Hilbert Class Field and the Artin Map

Albert Lopez Bruch

16 May, 2024

Recap from Talk 1

Recall the main results from last week:

Theorem

Let K be a number field. Then K has a maximal unramified abelian extensions H, denoted as the **Hilbert class field** *of K.*

Recap from Talk 1

Recall the main results from last week:

Theorem

Let K be a number field. Then K has a maximal unramified abelian extensions H, denoted as the **Hilbert class field** *of K. Furthermore,*

- $\mathrm{Gal}(H/K) \cong \mathrm{Cl}(K)$ *and hence* $[H : K] = h(K)$.

Recap from Talk 1

Recall the main results from last week:

Theorem

Let K be a number field. Then K has a maximal unramified abelian extensions H, denoted as the **Hilbert class field** *of K. Furthermore,*

- $\mathrm{Gal}(H/K) \cong \mathrm{Cl}(K)$ *and hence* $[H:K] = h(K)$.
- *Splitting Property: If $\mathfrak{p}$ is a prime ideal of K, and f is the order of $[\mathfrak{p}]$ in $\mathrm{Cl}(K)$, then $\mathfrak{p}$ splits into $h(K)/f$. In particular, $\mathfrak{p}$ is totally split in H if and only if $\mathfrak{p}$ is principal.*

Recap from Talk 1

Recall the main results from last week:

Theorem

Let K be a number field. Then K has a maximal unramified abelian extensions H, denoted as the **Hilbert class field** *of K. Furthermore,*

- $\mathrm{Gal}(H/K) \cong \mathrm{Cl}(K)$ *and hence* $[H : K] = h(K)$.
- *Splitting Property: If $\mathfrak{p}$ is a prime ideal of K, and f is the order of $[\mathfrak{p}]$ in $\mathrm{Cl}(K)$, then $\mathfrak{p}$ splits into $h(K)/f$. In particular, $\mathfrak{p}$ is totally split in H if and only if $\mathfrak{p}$ is principal.*
- *Capitulation property: Every ideal $\mathfrak{p}$ of K becomes principal in H.*

Recap from Talk 1

Using Galois correspondence and the fact that subfields of abelian unramified extensions are also abelian and unramified, the following correspondence holds.

Corollary

Let K be a number field. Then we have an inclusion-revsersing correspondence

$$\{\textit{Unramified abelian } K \subseteq F\} \longleftrightarrow \{\textit{Subgroups of } \mathrm{Cl}(K)\}$$

Example $K = \mathbb{Q}(\sqrt{-5})$

Hilbert Class Field

In the previous talk, we saw that $\mathbb{Q}(i, \sqrt{5})/\mathbb{Q}(\sqrt{-5})$ is unramified and since $h(K) = 2$, then $H = \mathbb{Q}(i, \sqrt{5})$.

Example $K = \mathbb{Q}(\sqrt{-5})$

Hilbert Class Field

In the previous talk, we saw that $\mathbb{Q}(i, \sqrt{5})/\mathbb{Q}(\sqrt{-5})$ is unramified and since $h(K) = 2$, then $H = \mathbb{Q}(i, \sqrt{5})$.

Capitulation Property

The map $Cl(K) \to Cl(H),\ [\mathfrak{a}] \mapsto [\mathfrak{a}\mathcal{O}_H]$ is a well-defined homomorphism and $\mathfrak{p} = (2, 1 + \sqrt{-5})$ is non-principal, so it is enough to show that $\mathfrak{p}\mathcal{O}_H$ is principal.

Example $K = \mathbb{Q}(\sqrt{-5})$

Hilbert Class Field
In the previous talk, we saw that $\mathbb{Q}(i, \sqrt{5})/\mathbb{Q}(\sqrt{-5})$ is unramified and since $h(K) = 2$, then $H = \mathbb{Q}(i, \sqrt{5})$.

Capitulation Property
The map $Cl(K) \to Cl(H),\ [\mathfrak{a}] \mapsto [\mathfrak{a}\mathcal{O}_H]$ is a well-defined homomorphism and $\mathfrak{p} = (2, 1 + \sqrt{-5})$ is non-principal, so it is enough to show that $\mathfrak{p}\mathcal{O}_H$ is principal.This is true because

$$\frac{2}{1+i} = 1 - i \quad \text{and} \quad \frac{1+\sqrt{-5}}{1+i} = \frac{1+\sqrt{5}}{2} - i\frac{1-\sqrt{5}}{2}$$

are algebraic integers and $N(\mathfrak{p}\mathcal{O}_H) = N((1+i)\mathcal{O}_H) = 4$.

Example $K = \mathbb{Q}(\sqrt{-5})$

Splitting Property: Let $\mathfrak{p}$ be a prime in K, and let $p\mathbb{Z} = \mathfrak{p} \cap \mathbb{Q}$.

Example $K = \mathbb{Q}(\sqrt{-5})$

Splitting Property: Let $\mathfrak{p}$ be a prime in K, and let $p\mathbb{Z} = \mathfrak{p} \cap \mathbb{Q}$.

- If $p = 2$, then $\mathfrak{p} = (2, 1 \pm \sqrt{-5})$ and $\mathfrak{p}\mathcal{O}_H = (1 \mp i)\mathcal{O}_H$ is prime.

Example $K = \mathbb{Q}(\sqrt{-5})$

Splitting Property: Let $\mathfrak{p}$ be a prime in K, and let $p\mathbb{Z} = \mathfrak{p} \cap \mathbb{Q}$.

- If $p = 2$, then $\mathfrak{p} = (2, 1 \pm \sqrt{-5})$ and $\mathfrak{p}\mathcal{O}_H = (1 \mp i)\mathcal{O}_H$ is prime.
- If $p = 5$, then $\mathfrak{p} = (\sqrt{-5})\mathcal{O}_K$ splits in H since 5 splits in $\mathbb{Q}(i)$.

Example $K = \mathbb{Q}(\sqrt{-5})$

Splitting Property: Let $\mathfrak{p}$ be a prime in K, and let $p\mathbb{Z} = \mathfrak{p} \cap \mathbb{Q}$.

- If $p = 2$, then $\mathfrak{p} = (2, 1 \pm \sqrt{-5})$ and $\mathfrak{p}\mathcal{O}_H = (1 \mp i)\mathcal{O}_H$ is prime.
- If $p = 5$, then $\mathfrak{p} = (\sqrt{-5})\mathcal{O}_K$ splits in H since 5 splits in $\mathbb{Q}(i)$.
- If $p \equiv 11, 13, 17, 19 \pmod{20}$, then $\mathfrak{p} = p\mathcal{O}_K$ is principal, and $\mathfrak{p}$ splits in H since p splits in $\mathbb{Q}(i)$ or $\mathbb{Q}(\sqrt{5})$.

Example $K = \mathbb{Q}(\sqrt{-5})$

Splitting Property: Let $\mathfrak{p}$ be a prime in K, and let $p\mathbb{Z} = \mathfrak{p} \cap \mathbb{Q}$.

- If $p = 2$, then $\mathfrak{p} = (2, 1 \pm \sqrt{-5})$ and $\mathfrak{p}\mathcal{O}_H = (1 \mp i)\mathcal{O}_H$ is prime.
- If $p = 5$, then $\mathfrak{p} = (\sqrt{-5})\mathcal{O}_K$ splits in H since 5 splits in $\mathbb{Q}(i)$.
- If $p \equiv 11, 13, 17, 19 \pmod{20}$, then $\mathfrak{p} = p\mathcal{O}_K$ is principal, and $\mathfrak{p}$ splits in H since p splits in $\mathbb{Q}(i)$ or $\mathbb{Q}(\sqrt{5})$.
- If $p \equiv 3, 7 \pmod{20}$, then p is inert in $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{5})$ but split in $\mathbb{Q}(\sqrt{-5})$. Thus $\mathfrak{p}$ is inert in H and non-principal since $x^2 + 5y^2 = p$ has no solutions.

