Ray class fields

Edwina Aylward

May 23, 2024

Recap of last week

Let L/K be a Galois extension. Let $\mathfrak{P}$ be an unramified prime of L lying over a prime $\mathfrak{p}$ of K. Last week Albert defined the **Artin symbol**

$$\left(\frac{L/K}{\mathfrak{P}}\right) \in \mathrm{Gal}(L/K)$$

which is the unique element that maps mod $\mathfrak{P}$ to the Frobenius element of $\mathrm{Gal}(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}})$.

When L/K is abelian, $\left(\frac{L/K}{\mathfrak{P}}\right)$ depends only on $\mathfrak{p}$ $\rightsquigarrow$ write $\left(\frac{L/K}{\mathfrak{p}}\right)$.

For L/K abelian and unramified, one defines the **Artin map**

$$\left(\frac{L/K}{\cdot}\right) : I_K \to \mathrm{Gal}(L/K), \quad \mathfrak{a} = \prod_i \mathfrak{p}^{r_i} \mapsto \prod_i \left(\frac{L/K}{\mathfrak{p}}\right)^{r_i}.$$

Artin reciprocity: If L is the Hilbert class field of K, then the Artin map induces an isomorphism

$$\mathrm{Cl}(K) = I_K/P_K \simeq \mathrm{Gal}(L/K).$$

Modulus

From now on assume L/K is abelian. The Artin symbol is still well-defined away from the ramified primes of L/K, so one can define an Artin map for L/K on a subgroup of I_K.

Definition

Let K be a number field.

1. A modulus $\mathfrak{m}$ for K is a pair $(\mathfrak{m}_0, \mathfrak{m}_\infty)$ where $\mathfrak{m}_0$ is an integral ideal of K and $\mathfrak{m}_\infty$ is a subset of the real embeddings of K. Formally, one writes $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$.
2. Let $I_K(\mathfrak{m})$ denote the group of all fractional $\mathcal{O}_K$-ideals relatively prime to $\mathfrak{m}_0$.

Elements of $I_K(\mathfrak{m})$ are of the form $\mathfrak{a}/\mathfrak{b}$ where $\mathfrak{a}$, $\mathfrak{b}$ are coprime integral ideals in K that are coprime to $\mathfrak{m}_0$.

Artin map for abelian extensions

Definition

If L/K is an abelian extension, $\mathfrak{m}$ a modulus for K divisible by all primes that ramify in L, then one has a well-defined Artin map

$$\Phi_{\mathfrak{m}}\colon \left(\frac{L/K}{\cdot}\right) : I_K(\mathfrak{m}) \to \mathrm{Gal}(L/K)$$

defined as before by extending the Artin symbol multiplicatively.

Example

Let $L = \mathbb{Q}(\zeta_m)$, $K = \mathbb{Q}$. Then $\mathfrak{m} = (m)\infty$ is divisible by all ramified primes of L/K. Thus we have $\Phi_{\mathfrak{m}}\colon I_{\mathbb{Q}}(\mathfrak{m}) \to \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \simeq (\mathbb{Z}/m\mathbb{Z})^\times$ where for $\frac{a}{b}\mathbb{Z} \in I_{\mathbb{Q}}(m)$ with $\frac{a}{b} > 0$ one has

$$\Phi_{\mathfrak{m}}(\frac{a}{b}\mathbb{Z}) = [a][b]^{-1} \in (\mathbb{Z}/m\mathbb{Z})^\times.$$

This is surjective.

CFT for abelian extensions

We saw that unramified extensions of K gave Galois groups isomorphic to subgroups of $\mathrm{Cl}(K)$.
Next, we define generalized ideal class groups, which we will see to be the Galois groups of all abelian extensions of K.

Ray class groups

Definition (Ray group)

Given a modulus $\mathfrak{m}$ of K, let $P_K(\mathfrak{m})$ be the subgroup of $I_K(\mathfrak{m})$ consisting of all principal fractional ideals (α) where $\alpha \in K^\times$ satisfies

1. $v_\mathfrak{p}(\alpha - 1) \geq v_\mathfrak{p}(\mathfrak{m}_0)$ for each finite prime $\mathfrak{p}$,
2. $\sigma(\alpha) > 0$ for every real infinite prime $\sigma \mid \mathfrak{m}$.

