LECTURE 4

YIHANG ZHU

1. Basic ramification theory

In this section L/K is a finite Galois extension of number fields of degree n. The Galois group $\mathrm{Gal}(L/K)$ acts on various invariants of L, for instance the group of fractional ideals I_L and the class group $\mathrm{Cl}(L)$. If $\mathfrak{P}$ is a prime of L above $\mathfrak{p}$ of K, then any element of $\mathrm{Gal}(L/K)$ sends $\mathfrak{P}$ to another prime above $\mathfrak{p}$. We have

Proposition 1.1. *Let L/K be a finite Galois extension of number fields. Then for any prime $\mathfrak{p}$ of K, the Galois group $\mathrm{Gal}(L/K)$ acts transitively on the set $\{\mathfrak{P}_i\}_{1\leq i\leq g}$ of primes of L above $\mathfrak{p}$. In particular, the inertia degrees f_i are the same, denoted by $f = f(\mathfrak{p}, L/K)$, and by unique factorization, the ramification degrees e_i are the same, denoted by $e = e(\mathfrak{p}, L/K)$. The fundamental identity reduces to*

$$efg = n.$$

Let $\mathfrak{P}$ be a prime of L above a prime $\mathfrak{p}$ of K. Let e, f, g be as above.

Definition 1.2. The stabilizer of $\mathfrak{P}$ in $\mathrm{Gal}(L/K)$ is called the *decomposition group* of $\mathfrak{B}$, denoted by $D(\mathfrak{P})$. The corresponding subfield $L^{D(\mathfrak{P})}$ of L is called the *decomposition field*, denoted by $Z_{\mathfrak{P}}$.

Remark 1.3. For $\sigma \in \mathrm{Gal}(L/K)$, $D(\sigma\mathfrak{P}) = \sigma D(\mathfrak{P})\sigma^{-1}$ and $Z_{\sigma\mathfrak{P}} = \sigma(Z_{\mathfrak{P}})$.

The group $\mathfrak{P}$ is the stabilizer in a group of order n on an orbit of cardinality g, so its order is $n/g = ef$. Let $\mathfrak{P}_Z$ be the prime of $Z_{\mathfrak{P}}$ lying under $\mathfrak{P}$. The Galois group of $L/Z_{\mathfrak{P}}$ is $D(\mathfrak{P})$, and it should act transitively on the primes of L above $\mathfrak{P}_Z$. This shows that $\mathfrak{P}$ is the only prime of L above $\mathfrak{P}_Z$.

Proposition 1.4. $e(\mathfrak{P}/\mathfrak{P}_Z) = e(\mathfrak{P}/\mathfrak{p}), f(\mathfrak{P}/\mathfrak{P}_Z) = f(\mathfrak{P}/\mathfrak{p}), e(\mathfrak{P}_Z/\mathfrak{p}) = f(\mathfrak{P}_Z/\mathfrak{p}) = 1$.

Proof. We have $e(\mathfrak{P}/\mathfrak{P}_Z)e(\mathfrak{P}_Z/\mathfrak{p}) = e(\mathfrak{P}/\mathfrak{p})$ and $f(\mathfrak{P}/\mathfrak{P}_Z)f(\mathfrak{P}_Z/\mathfrak{p}) = f(\mathfrak{P}/\mathfrak{p})$ because the functions $e(\cdot), f(\cdot)$ are certainly multiplicative in the suitable sense. But by the fundamental identity applied to the extension $L/Z_{\mathfrak{P}}$ which is of degree $e(\mathfrak{P}/\mathfrak{p})f(\mathfrak{P}/\mathfrak{p})$, we have $e(\mathfrak{P}/\mathfrak{P}_Z)f(\mathfrak{P}/\mathfrak{P}_Z) = e(\mathfrak{P}/\mathfrak{p})f(\mathfrak{P}/\mathfrak{p})$. □

The decomposition group $D(\mathfrak{P})$ acts on the residue field $\mathcal{O}_L/\mathfrak{P}$, and the action is trivial on the subfield $\mathcal{O}_K/\mathfrak{p}$, so we get a homomorphism

$$D(\mathfrak{P}) \to \mathrm{Gal}(\kappa(\mathfrak{P})/\kappa(\mathfrak{p})).$$

Lemma 1.5. *The above homomorphism is surjective.*

Definition 1.6. We call the kernel of the above homomorphism the *inertia group* of $\mathfrak{P}$, denoted by $I(\mathfrak{P})$. Its fixed field is called the *inertia field* of $\mathfrak{P}$ and denoted by $T_{\mathfrak{P}}$.