Example $K = \mathbb{Q}(\sqrt{-5})$

Splitting Property: Let $\mathfrak{p}$ be a prime in K, and let $p\mathbb{Z} = \mathfrak{p} \cap \mathbb{Q}$.

- If $p = 2$, then $\mathfrak{p} = (2, 1 \pm \sqrt{-5})$ and $\mathfrak{p}\mathcal{O}_H = (1 \mp i)\mathcal{O}_H$ is prime.
- If $p = 5$, then $\mathfrak{p} = (\sqrt{-5})\mathcal{O}_K$ splits in H since 5 splits in $\mathbb{Q}(i)$.
- If $p \equiv 11, 13, 17, 19 \pmod{20}$, then $\mathfrak{p} = p\mathcal{O}_K$ is principal, and $\mathfrak{p}$ splits in H since p splits in $\mathbb{Q}(i)$ or $\mathbb{Q}(\sqrt{5})$.
- If $p \equiv 3, 7 \pmod{20}$, then p is inert in $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{5})$ but split in $\mathbb{Q}(\sqrt{-5})$. Thus $\mathfrak{p}$ is inert in H and non-principal since $x^2 + 5y^2 = p$ has no solutions.
- If $p \equiv 1, 9 \pmod{20}$, then p is totally split in H.

Example $K = \mathbb{Q}(\sqrt{-5})$

Splitting Property: Let $\mathfrak{p}$ be a prime in K, and let $p\mathbb{Z} = \mathfrak{p} \cap \mathbb{Q}$.

- If $p = 2$, then $\mathfrak{p} = (2, 1 \pm \sqrt{-5})$ and $\mathfrak{p}\mathcal{O}_H = (1 \mp i)\mathcal{O}_H$ is prime.
- If $p = 5$, then $\mathfrak{p} = (\sqrt{-5})\mathcal{O}_K$ splits in H since 5 splits in $\mathbb{Q}(i)$.
- If $p \equiv 11, 13, 17, 19 \pmod{20}$, then $\mathfrak{p} = p\mathcal{O}_K$ is principal, and $\mathfrak{p}$ splits in H since p splits in $\mathbb{Q}(i)$ or $\mathbb{Q}(\sqrt{5})$.
- If $p \equiv 3, 7 \pmod{20}$, then p is inert in $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{5})$ but split in $\mathbb{Q}(\sqrt{-5})$. Thus $\mathfrak{p}$ is inert in H and non-principal since $x^2 + 5y^2 = p$ has no solutions.
- If $p \equiv 1, 9 \pmod{20}$, then p is totally split in H. Hence,

Corollary

The splitting property for K holds if and only if every prime $p \equiv 1, 9 \pmod{20}$ can be written as $p = x^2 + 5y^2$.

Today's Plan

Number Theory Preliminaries

Let L/K be an extension of number fields and let $\mathfrak{p}$ be a prime in K.

Number Theory Preliminaries

Let L/K be an extension of number fields and let $\mathfrak{p}$ be a prime in K. Then we have a decomposition

$$\mathfrak{p}\mathcal{O}_L = \prod_{i=1}^{g} \mathfrak{P}_i^{e_i},$$

where e_i is the ramification index and $f_i = [\mathcal{O}_L/\mathfrak{P}_i : \mathcal{O}_K/\mathfrak{p}]$ is the residue degree.

Number Theory Preliminaries

Let L/K be an extension of number fields and let $\mathfrak{p}$ be a prime in K. Then we have a decomposition

$$\mathfrak{p}\mathcal{O}_L = \prod_{i=1}^{g} \mathfrak{P}_i^{e_i},$$

where e_i is the ramification index and $f_i = [\mathcal{O}_L/\mathfrak{P}_i : \mathcal{O}_K/\mathfrak{p}]$ is the residue degree. We have the fundamental formula

$$[L : K] = \sum_{i=1}^{g} e_i f_i.$$

Number Theory Preliminaries

If L/K is Galois and $G = \mathrm{Gal}(L/K)$, then

$$\mathfrak{p}\mathcal{O}_L = \left(\prod_{i=1}^{g} \mathfrak{P}_i\right)^e$$

and $[L : K] = efg$.

Number Theory Preliminaries

If L/K is Galois and $G = \mathrm{Gal}(L/K)$, then

$$\mathfrak{p}\mathcal{O}_L = \left(\prod_{i=1}^{g} \mathfrak{P}_i\right)^e$$

and $[L:K] = efg$.For any $\mathfrak{P} \mid \mathfrak{p}$, the decomposition group $D_{\mathfrak{P}} = \{\sigma \in G : \sigma(\mathfrak{P}) = \mathfrak{P}\}$ fits in the short exact sequence

$$0 \longrightarrow I_{\mathfrak{P}} \longrightarrow D_{\mathfrak{P}} \xrightarrow{\epsilon} \mathrm{Gal}(\mathcal{O}_L/\mathfrak{P}/\mathcal{O}_K/\mathfrak{p}) \longrightarrow 0.$$

Number Theory Preliminaries

If L/K is Galois and $G = \mathrm{Gal}(L/K)$, then

$$\mathfrak{p}\mathcal{O}_L = \left(\prod_{i=1}^{g} \mathfrak{P}_i\right)^e$$

and $[L:K] = efg$.For any $\mathfrak{P} \mid \mathfrak{p}$, the decomposition group $D_{\mathfrak{P}} = \{\sigma \in G : \sigma(\mathfrak{P}) = \mathfrak{P}\}$ fits in the short exact sequence

$$0 \longrightarrow I_{\mathfrak{P}} \longrightarrow D_{\mathfrak{P}} \xrightarrow{\epsilon} \mathrm{Gal}(\mathcal{O}_L/\mathfrak{P}/\mathcal{O}_K/\mathfrak{p}) \longrightarrow 0.$$

If $I_{\mathfrak{P}} = \{1\} \iff e = 1 \iff \mathfrak{p}$ unramified, then $D_{\mathfrak{P}} \cong \mathrm{Gal}(\mathcal{O}_L/\mathfrak{P}/\mathcal{O}_K/\mathfrak{p})$ and so there is one unique $\sigma_{\mathfrak{P}} \in G$ (denoted the Frobenius element of $\mathfrak{P}$) such that

$$\sigma_{\mathfrak{P}}(x) \equiv x^{N(\mathfrak{p})} \pmod{\mathfrak{P}} \text{ for all } x \in L.$$

Number Theory Preliminaries

If $\mathfrak{P}' \mid \mathfrak{p}$ then $\mathfrak{P}' = \tau(\mathfrak{P})$ for some $\tau \in G$. Then

$$D_{\mathfrak{P}'} = \tau D_{\mathfrak{P}} \tau^{-1} \text{ and } \sigma_{\mathfrak{P}'} = \tau \sigma_{\mathfrak{P}} \tau^{-1}.$$

Number Theory Preliminaries

If $\mathfrak{P}' \mid \mathfrak{p}$ then $\mathfrak{P}' = \tau(\mathfrak{P})$ for some $\tau \in G$. Then

$$D_{\mathfrak{P}'} = \tau D_{\mathfrak{P}} \tau^{-1} \text{ and } \sigma_{\mathfrak{P}'} = \tau \sigma_{\mathfrak{P}} \tau^{-1}.$$

Definition

Suppose L/K is Galois with $G = \mathrm{Gal}(L/K)$ and let $\mathfrak{p} \subset \mathcal{O}_K$ unramified in L. Then the **Artin symbol** of $\mathfrak{p}$ in L

$$\left(\frac{L/K}{\mathfrak{p}}\right) := \{\sigma_{\mathfrak{P}} \in G : \mathfrak{P} \mid \mathfrak{p}\}$$

defines a conjugacy class of G.