Example

Let $K = \mathbb{Q}$ and $\mathfrak{m} = (m),\ m \in \mathbb{N}$. Consider $\frac{a}{b}\mathbb{Z} \in I_\mathbb{Q}(\mathfrak{m})$. For $p^k \mid m$,

$$v_p(\frac{a}{b} - 1) = v_p(a - b) + v_p(b) \geq k \implies a \equiv b \mod p^k.$$

Thus

$$P_\mathbb{Q}(\mathfrak{m}) = \{\frac{a}{b}\mathbb{Z} \in I_\mathbb{Q}(\mathfrak{m}) \mid a \equiv b \bmod m\}.$$

If $\mathfrak{m}' = (m)\infty$, then $P_\mathbb{Q}(\mathfrak{m}') = \{\frac{a}{b}\mathbb{Z} \in I_\mathbb{Q}(\mathfrak{m}') \mid a \equiv b \bmod m,\ a/b > 0\}$.

Generalised ideal class group

Definition (Congruence subgroup)

A subgroup $H \subset I_K(\mathfrak{m})$ is a congruence subgroup for $\mathfrak{m}$ if it satisfies

$$P_K(\mathfrak{m}) \subset H \subset I_K(\mathfrak{m}).$$

Definition (Generalised ideal class group)

Let H be a congruence subgroup, then the quotient

$$I_K(\mathfrak{m})/H$$

is a generalised ideal class group for $\mathfrak{m}$.

Definition (Ray class group)

If $H = P_K(\mathfrak{m})$, then $I_K(\mathfrak{m})/P_K(\mathfrak{m})$ is known as the ray class group.

Takagi Existence theorem

Theorem (Existence theorem)

Let $\mathfrak{m}$ be a modulus of K and let H be a congruence subgroup for $\mathfrak{m}$, i.e.

$$P_K(\mathfrak{m}) \subset H \subset I_K(\mathfrak{m}).$$

Then there is a **unique** *abelian extension L/K such that all its ramified primes divide $\mathfrak{m}$, and*

$$I_K(\mathfrak{m})/H \simeq \mathrm{Gal}(L/K)$$

under the Artin map $\Phi_{\mathfrak{m}}$.

Ray class field

Definition (Ray class field)

Let $\mathfrak{m}$ be any modulus for K. The ray class field is the **unique** abelian extension $K_{\mathfrak{m}}$ of K such that

$$\mathrm{Gal}(K_{\mathfrak{m}}/K) \simeq I_K(\mathfrak{m})/P_K(\mathfrak{m}).$$

Example (Cyclotomic extensions)

Let $K = \mathbb{Q}$, $m \in \mathbb{Z}_{>0}$, $m \not\equiv 2 \mod 4$. For $\mathfrak{m} = (m)\infty$,

$$P_{\mathbb{Q}}(\mathfrak{m}) = \{\frac{a}{b}\mathbb{Z} \in I_{\mathbb{Q}}(\mathfrak{m}) \colon a \equiv b \mod m, \frac{a}{b} > 0\}.$$

When $L = \mathbb{Q}(\zeta_m)$, we saw that $\Phi_{L/K,\mathfrak{m}}((a/b)\mathbb{Z}) = [a][b]^{-1}$ for $a/b > 0$.
Thus $\ker(\Phi_{L/K,\mathfrak{m}}) = P_{\mathbb{Q}}(\mathfrak{m}) \implies K_{\mathfrak{m}} = \mathbb{Q}(\zeta_m)$.
If we take the modulus $\mathfrak{m} = (m)$, then the ray class field is $\mathbb{Q}(\zeta_m + \zeta_m^{-1})$.

Ray class groups over $\mathbb{Q}(i)$

Consider $K = \mathbb{Q}(i)$ and modulus $\mathfrak{m}$. Recall $\mathrm{Cl}(K) = 1$. One has

$$P_K(\mathfrak{m}) = \{\frac{\alpha}{\beta}\mathbb{Z}[i] \mid \alpha \equiv \beta \mod \mathfrak{m}\}.$$

If $\beta \in \mathbb{Z}[i]$ is coprime to $\mathfrak{m}$, then there exists $\gamma \in \mathbb{Z}[i]$ such that $1/\beta \equiv \gamma \mod \mathfrak{m}$. Thus $\alpha/\beta\mathbb{Z}[i] \equiv \alpha\gamma\mathbb{Z}[i] \mod P_K(\mathfrak{m})$.
Therefore $I_K(\mathfrak{m})/P_K(\mathfrak{m})$ consists of integral ideal representatives mod $\mathfrak{m}$ that are coprime to $\mathfrak{m}$, i.e.

$$I_K(\mathfrak{m})/P_K(\mathfrak{m}) = (\mathbb{Z}[i]/\mathfrak{m})^\times/U(K)$$

where $U(K) = \{\pm 1, \pm i\}$ is the unit group of K.

