields are. It turns out $K_{m\infty} = \mathbb{Q}(\zeta_m)$. This is because

$$\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \cong \mathrm{Cl}_{\mathbb{Q}}^{m\infty} \cong (\mathbb{Z}/m\mathbb{Z})^\times$$

Kronecker-Weber Theorem

Let $K = \mathbb{Q}$. We want to know what the ray class fields are. It turns out $K_{m\infty} = \mathbb{Q}(\zeta_m)$. This is because

$$\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \cong \mathrm{Cl}_{\mathbb{Q}}^{m\infty} \cong (\mathbb{Z}/m\mathbb{Z})^\times$$

and the primes that split in $\mathbb{Q}(\zeta_m)$ are exactly the primes in $P_K^{m\infty} = \{\frac{a}{b}\mathbb{Q} \mid \frac{a}{b} \equiv 1 \pmod{m}\}$ (i.e. the primes that are 1 mod m).

Kronecker-Weber Theorem

Let $K = \mathbb{Q}$. We want to know what the ray class fields are. It turns out $K_{m\infty} = \mathbb{Q}(\zeta_m)$. This is because

$$\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \cong \mathrm{Cl}_{\mathbb{Q}}^{m\infty} \cong (\mathbb{Z}/m\mathbb{Z})^\times$$

and the primes that split in $\mathbb{Q}(\zeta_m)$ are exactly the primes in $P_K^{m\infty} = \{\frac{a}{b}\mathbb{Q} \mid \frac{a}{b} \equiv 1 \pmod{m}\}$ (i.e. the primes that are 1 mod m). It turns out that K_m, the other possible type of ray class fields for $\mathbb{Q}$, are of the form $\mathbb{Q}(\zeta_m + \zeta_m^{-1})$, which are index-2 subfields of $\mathbb{Q}(\zeta_m)$. Either way, we get the following:

Kronecker-Weber Theorem

Let $K = \mathbb{Q}$. We want to know what the ray class fields are. It turns out $K_{m\infty} = \mathbb{Q}(\zeta_m)$. This is because

$$\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \cong \mathrm{Cl}_{\mathbb{Q}}^{m\infty} \cong (\mathbb{Z}/m\mathbb{Z})^\times$$

and the primes that split in $\mathbb{Q}(\zeta_m)$ are exactly the primes in $P_K^{m\infty} = \{\frac{a}{b}\mathbb{Q} \mid \frac{a}{b} \equiv 1 \pmod{m}\}$ (i.e. the primes that are 1 mod m). It turns out that K_m, the other possible type of ray class fields for $\mathbb{Q}$, are of the form $\mathbb{Q}(\zeta_m + \zeta_m^{-1})$, which are index-2 subfields of $\mathbb{Q}(\zeta_m)$. Either way, we get the following:

Theorem (Kronecker-Weber)

Every finite abelian extension of $\mathbb{Q}$ is contained within $\mathbb{Q}(\zeta_m)$ for some $m > 0$.