Number Theory Preliminaries

If $\mathfrak{P}' \mid \mathfrak{p}$ then $\mathfrak{P}' = \tau(\mathfrak{P})$ for some $\tau \in G$. Then

$$D_{\mathfrak{P}'} = \tau D_{\mathfrak{P}} \tau^{-1} \text{ and } \sigma_{\mathfrak{P}'} = \tau \sigma_{\mathfrak{P}} \tau^{-1}.$$

Definition

Suppose L/K is Galois with $G = \mathrm{Gal}(L/K)$ and let $\mathfrak{p} \subset \mathcal{O}_K$ unramified in L. Then the **Artin symbol** of $\mathfrak{p}$ in L

$$\left(\frac{L/K}{\mathfrak{p}}\right) := \{\sigma_{\mathfrak{P}} \in G : \mathfrak{P} \mid \mathfrak{p}\}$$

defines a conjugacy class of G.

Clearly, if G is abelian, then $((L/K)/\mathfrak{p})$ is an element of G.

Examples

Example

Let $K = \mathbb{Q}$ and $L = \mathbb{Q}(\sqrt{D})$ a quadratic extension. If $p \nmid D$ is an odd rational prime, then

$$\left(\frac{\mathbb{Q}(\sqrt{D})/\mathbb{Q}}{(p)}\right)(a + b\sqrt{D}) = a + \left(\frac{D}{p}\right) b\sqrt{D}.$$

Examples

Example

Let $K = \mathbb{Q}$ and $L = \mathbb{Q}(\sqrt{D})$ a quadratic extension. If $p \nmid D$ is an odd rational prime, then

$$\left(\frac{\mathbb{Q}(\sqrt{D})/\mathbb{Q}}{(p)}\right)(a + b\sqrt{D}) = a + \left(\frac{D}{p}\right) b\sqrt{D}.$$

Example

Let $K = \mathbb{Q}$ and $L = \mathbb{Q}(\zeta_N)$ be the N-th cyclotomic extension. If $p \nmid N$ is a rational prime, then

$$\left(\frac{\mathbb{Q}(\zeta_N)/\mathbb{Q}}{(p)}\right)(\zeta_N) = \zeta_N^p.$$

The Artin Map

Definition (Artin Map)

Let K be a number and let L be an abelian extension. We define $\mathcal{I}_K$ to be the group of fractional ideals of K and $\mathcal{I}_{L/K}$ be the subgroup of $\mathcal{I}_K$ generated by the primes of K unramified in L.

The Artin Map

Definition (Artin Map)

Let K be a number and let L be an abelian extension. We define $\mathcal{I}_K$ to be the group of fractional ideals of K and $\mathcal{I}_{L/K}$ be the subgroup of $\mathcal{I}_K$ generated by the primes of K unramified in L.

If $\mathfrak{a} = \prod \mathfrak{p}_i^{n_i} \in \mathcal{I}_{L/K}$, then $n_i \neq 0 \implies \mathfrak{p}_i$ is unramified.

The Artin Map

Definition (Artin Map)

Let K be a number and let L be an abelian extension. We define $\mathcal{I}_K$ to be the group of fractional ideals of K and $\mathcal{I}_{L/K}$ be the subgroup of $\mathcal{I}_K$ generated by the primes of K unramified in L.

If $\mathfrak{a} = \prod \mathfrak{p}_i^{n_i} \in \mathcal{I}_{L/K}$, then $n_i \neq 0 \implies \mathfrak{p}_i$ is unramified.

Definition

Let L/K be an abelian extension. The **Artin Map** is defined as

$$\left(\frac{L/K}{\cdot}\right) : \mathcal{I}_{L/K} \longrightarrow \mathrm{Gal}(L/K)$$

$$\mathfrak{a} = \prod_{i=1}^{m} \mathfrak{p}_i^{n_i} \longmapsto \prod_{i=1}^{m} \left(\frac{L/K}{\mathfrak{p}_i}\right)^{n_i}.$$

Properties of the Artin Map

The Artin Map satisfies many important properties.

Properties of the Artin Map

The Artin Map satisfies many important properties.

- It is a homomorphism.

Properties of the Artin Map

The Artin Map satisfies many important properties.

- It is a homomorphism.
- It is compatible with restrictions. That is, if $K \subseteq F \subseteq L$ is a tower of abelian extensions, then the diagram

$$\begin{tikzcd} \mathcal{I}_K \arrow[r, "Art_{L/K}"] \arrow[dr, "Art_{F/K}"'] & \mathrm{Gal}(L/K) \arrow[d, "Res_{L/F}"] \\ & \mathrm{Gal}(F/K) \end{tikzcd}$$

  commutes.

Properties of the Artin Map

The Artin Map satisfies many important properties.

- It is a homomorphism.
- It is compatible with restrictions. That is, if $K \subseteq F \subseteq L$ is a tower of abelian extensions, then the diagram

$$\begin{tikzcd} \mathcal{I}_K \arrow[r, "Art_{L/K}"] \arrow[dr, "Art_{F/K}"'] & \mathrm{Gal}(L/K) \arrow[d, "Res_{L/F}"] \\ & \mathrm{Gal}(F/K) \end{tikzcd}$$

commutes.This follows directly from

$$\left(\frac{L/K}{\mathfrak{p}}\right)\Big|_F = \left(\frac{F/K}{\mathfrak{p}}\right).$$

Properties of the Artin Map

The Artin Map satisfies many important properties.

- It is a homomorphism.
- It is compatible with restrictions. That is, if $K \subseteq F \subseteq L$ is a tower of abelian extensions, then the diagram

$$\begin{tikzcd} \mathcal{I}_K \arrow[r, "Art_{L/K}"] \arrow[dr, "Art_{F/K}"'] & \mathrm{Gal}(L/K) \arrow[d, "Res_{L/F}"] \\ & \mathrm{Gal}(F/K) \end{tikzcd}$$

  commutes.This follows directly from

$$\left(\frac{L/K}{\mathfrak{p}}\right)\bigg|_F = \left(\frac{F/K}{\mathfrak{p}}\right).$$

- It is surjective (next slide).

Surjectivity of the Artin Map

Theorem (Chebotarev Density Theorem)

Let L/K be Galois with $G = \mathrm{Gal}(L/K)$. Let $\sigma \in G$ and let C_σ be its conjugacy class.

Surjectivity of the Artin Map

Theorem (Chebotarev Density Theorem)

Let L/K be Galois with $G = \mathrm{Gal}(L/K)$. Let $\sigma \in G$ and let C_σ be its conjugacy class. Then the set

$$\mathcal{S}_\sigma := \left\{ \mathfrak{p} \subset \mathcal{O}_K \middle| \left(\frac{L/K}{\mathfrak{p}}\right) = C_\sigma \right\}$$

has dirichlet Density

$$\delta(S_\sigma) = \frac{|C_\sigma|}{|G|}$$

Surjectivity of the Artin Map

Corollary

Let L/K be an abelian extension. Then the Artin map is a surjective homomorphism.

Surjectivity of the Artin Map

Corollary

Let L/K be an abelian extension. Then the Artin map is a surjective homomorphism.

Proof.

Let $\sigma \in G$ and since $|C_\sigma|/|G| = 1/[L:K] > 0$, there is some $\mathfrak{p} \subset \mathcal{O}_K$ (in fact, infinitely many) such that $((L/K)/\mathfrak{p}) = \sigma$. $\square$

Surjectivity of the Artin Map

Corollary

Let L/K be an abelian extension. Then the Artin map is a surjective homomorphism.

Proof.