Remark 1.7. The order of $I(\mathfrak{P})$ is equal to $ef/f = e$. Hence $\mathfrak{p}$ is unramified in L if and only if $I(\mathfrak{P}) = 1$.

In summary, we have a chain of groups $\mathrm{Gal}(L/K) \supset D(\mathfrak{P}) \supset I(\mathfrak{P})$, corresponding to a chain of fields $K \subset Z_{\mathfrak{P}} \subset T_{\mathfrak{P}} \subset L$. Let $\mathfrak{P}_Z, \mathfrak{P}_T$ be the primes of $Z_{\mathfrak{P}}$ and $T_{\mathfrak{P}}$ under $\mathfrak{P}$ respectively.

- In the extension $Z_{\mathfrak{P}}/K$, which might not be Galois, we have $\kappa(\mathfrak{P}_Z) = \kappa(\mathfrak{p})$ and $\mathfrak{P}_Z$ is unramified over $\mathfrak{p}$.
- The extension $Z_{\mathfrak{P}} \subset T_{\mathfrak{P}}$ is Galois with Galois group naturally isomorphic to $\mathrm{Gal}(\kappa(\mathfrak{P})/\kappa(\mathfrak{p}))$. The prime $\mathfrak{P}_Z$ stays inert in the extension $T_{\mathfrak{P}}/Z_{\mathfrak{P}}$, namely $\mathfrak{P}_T = \mathfrak{P}_Z \mathcal{O}_{T_{\mathfrak{P}}}$.
- In the extension $L/T_{\mathfrak{P}}$, the prime $\mathfrak{P}_T$ factorizes as $\mathfrak{P}^e$ in L, with no residue extension, i.e. $\kappa(\mathfrak{P}) = \kappa(\mathfrak{P}_T)$.

Definition 1.8. Suppose $\mathfrak{p}$ is a prime of K unramified in L. For each prime $\mathfrak{P}$ of L above $\mathfrak{p}$, define the element $\mathrm{Frob}_{\mathfrak{P}/\mathfrak{p}} \in \mathrm{Gal}(L/K)$ to be the preimage of the Frobenius element $x \mapsto x^{|\kappa(\mathfrak{p})|}$ under the isomorphism $D(\mathfrak{P}) \to \mathrm{Gal}(\kappa(\mathfrak{P})/\kappa(\mathfrak{p}))$. When $\mathfrak{P}$ varies, the elements $\mathrm{Frob}_{\mathfrak{P}/\mathfrak{p}}$ form a conjugacy class of $\mathrm{Gal}(L/K)$, denoted by $\mathrm{Frob}_{\mathfrak{p}} = (\mathfrak{p}, L/K)$, called the *Frobenius conjugacy class* or the *Artin symbol*.

Remark 1.9. By definition, $\mathrm{Frob}_{\mathfrak{P}/\mathfrak{p}}$ is the unique element $\sigma \in \mathrm{Gal}(L/K)$ characterized by the following property: For any $x \in \mathcal{O}_L$,

$$\sigma x \equiv x^{|\kappa(\mathfrak{p})|} \mod \mathfrak{P}, \text{ i.e. } \sigma x - x^{|\kappa(\mathfrak{p})|} \in \mathfrak{P}.$$

Remark 1.10. When L/K is abelian, the Frobenius conjugacy class becomes an element.

2. Unramified class field theory

Definition 2.1. Let v be a real embedding of K. We say v is unramified in L if v extends to a real embedding of L (rather than a complex embedding).

Example 2.2. The real embedding of $\mathbb{Q}$ is unramified in $\mathbb{Q}(\sqrt{2})$, but ramified in $\mathbb{Q}(\sqrt{-2})$.

Definition 2.3. We say L/K is *unramified everywhere* or simply *unramified* if any prime ideal of K is unramified in L, and any real embedding of K is unramified in L.

The following theorem is an important special case of class field theory.