Ray class groups over $\mathbb{Q}(i)$, $\mathfrak{m} = (3), (5), (13)$

- Consider $\mathfrak{m} = (3)$. Then

$$(\mathbb{Z}[i]/\mathfrak{m})^\times / U(K) = \mathbb{F}_9^\times / U(K) = \mathbb{Z}/2\mathbb{Z}.$$

  generated by $(1+i)$.

- Consider $\mathfrak{m} = (5)$. Then

$$(\mathbb{Z}[i]/\mathfrak{m})^\times / U(K) = (\mathbb{F}_5^\times \times \mathbb{F}_5^\times)/U(K) = \mathbb{Z}/4\mathbb{Z},$$

  generated by $(1+i)$.

- Consider $\mathfrak{m} = (13)$. Then

$$(\mathbb{Z}[i]/\mathfrak{m})^\times / U(K) = (\mathbb{F}_{13}^\times \times \mathbb{F}_{13}^\times)/U(K) \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}.$$

Artin reciprocity

Conversely, given an abelian extension L/K, we want to describe $\mathrm{Gal}(L/K)$ as a generalised ideal class group for some modulus, induced by the Artin map.

Theorem (Artin reciprocity)

Let L/K be abelian. There exists a modulus $\mathfrak{m}$, divisible by all the primes that ramify in L/K, such that

- $\Phi_{\mathfrak{m}} \colon I_K(\mathfrak{m}) \to \mathrm{Gal}(L/K)$ *is surjective,*
- $\ker(\Phi_{\mathfrak{m}})$ *is a congruence subgroup,*
- *we have an isomorphism*

$$I_K(\mathfrak{m})/\ker(\Phi_{\mathfrak{m}}) \simeq \mathrm{Gal}(L/K).$$

This means the Artin map factors through the ray class group for $\mathfrak{m}$. Such a modulus satisfying this theorem is not unique, but there is a unique 'minimal' modulus.

Conductor

Theorem (Conductor theorem)

Let L/K be an abelian extension. Then there exists a **unique** *modulus $\mathfrak{f} = \mathfrak{f}(L/K)$ such that*

1. *a prime of K ramifies in L if and only if it divides $\mathfrak{f}$,*
2. *let $\mathfrak{m}$ be a modulus divisible by all primes of K that ramify in L. Then $\ker(\Phi_{\mathfrak{m}})$ is a congruence subgroup for $\mathfrak{m}$ if and only if $\mathfrak{f} \mid \mathfrak{m}$.*

Remark

The conductor is the greatest common divisor of all moduli $\mathfrak{m}$ of K for which the Artin reciprocity theorem holds for L/K and $\mathfrak{m}$. In particular the Artin reciprocity theorem holds for $\mathfrak{f}(L/K)$ and it is the minimal such modulus.

Conductor

Example (Quadratic fields)

Let $K = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt{d})$ for d a square-free integer. Let Δ be the discriminant. Then

$$\mathfrak{f}(L/K) = \begin{cases} |\Delta| & d > 0, \\ |\Delta|\infty & d < 0. \end{cases}$$

Example (Cyclotomic fields)

$$\mathfrak{f}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) = \begin{cases} 1 & m \leq 2, \\ (m/2)\infty & m = 2n, n > 1 \text{ odd}, \\ m\infty & \text{otherwise}. \end{cases}$$

Conductor

Example (Warning)

The conductor isn't just the product of ramified primes. For example, let $K = \mathbb{Q}$, $L = \mathbb{Q}(\alpha)$ with $\alpha^3 - 3\alpha - 1 = 0$. This is only ramified at 3. However

- $\ker(\Phi_{\mathfrak{m}})$ isn't a congruence subgroup for $\mathfrak{m} = (3), (3)\infty$,
- $\ker(\Phi_{\mathfrak{m}})$ is a congruence subgroup for $\mathfrak{m} = (9)$.