Let $\sigma \in G$ and since $|C_\sigma|/|G| = 1/[L:K] > 0$, there is some $\mathfrak{p} \subset \mathcal{O}_K$ (in fact, infinitely many) such that $((L/K)/\mathfrak{p}) = \sigma$. $\square$

Corollary (Dirichlet)

Let N, a be comprime integers. Then $S = \{p : p \equiv a \pmod{N}\}$ has density $\delta(S) = 1/\phi(N)$.

Surjectivity of the Artin Map

Corollary

Let L/K be an abelian extension. Then the Artin map is a surjective homomorphism.

Proof.

Let $\sigma \in G$ and since $|C_\sigma|/|G| = 1/[L:K] > 0$, there is some $\mathfrak{p} \subset \mathcal{O}_K$ (in fact, infinitely many) such that $((L/K)/\mathfrak{p}) = \sigma$. $\square$

Corollary (Dirichlet)

Let N, a be comprime integers. Then $S = \{p : p \equiv a \pmod{N}\}$ has density $\delta(S) = 1/\phi(N)$.

Proof.

Consider $\mathbb{Q}(\zeta_N)/\mathbb{Q}$ with $|\mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})| = \phi(N)$, and note $((L/K)/p)(\zeta_N) = \zeta_N^a$ if and only if $p \in S$. $\square$

For the reminder of the talk, we assume that L/K is unramified at finite primes, so that $\mathcal{I}_{L/K} = \mathcal{I}_K$.

For the reminder of the talk, we assume that L/K is unramified at finite primes, so that $\mathcal{I}_{L/K} = \mathcal{I}_K$. If $L = H$ is the HCF, then we have the following

Hilbert Class Field and the Artin Map

For the reminder of the talk, we assume that L/K is unramified at finite primes, so that $\mathcal{I}_{L/K} = \mathcal{I}_K$. If $L = H$ is the HCF, then we have the following

Theorem (Artin Reciprocity for HCF)

Let H be the HCF of K. The Artin map $((H/K), \cdot) : \mathcal{I}_K \to \mathrm{Gal}(H/K)$ is a surjective homomorphism with kernel $\mathcal{P}_K$, the group of principal fractional ideals.

Hilbert Class Field and the Artin Map

For the reminder of the talk, we assume that L/K is unramified at finite primes, so that $\mathcal{I}_{L/K} = \mathcal{I}_K$. If $L = H$ is the HCF, then we have the following

Theorem (Artin Reciprocity for HCF)

Let H be the HCF of K. The Artin map $((H/K), \cdot) : \mathcal{I}_K \to \mathrm{Gal}(H/K)$ is a surjective homomorphism with kernel $\mathcal{P}_K$, the group of principal fractional ideals. Hence, then Artin map gives an explicit isomorphism $\mathrm{Cl}(K) = \mathcal{I}_K/\mathcal{P}_K \cong \mathrm{Gal}(H/K)$.

For the reminder of the talk, we assume that L/K is unramified at finite primes, so that $\mathcal{I}_{L/K} = \mathcal{I}_K$. If $L = H$ is the HCF, then we have the following

Theorem (Artin Reciprocity for HCF)

Let H be the HCF of K. The Artin map $((H/K), \cdot) : \mathcal{I}_K \to \mathrm{Gal}(H/K)$ is a surjective homomorphism with kernel $\mathcal{P}_K$, the group of principal fractional ideals. Hence, then Artin map gives an explicit isomorphism $\mathrm{Cl}(K) = \mathcal{I}_K/\mathcal{P}_K \cong \mathrm{Gal}(H/K)$.

Example

Let $p \equiv 1 \pmod 4$ be a rational prime. The field extension $\mathbb{Q}(i, \sqrt{-p})/\mathbb{Q}(\sqrt{-p})$ is unramified.

Hilbert Class Field and the Artin Map

For the reminder of the talk, we assume that L/K is unramified at finite primes, so that $\mathcal{I}_{L/K} = \mathcal{I}_K$. If $L = H$ is the HCF, then we have the following

Theorem (Artin Reciprocity for HCF)

Let H be the HCF of K. The Artin map $((H/K), \cdot) : \mathcal{I}_K \to \mathrm{Gal}(H/K)$ is a surjective homomorphism with kernel $\mathcal{P}_K$, the group of principal fractional ideals. Hence, then Artin map gives an explicit isomorphism $\mathrm{Cl}(K) = \mathcal{I}_K/\mathcal{P}_K \cong \mathrm{Gal}(H/K)$.

Example

Let $p \equiv 1 \pmod 4$ be a rational prime. The field extension $\mathbb{Q}(i, \sqrt{-p})/\mathbb{Q}(\sqrt{-p})$ is unramified. Hence the class number of $\mathbb{Q}(\sqrt{-p})$ (which we denote $h(p)$) is even.

Splitting Property in the HCF

Corollary (Splitting Property)

Let $\mathfrak{p}$ be a prime in K and let f be the order of $[\mathfrak{p}]$ in $\mathrm{Cl}(K)$. Then $\mathfrak{p}$ factors into $h(K)/f$ distinct primes in H all of degree f.

Splitting Property in the HCF

Corollary (Splitting Property)

Let $\mathfrak{p}$ be a prime in K and let f be the order of $[\mathfrak{p}]$ in $\mathrm{Cl}(K)$. Then $\mathfrak{p}$ factors into $h(K)/f$ distinct primes in H all of degree f.

Proof.

The order of $[\mathfrak{p}]$ in $\mathrm{Cl}(K)$ equals the order of $((H/K)/\mathfrak{p})$ in $\mathrm{Gal}(H/K)$ and thus also the order of $D_{\mathfrak{p}}$.

Splitting Property in the HCF

Corollary (Splitting Property)

Let $\mathfrak{p}$ be a prime in K and let f be the order of $[\mathfrak{p}]$ in $\mathrm{Cl}(K)$. Then $\mathfrak{p}$ factors into $h(K)/f$ distinct primes in H all of degree f.

Proof.

The order of $[\mathfrak{p}]$ in $\mathrm{Cl}(K)$ equals the order of $((H/K)/\mathfrak{p})$ in $\mathrm{Gal}(H/K)$ and thus also the order of $D_{\mathfrak{p}}$. Hence, if $\mathfrak{P} \mid \mathfrak{p}$, then $f = [\mathcal{O}_H/\mathfrak{P} : \mathcal{O}_K/\mathfrak{p}]$ is the residual degree. $\square$

Splitting Property in the HCF

Corollary (Splitting Property)

Let $\mathfrak{p}$ be a prime in K and let f be the order of $[\mathfrak{p}]$ in $\mathrm{Cl}(K)$. Then $\mathfrak{p}$ factors into $h(K)/f$ distinct primes in H all of degree f.

Proof.

The order of $[\mathfrak{p}]$ in $\mathrm{Cl}(K)$ equals the order of $((H/K)/\mathfrak{p})$ in $\mathrm{Gal}(H/K)$ and thus also the order of $D_{\mathfrak{p}}$. Hence, if $\mathfrak{P} \mid \mathfrak{p}$, then $f = [\mathcal{O}_H/\mathfrak{P} : \mathcal{O}_K/\mathfrak{p}]$ is the residual degree. □

Corollary

Let L/K be an abelian unramified extension and let $\mathfrak{p}$ be a principal prime of K. Then $\mathfrak{p}$ is completely split on L.

Capitulation Property in the HCF

Definition (Transfer Maps)

Let $H \leq G$ be groups with $G = \cup_{i=1}^{n} x_i H$. Fix some $y \in G$ and let $h_{i,y} \in H$ be such that $yx_i = x_j h_{i,y}$ for some j.