Theorem 2.4 (Unramified Class Field Theory)**.** *Let K be a number field. Fix an algebraic closure $\bar{K}$ of K. Inside $\bar{K}$ there exists a finite extension H/K that is abelian and unramified, such that any abelian and unramified extension of K contained in $\bar{K}$ is contained in L. Moreover, the map*

$$I_K \to \mathrm{Gal}(H/K), \mathfrak{p} \mapsto (\mathfrak{p}, H/K)$$

induces an isomorphism

$$\mathrm{Cl}(K) \xrightarrow{\sim} \mathrm{Gal}(H/K).$$

The field H is called the Hilbert class field of K.

Remark 2.5. A priori it may happen that K had arbitrarily large abelian unramified extensions, and in that case there would not be a maximal one.

Example 2.6. If $h_K = 1$ then $H = K$. In particular $\mathbb{Q}$ has no abelian unramified extension. In fact $\mathbb{Q}$ does not admit any unramified extension.

Example 2.7. The Hilbert class field of $K = \mathbb{Q}(\sqrt{-14})$ is $K(\sqrt{2\sqrt{2}-1})$. To show this, one first checks that $K(\sqrt{2\sqrt{2}-1})/K$ is a degree 4 abelian extension unramified everywhere. Next the class number of K can be computed (e.g. using the class number formula) to be 4. These two things imply that $K(\sqrt{2\sqrt{2}-1})$ is indeed the Hilbert class field of K.

Corollary 2.8. *Let H be the Hilbert class field of K. Then a prime $\mathfrak{p}$ of K is split in H if and only if $\mathfrak{p}$ is principal.*

Proof. Since $\mathfrak{p}$ is unramified, from the fundamental identity $n = fg$ we see that $\mathfrak{p}$ is split if and only if $f = 1$. But $f = 1$ means $(\mathfrak{p}, H/K) = 1$. □

Theorem 2.9 (Artin's principal ideal theorem)**.** *Let H be the Hilbert class field of K. Let $\mathfrak{a}$ be a fractional ideal of K. Then $\mathfrak{a}\mathcal{O}_H$ is a principal fractional ideal of H.*

Example 2.10. Using the last theorem, we can deduce the following statement: Let $f(X) = (X^2+1)^2 - 8$. A prime number p is of the form $p = x^2 + 14y^2, x, y \in \mathbb{Z}$, if and only if

$$(*) \qquad (\frac{-14}{p}) = 1, \& \exists x \in \mathbb{Z}, f(x) \equiv 0 \mod p$$

To prove this, let $K = \mathbb{Q}(\sqrt{-14})$ and H be the Hilbert class field of K. By the previous example, we know $H = K(\alpha)$ where α has minimal polynomial $f(X)$ over $\mathbb{Q}$. It is not hard to show that the condition $(*)$ is equivalent to the condition that p is split in H. But we have $p = x^2 + 14y^2 \Leftrightarrow p\mathcal{O}_K = \mathfrak{p}\bar{\mathfrak{p}}$ with $\mathfrak{p}$ a principal prime ideal of $\mathcal{O}_K$, $\Leftrightarrow p\mathcal{O}_K = \mathfrak{p}\bar{\mathfrak{p}}$ with $\mathfrak{p}$ a prime ideal of $\mathcal{O}_K$ that is split in H, $\Leftrightarrow p$ is split in H.

If we want to generalize the last example to study $p = x^2 + ny^2, n \geq 1$, we would like to find explicit generators of the Hilbert class field of $K = \mathbb{Q}(\sqrt{-n})$. In fact for general n, there is no reason to hope that $\mathbb{Z}[\sqrt{-n}] = \mathcal{O}_K$, (e.g. $n = 9$), and when $\mathbb{Z}[\sqrt{-n}] \neq \mathcal{O}_K$, we indeed need to look at abelian extensions of K other than the Hilbert class field, and to try to find their generators. The theory of complex multiplication, the main theme of the tutorial, provides a systematic way of doing that.

When we start to talk about complex multiplication, the first goal will be to generate the Hilbert class field of an imaginary quadratic field using special values of a holomorphic function called j, defined on the upper half plane $\{z \in \mathbb{C} | \Im z > 0\}$.