Remark

The conductor can be computed as the product of local conductors.

Every abelian extension in a ray class field

Corollary (of Takagi existence + Artin reciprocity)

Let L/K and M/K be abelian extensions. Then $L \subset M$ if and only if there is a modulus $\mathfrak{m}$, divisible by all primes of K ramified in either L or M, such that

$$P_K(\mathfrak{m}) \subset \ker(\Phi_{M/K,\mathfrak{m}}) \subset \ker(\Phi_{L/K,\mathfrak{m}}).$$

Corollary

Every abelian extension is contained in a ray class field.

Proof.

If L/K is abelian, and $\mathfrak{f}(L/K) \mid \mathfrak{m}$, then $H := \ker(\Phi_{L/K,\mathfrak{m}})$ is a congruence subgroup by Artin reciprocity, so $P_K(\mathfrak{m}) \subset H$. Then by the above $K_{\mathfrak{m}} \supset L$. □

Kronecker-Weber theorem

Theorem (Kronecker-Weber)

Let $L/\mathbb{Q}$ be an abelian extension. Then there is a positive integer m such that $L \subset \mathbb{Q}(\zeta_m)$.

Proof.

There is an integer m such that $\mathfrak{f}(L/K) \mid (m)\infty := \mathfrak{m}$. Then $L \subset \mathbb{Q}_{\mathfrak{m}} = \mathbb{Q}(\zeta_m)$. □

Example

Consider $L = \mathbb{Q}(\sqrt{d})$ with discriminant Δ. Then $L \subset \mathbb{Q}(\zeta_{|\Delta|})$.

Decomposition Law

Theorem

Let L/K be an abelian extension of degree n. Let $\mathfrak{p}$ be an unramified prime in K. Let $\mathfrak{m}$ be a modulus divisible by $\mathfrak{f}(L/K)$, but not by $\mathfrak{p}$. Suppose f is the the smallest positive integer such that

$$p^f \in \ker(\Phi_{\mathfrak{m}}).$$

Then $\mathfrak{p}$ decomposes in L into a product

$$\mathfrak{p} = \mathfrak{P}_1 \cdots \mathfrak{P}_r$$

of $r = n/f$ distinct prime ideals of degree f over $\mathfrak{p}$.

Example

Consider $\mathbb{Q}(\zeta_q)/\mathbb{Q}$, q prime. For $p \neq q$, p factors into $(q-1)/f$ primes, where f is the least positive integer such that $q \mid p^f - 1$, i.e. $p^f\mathbb{Z} \in P_{\mathbb{Q}}(q\infty)$.

Quadratic reciprocity

Ray class fields over $\mathbb{Q}(i)$

Let $K = \mathbb{Q}(i)$. Recall that we computed

$$\begin{aligned} I_K(\mathfrak{m})/P_K(\mathfrak{m}) &= \mathbb{Z}/2\mathbb{Z}, & \mathfrak{m} &= (3), \\ I_K(\mathfrak{m})/P_K(\mathfrak{m}) &= \mathbb{Z}/4\mathbb{Z}, & \mathfrak{m} &= (5), \\ I_K(\mathfrak{m})/P_K(\mathfrak{m}) &= \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}, & \mathfrak{m} &= (13). \end{aligned}$$

Claim: for $\mathfrak{m} = (3)$, $K_\mathfrak{m} = \mathbb{Q}(i, \zeta_3) = K(\zeta_3)$.
Note $\mathrm{Gal}(K(\zeta_3)/K) \simeq (\mathbb{Z}/3\mathbb{Z})^\times$. If $(a+ib)\mathbb{Z}[i] \in I_K(\mathfrak{m})$ is a prime ideal, then the Artin symbol is defined by

$$\left(\frac{K(\zeta_3)/K}{a+ib}\right)(\zeta_3) = \zeta_3^{N_{K/\mathbb{Q}}(a+ib)}.$$

$\Phi_\mathfrak{m}$ is surjective (image of $1+i$ non-trivial), so $[I_K(\mathfrak{m}) : \ker(\Phi_\mathfrak{m})] = 2$. If $a + ib \equiv 1 \pmod 3$ for $a + ib \in \mathbb{Z}[i]$ then $N_{K/\mathbb{Q}}(a+ib) \equiv 1 \pmod 3$ so that $\zeta_3^{N_{K/\mathbb{Q}}(a+ib)} = \zeta_3$ and $(a+ib)\mathbb{Z}[i] \in \ker \Phi_\mathfrak{m}$. Thus
$P_K(\mathfrak{m}) \in \ker(\Phi_\mathfrak{m}) \implies P_K(\mathfrak{m}) = \ker(\Phi_\mathfrak{m})$ since they have equal index in $I_K(\mathfrak{m})$.