Capitulation Property in the HCF

Definition (Transfer Maps)

Let $H \leq G$ be groups with $G = \cup_{i=1}^{n} x_i H$. Fix some $y \in G$ and let $h_{i,y} \in H$ be such that $yx_i = x_j h_{i,y}$ for some j. The tansfer map is defined as

$$\begin{aligned} \mathrm{Ver} : G^{ab} &\longrightarrow H^{ab} \\ y[G,G] &\longmapsto \left(\prod_{i=1}^{n} h_{i,y}\right)[H,H]. \end{aligned}$$

Capitulation Property in the HCF

Definition (Transfer Maps)

Let $H \leq G$ be groups with $G = \cup_{i=1}^{n} x_i H$. Fix some $y \in G$ and let $h_{i,y} \in H$ be such that $yx_i = x_j h_{i,y}$ for some j. The tansfer map is defined as

$$\begin{aligned} \mathrm{Ver} : G^{ab} &\longrightarrow H^{ab} \\ y[G,G] &\longmapsto \left(\prod_{i=1}^{n} h_{i,y} \right) [H,H]. \end{aligned}$$

Theorem

Let $H = [G,G]$ be the commutator subgroup of G. Then $\mathrm{Ver} : G^{ab} \to H^{ab}$ is the trivial homomorphism.

Capitulation Property in the HCF

Theorem (Capitulation Theorem)

Let K be a number field and let H be its HCF. Then any prime $\mathfrak{p}$ in K becomes principal in H.

Capitulation Property in the HCF

Theorem (Capitulation Theorem)

Let K be a number field and let H be its HCF. Then any prime $\mathfrak{p}$ in K becomes principal in H.

Proof.

Let H' be the HCF of H, and H'/K is Galois since H' is intrinsic over K.

Capitulation Property in the HCF

Theorem (Capitulation Theorem)

Let K be a number field and let H be its HCF. Then any prime $\mathfrak{p}$ in K becomes principal in H.

Proof.

Let H' be the HCF of H, and H'/K is Galois since H' is intrinsic over K. By definition, $\mathrm{Gal}(H/K)$ is the largest abelian quotient of $\mathrm{Gal}(H'/K)$, so $\mathrm{Gal}(H/K) = \mathrm{Gal}(H'/K)^{ab}$ and $\mathrm{Gal}(H'/H)$ is its commutator subgroup.

Capitulation Property in the HCF

Theorem (Capitulation Theorem)

Let K be a number field and let H be its HCF. Then any prime $\mathfrak{p}$ in K becomes principal in H.

Proof.

Let H' be the HCF of H, and H'/K is Galois since H' is intrinsic over K. By definition, $\mathrm{Gal}(H/K)$ is the largest abelian quotient of $\mathrm{Gal}(H'/K)$, so $\mathrm{Gal}(H/K) = \mathrm{Gal}(H'/K)^{ab}$ and $\mathrm{Gal}(H'/H)$ is its commutator subgroup. We have a commutative diagram

$$\begin{tikzcd}
\mathcal{I}_K \arrow[r, "Art_{H/K}"] \arrow[d] & \mathrm{Gal}(H/K) = \mathrm{Gal}(H'/K)^{ab} \arrow[d, "Ver"] \\
\mathcal{I}_H \arrow[r, "Art_{H'/H}"] & \mathrm{Gal}(H'/H) = \mathrm{Gal}(H'/H)^{ab}
\end{tikzcd}$$

□

Quadratic Subfields of Cyclotomic Extensions

Lemma

Let p be an odd prime and let $p^* = (-1)^{(p-1)/2}p$.

Quadratic Subfields of Cyclotomic Extensions

Lemma

Let p be an odd prime and let $p^* = (-1)^{(p-1)/2}p$. Then

- $\mathbb{Q}(\sqrt{p^*})$ *is the unique quadratic subfield of* $\mathbb{Q}(\zeta_p)$*.*

Quadratic Subfields of Cyclotomic Extensions

Lemma

Let p be an odd prime and let $p^* = (-1)^{(p-1)/2}p$. Then

- $\mathbb{Q}(\sqrt{p^*})$ *is the unique quadratic subfield of* $\mathbb{Q}(\zeta_p)$.
- $\mathbb{Q}(i), \mathbb{Q}(\sqrt{\pm p})$ *are the unique quadratic subfields of* $\mathbb{Q}(\zeta_{4p})$.

Proof.

The number of quadratic subfields is determined by Galois correspondence.

Quadratic Subfields of Cyclotomic Extensions

Lemma

Let p be an odd prime and let $p^* = (-1)^{(p-1)/2}p$. Then

- $\mathbb{Q}(\sqrt{p^*})$ *is the unique quadratic subfield of* $\mathbb{Q}(\zeta_p)$.
- $\mathbb{Q}(i), \mathbb{Q}(\sqrt{\pm p})$ *are the unique quadratic subfields of* $\mathbb{Q}(\zeta_{4p})$.

Proof.

The number of quadratic subfields is determined by Galois correspondence. Also, p is the only prime that ramifies in $\mathbb{Q}(\zeta_p)$, and the only quadratic subfield unramified outside p is $\mathbb{Q}(\sqrt{p^*})$.

Quadratic Subfields of Cyclotomic Extensions

Lemma

Let p be an odd prime and let $p^* = (-1)^{(p-1)/2}p$. Then

- $\mathbb{Q}(\sqrt{p^*})$ *is the unique quadratic subfield of* $\mathbb{Q}(\zeta_p)$.
- $\mathbb{Q}(i), \mathbb{Q}(\sqrt{\pm p})$ *are the unique quadratic subfields of* $\mathbb{Q}(\zeta_{4p})$.

Proof.

The number of quadratic subfields is determined by Galois correspondence. Also, p is the only prime that ramifies in $\mathbb{Q}(\zeta_p)$, and the only quadratic subfield unramified outside p is $\mathbb{Q}(\sqrt{p^*})$. The second part is similar with ramification at 2 and p. $\square$

Quadratic Subfields of Cyclotomic Extensions

Lemma

Let p be an odd prime and let $p^* = (-1)^{(p-1)/2}p$. Then

- $\mathbb{Q}(\sqrt{p^*})$ *is the unique quadratic subfield of* $\mathbb{Q}(\zeta_p)$.
- $\mathbb{Q}(i), \mathbb{Q}(\sqrt{\pm p})$ *are the unique quadratic subfields of* $\mathbb{Q}(\zeta_{4p})$.

Proof.

The number of quadratic subfields is determined by Galois correspondence. Also, p is the only prime that ramifies in $\mathbb{Q}(\zeta_p)$, and the only quadratic subfield unramified outside p is $\mathbb{Q}(\sqrt{p^*})$. The second part is similar with ramification at 2 and p. □

Also, using Gauss sums, one can explicitly compute that

$$p^* = \left(\sum_{a=1}^{p-1} \left(\frac{a}{p} \right) \zeta_p^a \right)^2 .$$

Example $\mathbb{Q}(\sqrt{-5})$ revisited

Let $\mathfrak{p}$ be a prime in K not above 2 or 5 and let $H = \mathbb{Q}(i, \sqrt{5})$ be its HCF.

Example $\mathbb{Q}(\sqrt{-5})$ revisited

Let $\mathfrak{p}$ be a prime in K not above 2 or 5 and let $H = \mathbb{Q}(i, \sqrt{5})$ be its HCF. Then by Artin Reciprocity

$$\mathfrak{p} \text{ is principal} \iff \mathfrak{p}\mathcal{O}_H \text{ splits} \iff \left(\frac{H/K}{\mathfrak{p}}\right) = \mathrm{Id}_H.$$

Example $\mathbb{Q}(\sqrt{-5})$ revisited

Let $\mathfrak{p}$ be a prime in K not above 2 or 5 and let $H = \mathbb{Q}(i, \sqrt{5})$ be its HCF. Then by Artin Reciprocity

$$\mathfrak{p} \text{ is principal} \iff \mathfrak{p}\mathcal{O}_H \text{ splits} \iff \left(\frac{H/K}{\mathfrak{p}}\right) = \mathrm{Id}_H.$$

Since $\mathbb{Q}(i, \sqrt{5}) \subset L := \mathbb{Q}(\zeta_{20})$, we have $((L/K)/\mathfrak{p})(\zeta_{20}) = \zeta_{20}^{N(\mathfrak{p})}$ and

$$\left(\frac{H/K}{\mathfrak{p}}\right) = \left(\frac{L/K}{\mathfrak{p}}\right)\Big|_H,$$

Example $\mathbb{Q}(\sqrt{-5})$ revisited

Let $\mathfrak{p}$ be a prime in K not above 2 or 5 and let $H = \mathbb{Q}(i, \sqrt{5})$ be its HCF. Then by Artin Reciprocity

$$\mathfrak{p} \text{ is principal } \iff \mathfrak{p}\mathcal{O}_H \text{ splits } \iff \left(\frac{H/K}{\mathfrak{p}}\right) = \mathrm{Id}_H.$$

Since $\mathbb{Q}(i, \sqrt{5}) \subset L := \mathbb{Q}(\zeta_{20})$, we have $((L/K)/\mathfrak{p})(\zeta_{20}) = \zeta_{20}^{N(\mathfrak{p})}$ and

$$\left(\frac{H/K}{\mathfrak{p}}\right) = \left(\frac{L/K}{\mathfrak{p}}\right)\Big|_H,$$

so $\mathfrak{p}$ being principal depends only on $N(\mathfrak{p}) \pmod{20}$.

Example $\mathbb{Q}(\sqrt{-5})$ revisited

We can compute the behaviour explicitly. Note that

$$i = \zeta_{20}^5 \text{ and } \sqrt{-5} = \zeta_{20} + \zeta_{20}^3 + \zeta_{20}^7 + \zeta_{20}^9,$$

Example $\mathbb{Q}(\sqrt{-5})$ revisited

We can compute the behaviour explicitly. Note that

$$i = \zeta_{20}^5 \text{ and } \sqrt{-5} = \zeta_{20} + \zeta_{20}^3 + \zeta_{20}^7 + \zeta_{20}^9,$$

and hence, for $a \in (\mathbb{Z}/20\mathbb{Z})^*$, the map $\sigma_a : \zeta_{20} \mapsto \zeta_{20}^a$ fixes i if $a = 1, 9, 13, 17$ and fixes $\sqrt{-5}$ if $a = 1, 3, 7, 9$.

Example $\mathbb{Q}(\sqrt{-5})$ revisited

We can compute the behaviour explicitly. Note that

$$i = \zeta_{20}^5 \text{ and } \sqrt{-5} = \zeta_{20} + \zeta_{20}^3 + \zeta_{20}^7 + \zeta_{20}^9,$$

and hence, for $a \in (\mathbb{Z}/20\mathbb{Z})^*$, the map $\sigma_a : \zeta_{20} \mapsto \zeta_{20}^a$ fixes i if $a = 1, 9, 13, 17$ and fixes $\sqrt{-5}$ if $a = 1, 3, 7, 9$. Hence,

$$\mathfrak{p} \text{ is principal} \iff N(\mathfrak{p}) \equiv 1, 9 \pmod{20}.$$

Example $\mathbb{Q}(\sqrt{-5})$ revisited

We can compute the behaviour explicitly. Note that

$$i = \zeta_{20}^5 \text{ and } \sqrt{-5} = \zeta_{20} + \zeta_{20}^3 + \zeta_{20}^7 + \zeta_{20}^9,$$

and hence, for $a \in (\mathbb{Z}/20\mathbb{Z})^*$, the map $\sigma_a : \zeta_{20} \mapsto \zeta_{20}^a$ fixes i if $a = 1, 9, 13, 17$ and fixes $\sqrt{-5}$ if $a = 1, 3, 7, 9$. Hence,

$$\mathfrak{p} \text{ is principal} \iff N(\mathfrak{p}) \equiv 1, 9 \pmod{20}.$$

If $p\mathbb{Z} = \mathfrak{p} \cap \mathbb{Q}$ then $N(\mathfrak{p}) \equiv 1, 9 \pmod{20}$ if and only if $p \equiv 1, 9, 11, 13, 17, 19 \pmod{20}$.

Example $\mathbb{Q}(\sqrt{-5})$ revisited

We can compute the behaviour explicitly. Note that

$$i = \zeta_{20}^5 \text{ and } \sqrt{-5} = \zeta_{20} + \zeta_{20}^3 + \zeta_{20}^7 + \zeta_{20}^9,$$

and hence, for $a \in (\mathbb{Z}/20\mathbb{Z})^*$, the map $\sigma_a : \zeta_{20} \mapsto \zeta_{20}^a$ fixes i if $a = 1, 9, 13, 17$ and fixes $\sqrt{-5}$ if $a = 1, 3, 7, 9$. Hence,

$$\mathfrak{p} \text{ is principal} \iff N(\mathfrak{p}) \equiv 1, 9 \pmod{20}.$$

If $p\mathbb{Z} = \mathfrak{p} \cap \mathbb{Q}$ then $N(\mathfrak{p}) \equiv 1, 9 \pmod{20}$ if and only if $p \equiv 1, 9, 11, 13, 17, 19 \pmod{20}$.

Hence, if $p \equiv 1, 9 \pmod{20}$, then $N(\mathfrak{p}) = p$ and $\mathfrak{p}$ is principal, so we have shown

$$p = x^2 + 5y^2 \iff p \equiv 1, 9 \pmod{20}.$$

Example $K = \mathbb{Q}(\sqrt{-23})$

If $K = \mathbb{Q}(\sqrt{-23})$, then $\mathrm{Cl}(K) = C_3$ and H is the splitting field of the polynomial $x^3 - x + 1$ over $\mathbb{Q}$ (with discriminant -23, so $K \subset H$).

Example $K = \mathbb{Q}(\sqrt{-23})$

If $K = \mathbb{Q}(\sqrt{-23})$, then $\mathrm{Cl}(K) = C_3$ and H is the splitting field of the polynomial $x^3 - x + 1$ over $\mathbb{Q}$ (with discriminant -23, so $K \subset H$).

Let $\mathfrak{p}$ be a prime in K not above 2 and let $p\mathbb{Z} = \mathfrak{p} \cap \mathbb{Q}$. If $(-23/p) = (p/23) = -1$, then $\mathfrak{p} = p\mathcal{O}_K$ and $\mathfrak{p}$ is split in H.

Example $K = \mathbb{Q}(\sqrt{-23})$

If $K = \mathbb{Q}(\sqrt{-23})$, then $\mathrm{Cl}(K) = C_3$ and H is the splitting field of the polynomial $x^3 - x + 1$ over $\mathbb{Q}$ (with discriminant -23, so $K \subset H$).

Let $\mathfrak{p}$ be a prime in K not above 2 and let $p\mathbb{Z} = \mathfrak{p} \cap \mathbb{Q}$. If $(-23/p) = (p/23) = -1$, then $\mathfrak{p} = p\mathcal{O}_K$ and $\mathfrak{p}$ is split in H.

$$
\begin{tikzcd}
 & K(\alpha) \arrow[dl, dash, "3"'] \arrow[dd, dash, "S_3"'] \arrow[dr, dash, "2"] & \\
K \arrow[dr, dash, "2"'] & & \mathbb{Q}(\alpha) \arrow[dl, dash] \\
 & \mathbb{Q} &
\end{tikzcd}
$$

Example $K = \mathbb{Q}(\sqrt{-23})$

Let's assume $(p/23) = 1$, so $N(\mathfrak{p}) = p$.