Ray class fields over $\mathbb{Q}(i)$

Let $K = \mathbb{Q}(i)$. Recall that we computed

$$\begin{aligned} I_K(\mathfrak{m})/P_K(\mathfrak{m}) &= \mathbb{Z}/2\mathbb{Z}, & \mathfrak{m} &= (3), \\ I_K(\mathfrak{m})/P_K(\mathfrak{m}) &= \mathbb{Z}/4\mathbb{Z}, & \mathfrak{m} &= (5), \\ I_K(\mathfrak{m})/P_K(\mathfrak{m}) &= \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}, & \mathfrak{m} &= (13). \end{aligned}$$

For $\mathfrak{m} = (5)$, $K_\mathfrak{m} = \mathbb{Q}(i, \zeta_5)$.

For $\mathfrak{m} = (13)$, $\mathbb{Q}(i, \zeta_{13}) \subsetneq K_\mathfrak{m}$. The Artin map $\phi_\mathfrak{m}$ for $\mathbb{Q}(i, \zeta_{13})/K$ contains $P_K(\mathfrak{m})$ in its kernel.

No C_4 extension of $\mathbb{Q}(i)$ ramified only at 11.

Again let $K = \mathbb{Q}(i)$. Let L/K be an abelian extension, ramified only at 11. Then $\mathfrak{f} = \mathfrak{f}(L/K) = (11^n)\mathbb{Z}_K$ and $L \subset K_{\mathfrak{f}}$. One has

$$\mathrm{Gal}(K_{\mathfrak{f}}/K) \simeq I_K(\mathfrak{f})/P_K(\mathfrak{f}) = (\mathbb{Z}_K/(11^k))^{\times}/U(K)$$

$$= (11\text{-group}) \times \mathbb{F}_{121}^{\times}/U(K) = (11\text{-group}) \times (\mathbb{Z}/30\mathbb{Z}).$$

Then $\mathrm{Gal}(L/K)$ is a quotient of $\mathrm{Gal}(K_{\mathfrak{f}}/K)$. For example, this has no C_4 quotient, so there does not exist a C_4 extension of $\mathbb{Q}(i)$ ramified only at 11.

Ray class field for $\mathbb{Q}(\zeta_3)$

Let $K = \mathbb{Q}(\zeta_3)$. Then $\mathrm{Cl}(K) = 1$. Consider the modulus $\mathfrak{m} = 6\mathbb{Z}[\zeta_3]$. Now $6\mathbb{Z}[\zeta_3] = 2\mathbb{Z}[\zeta_3] \cdot (2+\zeta_3)^2\mathbb{Z}[\zeta_3]$. Thus

$$I_K(\mathfrak{m})/P_K(\mathfrak{m}) = (\mathbb{Z}[\zeta_3]/\mathfrak{m})^\times / U(K)$$

$$\simeq \left((\mathbb{Z}[\zeta_3]/(2))^\times \times (\mathbb{Z}[\zeta_3]/(2+\zeta_3)^2)^\times\right)/U(K) = C_3,$$

recalling $|U(K)| = 6$.

Claim: $K_\mathfrak{m} = \mathbb{Q}(\zeta_3, \sqrt[3]{2}) = K(\sqrt[3]{2})$.

By the decomposition law, a prime $\mathfrak{p}$ in K splits completely in $K_\mathfrak{m}$ if and only if it has a generator which is $1 \pmod{\mathfrak{m}}$. For example $5\mathbb{Z}_K$, $(1+6\zeta_3)\mathbb{Z}_K$ are prime and split in $K_\mathfrak{m}$. If $p \equiv 2 \pmod 3$ then it is inert in K and splits completely in $K_\mathfrak{m}/K$.