Example $K = \mathbb{Q}(\sqrt{-23})$

Let's assume $(p/23) = 1$, so $N(\mathfrak{p}) = p$. Then

$$\mathfrak{p} \text{ split in } H \iff p \text{ totally split in } H \iff$$
$$x^3 - x + 1 \pmod{p} \text{ has 3 distinct roots} \iff$$
$$x^3 - x + 1 = 0 \pmod{p} \text{ has a solution.}$$

Example $K = \mathbb{Q}(\sqrt{-23})$

Let's assume $(p/23) = 1$, so $N(\mathfrak{p}) = p$. Then

$$\mathfrak{p} \text{ split in } H \iff p \text{ totally split in } H \iff$$
$$x^3 - x + 1 \pmod{p} \text{ has 3 distinct roots} \iff$$
$$x^3 - x + 1 = 0 \pmod{p} \text{ has a solution.}$$

Putting everything together,

$$p = x^2 + xy + 6y^2 \iff \mathfrak{p} \text{ is principal} \iff$$
$$(p/23) = 1 \text{ and } x^3 - x + 1 = 0 \text{ has a solution mod } p.$$

Example $K = \mathbb{Q}(\sqrt{-23})$

Let's assume $(p/23) = 1$, so $N(\mathfrak{p}) = p$. Then

$$\mathfrak{p} \text{ split in } H \iff p \text{ totally split in } H \iff$$
$$x^3 - x + 1 \pmod{p} \text{ has 3 distinct roots } \iff$$
$$x^3 - x + 1 = 0 \pmod{p} \text{ has a solution.}$$

Putting everything together,

$$p = x^2 + xy + 6y^2 \iff \mathfrak{p} \text{ is principal } \iff$$
$$(p/23) = 1 \text{ and } x^3 - x + 1 = 0 \text{ has a solution mod } p.$$

Finally,

$$p = x^2 + xy + 6y^2 \iff p = a^2 + 23b^2$$

since y must be even and $x^2 + xy + 6y^2 = (x + y/2)^2 + 23(y/2)^2$.

Primes of the form $x^2 + ny^2$

Following a similar reasoning to the previous example, one can prove the following.

Primes of the form $x^2 + ny^2$

Following a similar reasoning to the previous example, one can prove the following.

Theorem

Let $n > 0$ be a squarefree positive integer such that $n \not\equiv 3 \pmod 4$.

Primes of the form $x^2 + ny^2$

Following a similar reasoning to the previous example, one can prove the following.

Theorem

Let $n > 0$ be a squarefree positive integer such that $n \not\equiv 3 \pmod 4$. Then there is a monic irreducible polynomial $f_n(x) \in \mathbb{Z}[x]$ such that if an odd prime p does not divide n or the discriminant of $f_n(x)$, then

$$p = x^2 + ny^2 \iff \begin{cases} (-n/p) = 1 \text{ and } f_n(x) \equiv 0 \pmod p \\ \text{has an integer solution.} \end{cases}$$

Primes of the form $x^2 + ny^2$

Following a similar reasoning to the previous example, one can prove the following.

Theorem

Let $n > 0$ be a squarefree positive integer such that $n \not\equiv 3 \pmod 4$. Then there is a monic irreducible polynomial $f_n(x) \in \mathbb{Z}[x]$ such that if an odd prime p does not divide n or the discriminant of $f_n(x)$, then

$$p = x^2 + ny^2 \iff \begin{cases} (-n/p) = 1 \text{ and } f_n(x) \equiv 0 \pmod p \\ \text{has an integer solution.} \end{cases}$$

Furthermore, $f_n(x)$ can be taken to be the minimal polynomial of a real algebraic integer α for which $H = K(\alpha)$ is the Hilbert class field of $K = \mathbb{Q}(\sqrt{-n})$.

Class numbers of $\mathbb{Q}(\sqrt{\pm p})$

Given n squarefree, let $h(n)$ be the class number of $\mathbb{Q}(\sqrt{n})$.

Class numbers of $\mathbb{Q}(\sqrt{\pm p})$

Given n squarefree, let $h(n)$ be the class number of $\mathbb{Q}(\sqrt{n})$.

Let p be a rational prime. We have seen that if $p \equiv 1 \pmod 4$, then $h(-p)$ is even.

Class numbers of $\mathbb{Q}(\sqrt{\pm p})$

Given n squarefree, let $h(n)$ be the class number of $\mathbb{Q}(\sqrt{n})$.

Let p be a rational prime. We have seen that if $p \equiv 1 \pmod 4$, then $h(-p)$ is even.

Theorem

Let p be a rational prime. Then $h(p)$ is always odd and $h(-p)$ is even if and only if $p \equiv 1 \pmod 4$.

Class numbers of $\mathbb{Q}(\sqrt{\pm p})$

Proof sketch for $h(p^*)$.

Suppose that $h(p^*)$ is even and let H be the HCF of $K = \mathbb{Q}(\sqrt{p^*})$. Let $G = \mathrm{Gal}(H/\mathbb{Q})$ and $A = \mathrm{Gal}(H/K)$.

Class numbers of $\mathbb{Q}(\sqrt{\pm p})$

Proof sketch for $h(p^*)$.

Suppose that $h(p^*)$ is even and let H be the HCF of $K = \mathbb{Q}(\sqrt{p^*})$. Let $G = \mathrm{Gal}(H/\mathbb{Q})$ and $A = \mathrm{Gal}(H/K)$. Let L be a fixed field by a Sylow 2-subgroup P of A. Since $P \trianglelefteq G$, L is Galois over $\mathbb{Q}$.

Class numbers of $\mathbb{Q}(\sqrt{\pm p})$

Proof sketch for $h(p^*)$.

Suppose that $h(p^*)$ is even and let H be the HCF of $K = \mathbb{Q}(\sqrt{p^*})$. Let $G = \mathrm{Gal}(H/\mathbb{Q})$ and $A = \mathrm{Gal}(H/K)$. Let L be a fixed field by a Sylow 2-subgroup P of A. Since $P \trianglelefteq G$, L is Galois over $\mathbb{Q}$.

One can prove that $\mathrm{Gal}(L/\mathbb{Q})$ has a C_4 or $C_2 \times C_2$ quotient, and there is $K \subseteq F \subseteq L$ such that $\mathrm{Gal}(F/\mathbb{Q}) \cong C_4$ or $C_2 \times C_2$.

Class numbers of $\mathbb{Q}(\sqrt{\pm p})$

Proof sketch for $h(p^*)$.

Suppose that $h(p^*)$ is even and let H be the HCF of $K = \mathbb{Q}(\sqrt{p^*})$. Let $G = \mathrm{Gal}(H/\mathbb{Q})$ and $A = \mathrm{Gal}(H/K)$. Let L be a fixed field by a Sylow 2-subgroup P of A. Since $P \trianglelefteq G$, L is Galois over $\mathbb{Q}$.

One can prove that $\mathrm{Gal}(L/\mathbb{Q})$ has a C_4 or $C_2 \times C_2$ quotient, and there is $K \subseteq F \subseteq L$ such that $\mathrm{Gal}(F/\mathbb{Q}) \cong C_4$ or $C_2 \times C_2$.

So there is a tower $\mathbb{Q} \subset K \subset F$ where p ramifies in $K/\mathbb{Q}$ and F/K is unramified.

Proof sketch for $h(p^*)$.

Suppose that $h(p^*)$ is even and let H be the HCF of $K = \mathbb{Q}(\sqrt{p^*})$. Let $G = \mathrm{Gal}(H/\mathbb{Q})$ and $A = \mathrm{Gal}(H/K)$. Let L be a fixed field by a Sylow 2-subgroup P of A. Since $P \trianglelefteq G$, L is Galois over $\mathbb{Q}$.

One can prove that $\mathrm{Gal}(L/\mathbb{Q})$ has a C_4 or $C_2 \times C_2$ quotient, and there is $K \subseteq F \subseteq L$ such that $\mathrm{Gal}(F/\mathbb{Q}) \cong C_4$ or $C_2 \times C_2$.

So there is a tower $\mathbb{Q} \subset K \subset F$ where p ramifies in $K/\mathbb{Q}$ and F/K is unramified. Hence, $\mathrm{Gal}(F/\mathbb{Q}) = C_4$ is impossible and if $\mathrm{Gal}(F/\mathbb{Q}) = C_2 \times C_2$, then F^{I_p} is a quadratic unramified extension of $\mathbb{Q}$, a contradiction. $\square$

Ramification at Infinite Places

Theorem (Artin Reciprocity for infinite primes)

Let K be a number field and let S be a subset of the set of real infinite places of K.

Ramification at Infinite Places

Theorem (Artin Reciprocity for infinite primes)

Let K be a number field and let $\mathcal{S}$ be a subset of the set of real infinite places of K. Then there is a maximal abelian extension $H_{\mathcal{S}}$ of K unramified at all finite primes and infinite primes outside $\mathcal{S}$.

Ramification at Infinite Places

Theorem (Artin Reciprocity for infinite primes)

Let K be a number field and let $\mathcal{S}$ be a subset of the set of real infinite places of K. Then there is a maximal abelian extension $H_{\mathcal{S}}$ of K unramified at all finite primes and infinite primes outside $\mathcal{S}$. Furthermore, the Artin map

$$\left(\frac{H_{\mathcal{S}}/K}{\cdot}\right) : \mathcal{I}_K \longrightarrow \mathrm{Gal}(H_{\mathcal{S}}/K)$$

is surjective with kernel $\mathcal{P}_{K,\mathcal{S}}$, the principal ideals generated by some α such that $\sigma(\alpha) > 0$ for all $\sigma \in \mathcal{S}$.

Narrow Class Group

Definition (Narrow class group)

If $\mathcal{S}$ contains all real infinite places, then $H^+ := H_{\mathcal{S}}$ is denoted the **extended Hilbert class field**.

Narrow Class Group

Definition (Narrow class group)

If $\mathcal{S}$ contains all real infinite places, then $H^+ := H_{\mathcal{S}}$ is denoted the **extended Hilbert class field**. Furthermore, $\mathcal{P}_K^+ := \mathcal{P}_{K,\mathcal{S}}$ is the group of **totally positive principal fractional ideals** of K

Narrow Class Group

Definition (Narrow class group)

If $\mathcal{S}$ contains all real infinite places, then $H^+ := H_{\mathcal{S}}$ is denoted the **extended Hilbert class field**. Furthermore, $\mathcal{P}_K^+ := \mathcal{P}_{K,\mathcal{S}}$ is the group of **totally positive principal fractional ideals** of K and $\mathrm{Cl}^+(K) = \mathcal{I}_K/\mathcal{P}_K^+$ is the **narrow class group** of K.

Narrow Class Group

Definition (Narrow class group)

If $\mathcal{S}$ contains all real infinite places, then $H^+ := H_\mathcal{S}$ is denoted the **extended Hilbert class field**. Furthermore, $\mathcal{P}_K^+ := \mathcal{P}_{K,\mathcal{S}}$ is the group of **totally positive principal fractional ideals** of K and $\mathrm{Cl}^+(K) = \mathcal{I}_K/\mathcal{P}_K^+$ is the **narrow class group** of K.

Lemma

Let r_2 be the number of real infinite places. Then $(\mathbb{Z}/2\mathbb{Z})^{r_2}$ surjects onto the kernel of the quotient map $\mathrm{Cl}^+(K) \to \mathrm{Cl}(K)$.

Narrow Class Group

Definition (Narrow class group)

If $\mathcal{S}$ contains all real infinite places, then $H^+ := H_{\mathcal{S}}$ is denoted the **extended Hilbert class field**. Furthermore, $\mathcal{P}_K^+ := \mathcal{P}_{K,\mathcal{S}}$ is the group of **totally positive principal fractional ideals** of K and $\mathrm{Cl}^+(K) = \mathcal{I}_K/\mathcal{P}_K^+$ is the **narrow class group** of K.

Lemma

Let r_2 be the number of real infinite places. Then $(\mathbb{Z}/2\mathbb{Z})^{r_2}$ surjects onto the kernel of the quotient map $\mathrm{Cl}^+(K) \to \mathrm{Cl}(K)$. Hence, $[H^+ : H] \mid 2^{r_2}$.

Extended HCF of Imaginary Quadratic Fields

Let D be a squarefree integer and let $K = \mathbb{Q}(\sqrt{D})$. If $D < 0$ then K has no real places, so $H^+ = H$.

Extended HCF of Imaginary Quadratic Fields

Let D be a squarefree integer and let $K = \mathbb{Q}(\sqrt{D})$. If $D < 0$ then K has no real places, so $H^+ = H$.

Theorem

If $D > 0$, let ϵ be a fundamental unit of K. Then $[H^+ : H] = 1$ or 2 according as $N_{K/\mathbb{Q}}(\epsilon) = -1$ or 1.

Extended HCF of Imaginary Quadratic Fields

Let D be a squarefree integer and let $K = \mathbb{Q}(\sqrt{D})$. If $D < 0$ then K has no real places, so $H^+ = H$.

Theorem

If $D > 0$, let ϵ be a fundamental unit of K. Then $[H^+ : H] = 1$ or 2 according as $N_{K/\mathbb{Q}}(\epsilon) = -1$ or 1.

Lemma

Let $D > 0$ be a squarefree integer. Then -1 is the norm of an **element** *of K^+ if and only if every odd prime divisor of D is congruent to $1 \pmod 4$.*

Extended HCF of Imaginary Quadratic Fields

Let D be a squarefree integer and let $K = \mathbb{Q}(\sqrt{D})$. If $D < 0$ then K has no real places, so $H^+ = H$.

Theorem

If $D > 0$, let ϵ be a fundamental unit of K. Then $[H^+ : H] = 1$ or 2 according as $N_{K/\mathbb{Q}}(\epsilon) = -1$ or 1.

Lemma

Let $D > 0$ be a squarefree integer. Then -1 is the norm of an **element** *of K^+ if and only if every odd prime divisor of D is congruent to $1 \pmod 4$.*

Corollary

If $D = p \equiv 3 \pmod 4$ is a rational prime, then $[H^+ : H] = 2$.

Extended HCF of Imaginary Quadratic Fields

Proposition

Let $D = p \equiv 1 \pmod 4$ be a rational prime. Then $H^+ = H$ and therefore $N_{K/\mathbb{Q}}(\epsilon) = -1$.

Extended HCF of Imaginary Quadratic Fields

Proposition

Let $D = p \equiv 1 \pmod 4$ be a rational prime. Then $H^+ = H$ and therefore $N_{K/\mathbb{Q}}(\epsilon) = -1$.

Proof.

The same proof we did to show that $h(p)$ is odd works to show that $[H^+ : K]$ is odd. So $[H^+ : H] = 1$. $\square$

However, it is **not true** that if D is only divisible by primes $p \equiv 1 \pmod 4$ then the fundamental unit is negative.

However, it is **not true** that if D is only divisible by primes $p \equiv 1 \pmod 4$ then the fundamental unit is negative.

Final fun fact!

However, it is **not true** that if D is only divisible by primes $p \equiv 1 \pmod 4$ then the fundamental unit is negative.

Final fun fact!

Theorem (Maybe)

Let $D(X)$ be the number of real quadratic fields whose discriminant $\Delta < X$ is not divisible by a prime congruent to 3 mod 4 *and $D^{-}(X)$ is those who have a negative unit. Then*

$$\lim_{X \to \infty} \frac{D^{-}(X)}{D(X)} = 1 - \prod_{j \geq 1 \text{ odd}} (1 - 2^{-j})$$

Thank you for listening!